Ciudad de México, 14 de mayo de 2019.

Versión estenográfica de la Sesión Especializada "Retos y Oportunidades en Ciberseguridad en el sector asegurador", en el marco de la 29 Convención de Aseguradores AMIS, llevada a cabo en el Salón Montejo 3, del Centro Citibanamex.

Moderador: Buenas tardes a todos.

Permíteme que me presente. Soy Óscar Díez, yo soy el Director General de INDRA y Minsait de México, y me invitaron a poder moderar este panel con tres colegas, y vamos a hacerlo de la forma más dinámica posible, y también queremos dejarle espacio para que ustedes puedan hacer preguntas.

Tenemos representado una aseguradora, está BANXICO, está también la Comisión, entonces yo creo que es un buen panel para hablar de este tema.

Déjenme que presento a los participantes. Aquí a mi izquierda está Silvia Villanueva. Ella es de AXA, es la Chef Segurity Office, y atiende a todos los nuevos mercados internacionales globales de AXA. A su lado Gerardo Rubio, él es el VP de Análisis y Estudios Sectoriales de la Comisión de Seguros y Fianzas, y finalmente Miguel Díaz, que es el Director de Sistemas de Pago de BANXICO.

Muchas gracias a todos. Bienvenidos.

Y me di a la tarea el día de ayer para introducir este panel a sacar unos datos de cómo está el mundo de la ciberseguridad en México y también lo primero que empecé a buscar es el mundo del cibercrimen.

Cuando nos ponemos a buscar estos datos, si alguno de ustedes los ha buscado van a ver que es difícil encontrar unos datos que coincidan unas fuentes y otras, pero más o menos yo lo que he sacado es que aproximadamente el costo del cibercrimen en México está entre los siete, nueve mil millones de dólares en el último año, en 2018, y dependiendo de unas fuentes u otras viene creciendo a ritmos del 30, 50, 60 por ciento. A esa velocidad crece el cibercrimen.

Ahora, yo les preguntaría a ustedes ¿los presupuestos que dedican sus organizaciones a ciberseguridad están creciendo a ritmos del 30, 60 por ciento? La verdad que yo no lo estoy percibiendo así, puede ser que alguna que venga muy chiquito sí esté duplicándose.

En Europa el crecimiento que está teniendo a nivel mundial, perdón, el cibercrimen, es en torno al 10, 15 por ciento, para que se hagan una idea.

Desafortunadamente este es un país donde estamos con unas tasas altas en ciberdelincuencia.

Y todo está muy vinculado también lo que les decía el mundo desde el punto de vista de la inversión que se hace en ciberseguridad, y les doy dos datos más. En Europa también es cierto que se ha desarrollado mucho el mundo del icomerse, esto no es para el Sector Asegurador en general, en las compañeras. Mundo Icomes, mundo digital.

El 23 por ciento de los presupuestos de las áreas de AT&T se van a ciberseguridad, 23 por ciento. En México, 5, y estamos en un mundo donde está creciendo muchísimo, es uno de los temas que quiero aquí de alguna forma también hablar con mis colegas de cómo se está implicando toda la parte de ciber seguridad con el crecimiento de nuevos negocios digitales.

Pero quédense con ese dato, 23 versus el 5. Yo creo que nos falta mucho.

Y un dato que saqué de la OEA, el impacto que estamos teniendo en Latinoamérica, en Ibitda, creo que casi todos trabajamos en base a este criterio, desde el punto de vista de ciber crímenes del 1.52 por ciento que nos está impactando.

Hacemos numerosos esfuerzos para mejorar nuestro Ibitda y al final, por ataques podemos estar perdiendo parte de él.

¿Qué retos veo o qué retos vemos desde el punto de vista de cómo ir mejorando? Pues sinceramente veo dos: uno, que seguramente muchos de ustedes lo están padeciendo y es que tenemos un déficit de talento de gente dentro del mundo de la ciber seguridad.

Nosotros en nuestra organización tenemos academias, tenemos un equipo que está creciendo, pero es un reto encontrar mucho talento. Y desafortunadamente en negocios como esto, pues muchas veces hay gente buena o buenos que están con los malos.

Entonces, cómo hacer atractivo para todo este crecimiento de este sector de la ciber y crear ese talento es uno de los retos que tenemos.

Y otro es invertirle más. Cada vez vemos más organizaciones y las aseguradoras están viendo ese camino, y algunos de ustedes estarán ahí, en el mundo allá, todo es allá, y vamos a desarrollar más, pues igual que las compañías se están metiendo o desarrollando nuevas apps, que si un chatweb por aquí.

Es raro ver dentro de las células, gente de ciber. Entonces, parece que estos se quedan como aislados, y se está metiendo muy poco la ciber seguridad, dentro del mundo del bussines.

