Ciudad de México, 10 de abril de 2024.

Versión estenográfica de la Sesión Especializada *Administración de riesgos de infraestructura crítica, ciberseguridad y el papel del seguro*, durante el segundo día de actividades de la 33 Convención de Aseguradores AMIS "Asegurando un Mundo en Transformación", llevada a cabo en la sede Expo Santa Fe.

Versión estenográfica del Panel "Administración de riesgos de infraestructura crítica, ciberseguridad y el papel del seguro".

Eugenia Martínez: Sé que suena siempre trillado en las convenciones abrir con: "Es un gusto para nosotros estar con ustedes", pero en verdad yo todavía tengo el corazón de aseguradora, entonces pienso que es un gusto para mí estar en AMIS, tanto para compartir espacio con mis colegas actuarios, compartir espacio con los aseguradores, que se conviertan definitivamente en profesionistas que admiro.

Entonces, es un gusto para mí estar con ustedes.

Les quiero contar brevemente. El tema de hoy es el de la Administración de riesgos, infraestructura crítica, ciberseguridad y el papel del seguro.

Y fíjense que a mí todavía me suena, en las reuniones que tenemos con la industria aseguradora mexicana, que llegamos a hablar y la gente se imagina esto.

Cuando hablamos de ciberseguridad, ciberataques, qué está pasando, todavía están pensando en un futuro, pues ahí está, quizá en algún momento lo tendremos cerca, pero no es un presente.

Ya lo vimos en esta Convención que es un presente y es bastante cercano. Lo podemos ver desde la perspectiva de la oferta, la perspectiva de las operaciones.

Hay una realidad en donde hay una digitalización inminente en todos los esquemas, pero además hay una necesidad también de protección.

Aquí vamos a entrar en un entorno, en una charla de un entorno macro y vamos a tratar de entrar después individualmente para ver qué es lo que observamos, al menos a nivel de la calificadora en cuestión de riesgos cibernéticos para las aseguradoras mexicanas.

Y bien, por ahí estuve buscando en internet, no sé si lo han buscado, los ciberataques a nivel global, pues resulta que está esta página Live Cyber Redma, que en tiempo real nos está mostrando cuáles son los ataques cibernéticos que se dan a nivel mundial.

Esta es una foto de solamente unos segundos, pero en realidad si se quedan viéndolo tres minutos parece una locura, porque están migrando todos los riesgos de un lado a otro, de mailware, phishing explote, esto es lo que monitorea esta página, es increíble, eso está pasando en tiempo real no sólo en nuestros dispositivos móviles, sino también en nuestras compañías. Entonces, ¿qué tanto es futuro? Pues no lo sé ¿verdad?

Aquí les muestro un índice, este es un índice un poquito más estandarizado a nivel global de lo que representa la ciberseguridad a nivel macro. Se ha publicado este national cybersecurity index en donde México se posiciona en el número 28 a nivel global, pero ¿qué mide? ¿qué es lo que realmente dice?

Estandariza criterios como qué tipo de crisis, manejo de crisis hay, qué tipo de políticas, cuál es la regulación de los países en torno a ciberseguridad, etcétera, entonces, ¿lugar 28 a nivel global qué significa en realidad?

Más que eso a mí me llamó la atención mucho una cosa, y les prometo que sería muy interesante que ustedes ya lo empiecen a pensar en sus entornos directos, mide la diferencia entre el national cybersecurity index, que es justamente el desarrollo en ciberseguridad que existe, y el desarrollo de tecnología digital.

La diferencia en México es de 23.83, bueno, en sus compañías o en sus entornos qué tanta digitalización hay y qué tanta ciberseguridad existe. Sería interesante que se lo pregunten, porque quizás hablamos mucho de innovar y sí vamos a hacer procesos muy coquetos, muy bonitos y muy accesibles, qué tanta protección hay detrás.

Para darles el contexto general, a nivel global aquí está la lista del top ten de países que tienen una clasificación más alta en riesgo de ciberseguridad.

Está en primer lugar Estados Unidos, con una puntuación de cien por ciento, ya les contaré un poco. Y en el siguiente cuadro hablamos, no es LATAM, perdón, es América, el Continente Americano, porque vemos Estados Unidos, Canadá y Brasil en los primeros lugares, México en el cuarto.

Y bien, ¿qué es lo que aquí me interesó mucho resaltar para aterrizarlo al sector asegurador mexicano?

Varias cosas.

Primero. No se trata nada más de tener una persona que se le ocurrió una idea muy bonita de implementar tecnología, se trata de tener todo un marco que realmente permita una gestión de riesgos cibernéticos y que realmente permita optimizar todo este esquema den pro de la compañía.

Bueno, no creo y no he visto aquí ninguna compañía sin fines de lucro, pero por ahí si existen hay otros foros.

Hay medidas jurídicas, técnicas, institucionales de captación y cooperación.

¿Qué quiere decir?

Hay marcos regulatorios bastante robustos en donde se establecen cuáles son los criterios que se determinen para identificar primero qué es un riesgo cibernético, en dónde podrían estar las causantes, cuál es el manejo del riesgo, cómo es que se gestiona un riesgo cibernético cuando este acontece.

Para darles el ejemplo, les traigo el caso de Estados Unidos, el país que tiene el cien por ciento.

Aquí existe primero una agencia, no la cybersecurity and infraestructure security agency.

Ellos tienen una estructura tan establecida en donde primero, me voy a enfocar aquí, tienen definidos qué sectores específicamente son clasificados como infraestructura crítica.

Estuve buscando en las páginas mexicanas, existe también la Secretaría de Seguridad Cibernética, y aquí no había establecido que, o sea, te dice general ¿no? Cualquier sector que pueda tener un impacto en la economía local, pero no te dice exactamente pueden ser presas, puede ser bases militares, puede ser comida y agricultura, pueden ser instituciones financieras, como es nuestro caso.

En este país, en Estados Unidos, no solamente existe la definición de qué sectores son clasificados como infraestructura crítica, sino quiénes son los participantes que intervienen, internos, externos. También existen los terceros, los proveedores de servicios, los que interactúan con este tipo de segmentos.

Existen políticas específicas, y una de las que más me llamó la atención es la relacionada con instituciones financieras.

En Estados Unidos las compañías tienen que avisar al menos cuatro días después de que se suscita cualquier evento cibernético a los reguladores.

Evidentemente es todo un tema, porque ustedes si algún día han tenido algún contacto con un riesgo cibernético, pues no se cuantifica inmediatamente, no es un dato que te atacan y ya tienes a los cuatro días el impacto.

Pero lo que sí sabes es que existió y qué operaciones te está impactando, cuáles son los riesgos que podrías tener.

Y aquí sí la función de riesgos me parece que ya tiene un papel bastante importante que generar, porque ya no se trata únicamente de decir: esto es un riesgo emergente, este es un riesgo que por ahí está. No, ahí está y al día de hoy, no podemos sin decir nombres, pero ya ha habido ataques a compañías aseguradoras mexicanas, ya ha

habido ataques a reguladores en toda la región, ya no es sorpresa, esto ya sucede.

Y aquí es en donde entra en función muy importante cuáles son las políticas y procedimientos que se ejecutan, y justamente cómo vemos esto como un beneficio.

Ahora bien, la pregunta del millón, y ya aterrizándolo: ¿la inversión digital es un pasivo o es un activo? Pues dependerá, dependerá de las diferentes ópticas que vamos a estar analizando.

Por un lado, sin lugar a dudas lo hemos platicado la oferta, cómo vas acercarte a un sector específico que quizás está en contra de un agente, pues quizás el único canal es la digitalización, cómo vas a tener base de datos más robustas, cómo vas a tener una mejor atención a cliente. Pues definitivamente sí es a través de la digitalización.

Ahí es en donde creo que en particular en la Industria Aseguradora Mexicana hay un retraso importante porque no hay un acercamiento digital palpable todavía en muchas de las compañías, están empezando por optimizar algunas operaciones, procesos operativos, pero no necesariamente llegando a este punto, llegando al punto de realmente cuál es mi valor agregado y en dónde puedo hacer mucho más eficiente en varios puntos.

Entonces, ¿qué es una realidad? Como administradores de riesgos en la función corresponde medir esa rentabilidad. ¿Qué tanto le genera un valor agregado a la compañía hacer qué? ¿Qué tanto realmente puede implicar también un riesgo adicional y qué puedo hacer yo para mitigarlo, porque siendo honestos, hablando de toda esta tecnología no sé si en algunas otras convenciones y foros han comentado, incluso la Inteligencia Artificial ya está preparada para generar códigos para hackear las protecciones que tú estableciste, pues ya es una locura y es como el círculo de qué fue primero, el huevito o la gallina, qué fue primero. Y esa es una realidad, qué hacemos como compañía realmente para decir estamos viviendo este presente o estamos en ese futuro que sabe Dios qué vamos a hacer y cómo vamos a reaccionar.

Hay una necesidad de contratación de profesionistas de seguridad, ¿pero quiénes lo saben? ¿Quiénes realmente están ahí? Bueno, en algunos otros espacios también se comenta, contratan a los mismos hackers para hacer las evaluaciones de riesgo y se vale porque son quienes tienen el conocimiento; pero también hay que pensar más allá, creo que en varios espacios aquí en AMIS se han conversado, la realidad es que muchas veces las compañías no están entrando a un esquema de análisis en la optimización de la digitalización, quiero digitalizar, ¿para qué? ¿Qué quiero lograr? Quiero lograr una buena atención, quiero lograr una eficiencia, quiero lograr un mejor manejo de datos, quiero lograr también estar en la punta del Iceberg, se vale.

Bueno, entonces cómo voy a monitorear todos estos tipos de riesgos, porque también si vas a contratar a una persona que se encargue de ello pues también son recursos y ellos tendrán que ser capaces también de poder medir esa rentabilidad dentro de la compañía que no es nada trivial.

La realidad es que el aumento en la frecuencia y en la severidad de los riesgos cibernéticos a las compañías en general ha ido en aumento, esa es una realidad.

Otra realidad que la medición, muchos de ustedes como probablemente actuarios o en la parte técnica y de riesgos, no existe la experiencia suficiente afortunadamente para medirlo, pero eso no significa que no está existiendo y que no estén expuestos a estos riesgos, como por ejemplo la disrupción de negocios que no se plantean en los riesgos cibernéticos; la falta de operaciones, muchas de las compañías han dejado de pagar siniestros por riesgos cibernéticos y esa es una realidad que las áreas de riesgo también deberían estar monitoreando.

Para darles una idea y esta es una publicación que sacó Fitch en este año particularmente; en 2017 hubo un ataque mundial de un malware llamado Petya, éste fue ocasionado durante el conflicto en Rusia y Ucrania, este malware imagínense que tuvo unas pérdidas económicas alrededor de 10 billones de dólares, nosotros lo equiparamos con un riesgo de tormenta media catastrófica en Estados Unidos, porque por ejemplo para darles del contexto Catrina fue 11 veces más grande que este ataque con 125 billones de dólares de

pérdidas económicas. Ahí está el contexto de lo que podemos medir y de lo que podemos ver, pero definitivamente está en las manos.

Y, bueno, nada más a mí me pareció interesante verlo. Esto que les muestro aquí es, literal, una búsqueda de nuestro sitio web, dije: “A ver qué tanto se publica a nivel de riesgo crediticio en cuestión de riesgos cibernéticos y de ciberseguridad”. Pues salió todo esto.

Estoy viendo temas desde Costa Rica, riesgo soberano en Costa Rica, estoy viendo el sector salud en Estados Unidos, instituciones financieras, *Extract Finance*, productos de *Extract Finance,* etcétera, etcétera, es una realidad.

Y aquí la pregunta, y esa es la que me gustaría dejar en sus mentes, cómo llega entonces y en este caso una agencia calificadora, pero cómo se evalúa el riesgo crediticio de un evento como estos, cómo se evalúa el riesgo cibernético y las afectaciones que pueden existir.

Bueno, aquí les dejo el ejemplo justo del *healthcare*, del ciberataque en Estados Unidos, este fue un periodicazo, no usen esas cifras como reales porque no las revisé, solo quise ponerles el periodicazo de 14 billones de rezagos por pérdidas, por reclamaciones por pagar, 14 billones de dólares.

¿Qué es lo que implicó? Esta compañía definitivamente tuvo que parar operaciones por unas semanas, esta compañía no pudo pagar sus servicios con terceros y, por lo tanto, tampoco pudo pagar sus reclamaciones. Creo que nadie quisiera estar en esa situación por un pequeño virus.

Ahora, pequeño virus resulta que sabían que el 85 por ciento de los hechos cibernéticos, de los ataques cibernéticos materializados provienen de un error humano, de nuestros empleados que dan clic al *fishing* de nosotras mismas que decimos: “Voy abrir este archivo, no pasa nada, sí voy a entrar a esta página, ahí abrimos la puerta, 85 por ciento, 14 billones de dólares”.

La otra noticia que también tengo, esto no es periodicazo, esa sí es de nuestra página, el incidente en Prudencial, que aquí es en donde les digo, aquí entró para nosotros también una parte muy importante de

monitoreo porque justamente comentamos que existió, la compañía dice: “¿Sabes qué? Nuestras estimaciones iniciales son que hay un efecto en tal, pero falta mucho y sabemos que lo que falta todavía es más fuerte de lo que inicialmente estamos proyectando. A eso nos estamos enfrentando hoy en día.

Y aquí me gusta comentarles cómo se ve ya tangiblemente o cómo trato de explicar tangiblemente cómo evaluamos nosotros un riesgo cibernético y cómo puede impactar en la calidad crediticia de un país, de una aseguradora, de una institución financiera, porque aquí hablo de lo mismo, pero les traje obviamente el ejemplo de las aseguradoras.

Nosotros tenemos factores crediticios y este es un ejemplo genérico para México en donde evaluamos diferentes factores crediticios. Entonces, ahora bien, una compañía, vamos a suponer, esta de salud es impactada por un evento de riesgos cibernético.

¿Qué sucedió? Inmediatamente ya sabíamos que había una deficiencia en la parte de performance, iba haber pérdidas ya seguro, ¿por qué? Porque la compañía primero dejó de producir, ya no pudo producir por dos semanas cuando menos, no pudo generar ingresos, aparte tuvo retrasos en los pagos con sus proveedores que también causaron en algunos casos algunas cuotas que pagar y obviamente tenemos el riesgo reputacional.

¿Qué más pasa? De manera inmediata nosotros lo que tenemos son lo que denominamos triggers. El trigger ya determina específicamente qué elementos crediticios pueden generar mayor sensibilidad a una calificación crediticia.

¿Entonces, qué sucede? Que si ya sabemos que una compañía tiene problemas de liquidez, entonces en Financial Performance en liquidez, yo voy a decir: “¿Sabes qué? Esta ya está muy cercana y cualquier cosa, y está, bueno, le puede terminar causando un deterioro importante en su perfil crediticio.

Y ¿qué puede pasar? Si esto no es contenido, y si esto también tiene un impacto mayor en su perfil financiero se puede migrar ese impacto a capitalización y apalancamiento. La compañía puede, incluso,

requerir capital para hacer frente a esas obligaciones. Y last, no least, porque ese siempre lo menciono fuertemente la parte de gobierno corporativo.

¿Cuál es el manejo de los riesgos que tienen las compañías? ¿Cuál es el manejo de crisis? ¿Qué hacen? ¿Qué hacen en sus compañías? ¿Tienen ahorita algún protocolo en el cual saben qué sucede?

Imagínense, y toco madera, no hay madera pero quien tenga madera, porque creo que nadie quiere que, por ejemplo, abran un archivo ahorita y luego, luego les aparece el negro y un monito de que algo pasó y está grave.

¿Qué hacen? ¿Saben qué hacer ustedes? ¿Saben? Hay alguna política que les diga: “En la compañía pasó esto. Entonces ponte a pensar tienes que ir con tu área de no sé quién”. Obviamente, yo creo que todos iríamos con nuestro Manager y le diríamos: “Tuve un problemita”. Pero hasta ese grado.

Para darles un contexto, nosotros en general, compañías aseguradoras que nos hayan compartido información de gobierno corporativo que sí tengan una estructura de riesgo cibernético. Una, una, una, una que en realidad, o sea, obviamente en otras pueden haberlo. Pero un componente tan complejo de riesgo corporativo, dentro de gobierno corporativo dentro de la administración de riesgos, no. Estoy de acuerdo. Y ahí volvemos a la discusión de activo contra pasivo.

Tampoco vas a querer tener un equipo muy sólido de ciberseguridad, que cuesta muy caro porque tampoco tienes la digitalización, pero hoy la respuesta la tienen ustedes, la tenemos nosotros como aseguradores, digo nosotros; pero la tenemos como aseguradores, porque justamente nos toca plantearnos eso el costo-beneficio.

Te puede salir muchísimo más caro, el no hacer esta introspección, y no me dejarán mentir pero el papel de las aseguradoras, el papel de las aseguradoras. Si se dan cuenta los el 80, 90 por ciento de esta presentación fue para ver hacia adentro.

Somos administradores de riesgos, somos administradores de riesgos. ¿Qué estamos haciendo en el interior? ¿Realmente estamos monitoreando los diferentes riesgos? ¿Realmente estamos atendiendo las necesidades? ¿Realmente estamos llegando a dar una oferta de valor agregado a través de la digitalización? ¿Realmente estamos operando digitalmente al interior?

Respondiendo esas dos preguntas, la pregunta es ¿qué vamos a ofrecer afuera? ¿Qué podemos hacer? Ayer decía Daniella Guerra: "Hay que prepararnos para asegurar el metaverso". Sí, por supuesto. ¿Estamos listos? ¿Lo estamos haciendo? ¿Estamos realmente en ese canal? Y ¿estamos realmente en la tesitura de poder hacer esa oferta cuando en el interior todavía, en el interior todavía hay ciertos elementos de riesgo que no estamos analizando? Esa realmente es la pregunta.

Y hasta acá dejo mi presentación, pero la dejo abierto a preguntas del público. Yo soy de las que pregunto. No, no es cierto. Hoy no.

Aquí hay una, don Roberto.

Roberto Ávila: Hola. Roberto Ávila, de seguros "Ve por más".

A lo mejor me salgo un poquito del tema, pero en la parte de los riesgos habíamos platicado alguna vez, te había preguntado ¿las calificadoras cómo están participando en marcar a las empresas que efectivamente sí tienen una huella verde en sus emisiones de activos? Porque al final creo que sí está muy relacionado al entorno de todos los riesgos, no solo ciberseguridad, sino todos los riesgos que están entrando a este esquema de administración de riesgos que debemos de monitorear y que al final están conectados.

Eugenia Martínez: Gracias por la pregunta, y qué bueno que me lo recordaste, porque justamente, y por eso no olviden sus notas, aquí les presento. Nosotros lo que hacemos, Roberto, es considerar. En todas nuestras calificaciones desde hace tres años sacamos ese semaforito que es del …

¿Nosotros qué es lo que hacemos? Evaluamos los diferentes criterios para justamente el cumplimiento. Entonces, ¿qué quiere decir? Por

ejemplo, la compañía que les conté de salud, que acabamos de ver, tiene una calificación más en deterioro en … en Social for cybersecurity, por la implicación que tenían.

También tienen en el en la parte de gobernance, la falta de manejo de crisis. ¿Y qué quiero decir? Cuando nosotros en cuestión de emisiones no hay un impacto directo en la calificación crediticia, pero puede haber un impacto directo en nuestra evaluación de ISG, y ahí sí podemos decir, y nuestra responsabilidad y parte de lo que ya siempre hacemos es cuando hay, imagina esto, nosotros sacamos estándares de ISG para las aseguradoras mexicanas, pero si sabemos, por ejemplo, si una compañía tiene más concentración, por ejemplo, está asegurando sindicatos o están asegurando un apetito mayor en energía. Esas compañías van a tener impactos ISG más altos. En esas compañías nosotros siempre hacemos un comentario. Cuando son calificaciones altas, decimos: “Esta compañía tiene un elemento ISG, que si tiene un impacto en su calificación y proviene de, y podrían ser las diferentes características de ISG. Gracias.

Presentador: Agradecemos a Eugenia. Eugenia, muchísimas gracias por este excelente análisis. Le damos un fuerte aplauso y vamos a pasar con nuestra siguiente sesión.

--oo0oo--