Entonces, yo creo que esos retos de invertir más y más talento, pues son cosas que nos faltan, desde mi punto de vista para seguir desarrollando.

Bueno, pues tras esta pequeña reflexión, me gustaría y ya que está aquí Gerardo, de la Comisión, desde el punto de vista cuál sería tu análisis del estatus, dentro del sector de seguros y fianzas, como dirías está el mundo de la ciber.

Gerardo Rubio: Claro, con mucho gusto.

Muchas gracias por la invitación, muchas gracias a todos los presentes.

Voy a empezar excusándome, yo no soy un experto en ciber seguridad, a diferencia de mis compañeros, pero sí estoy mucho en la parte de desarrollo de estudios. Entonces, algo nos toca entender de este tema.

Como primera reflexión y es un poco nada más recapitular lo que hemos estado viendo hoy en el día en algunas de las presentaciones, el sector seguros, el sector financiero en general, es un sector altamente susceptible de temas de riesgos de ciber seguridad, y a lo mejor aquí

es tratar incluso de generalizar un poco, hablar de todo lo que es el concepto de seguridad de la información, son muy susceptibles desde el punto de vista de la cantidad de información que tienen, de lo redituable que puede ser, pensemos un ataque o de lo desastroso que puede ser simplemente una mala planeación de la seguridad de la información.

Se señalan y hay, obviamente, muchos estudios y demás, pero lo que se empieza a ver es que el 90 o más del 90 por ciento de las compañías, por ejemplo, reciben ataques o recibieron el año pasado al menos un ataque. Hay grupos que nos mencionan que reciben ataques todos los días de una gran variedad de órdenes e incluso, de ya una encuesta que hacían a más de dos mil CEOs, gente de riesgos, gente de información, en la cual ellos manifestaban como sensación de los futuros riesgos, ponían los primeros dos riesgos cuestiones naturales, envejecimiento, pandemias, etcétera, pero ya el tercer y cuarto riesgo estaban relacionados con cuestiones de ataques cibernéticos y demás.

Entonces, claramente empieza a ser un tema de preocupación, a pesar de que, creo que es un tema que tiene más de 10 años en el lenguaje común, para poder hablar del estado de que percibo yo que existe hoy, la verdad es que tendría que haber un marco regulatorio completamente definido u obligado para que yo les pudiera decir, pues el 100 por ciento lo están cumpliendo o el 90 lo están cumpliendo.

La realidad es que la regulación actual no es que, no es que no lo contemple, si ustedes revisan perfectamente, define que uno de los riesgos que hay que considerar es el riesgo tecnológico, que esto tiene que ser como parte del Sistema General de Administración de Riesgos, digo, yo lo he dicho en muchos lados, aquí se los reitero, me parece que ese sistema tiene una finalidad importantísima en la definición de la institución, tiene que definirse desde los lugares o desde la alta dirección, desde el Consejo, tiene que ser una cosa que venga desde arriba.

Y, por lo tanto, pues yo les podría aquí curarme en salud y decirles: “ahí está señalado que tienen que ver cómo hacer su estrategia de riesgo tecnológico”.

Están todas las cuestiones de contratación de terceros, claramente buscando que exista la continuidad que, digamos, se cumplan todos los protocolos para que aquellos contratos de terceros realmente no generaran un riesgo.

Sin embargo, lo que les puedo decir es que, si bien está esa cuestión en la que yo podría encontrar elementos en la regulación que obligaría o que esperaría que hoy las instituciones tuvieran un marco claro de gestión del riesgo de seguridad de la información, la verdad es que a nivel internacional y un poco por todo lo que se ha venido escuchando, ha ido cobrando una importancia más grande, tanto que la AISS, la Asociación Internacional de Supervisores de Seguros, pues pudo dentro de su plan quinquenal pasado, uno de los temas importantes era la ciberseguridad. Es un tema que se va a seguir trabajando en los siguientes cinco años.

La OCDE genera todo el tiempo guías, recomendaciones y demás, el Consejo de Estabilidad Mexicano, uno de los temas más importantes que trabajó el año pasado es todo el tema de seguridad de la información.

Entonces, independiente de lo que hoy yo vea que puede estar o no en la regulación, claramente hay una preocupación cada vez más grande acerca de las responsabilidades o las definiciones que se tendrían que dar desde las esferas más altas y probablemente más adelante lo podamos platicar con un poquito más detalle, a lo mejor nada más para tratar de cerrar esta idea de qué es lo que veo hoy, lo único que podría yo decir que sí existe, en el cual están adheridos o al menos en principio todas las instituciones del sector, son las bases de coordinación, estas bases de coordinación que surgieron a partir de los ataques del Sistema de Pagos que ocurrió en el año pasado, que son bases que al menos sí cumplen ciertos principios muy racionales, la parte más importante es que participan, tanto las entidades, las autoridades, participan las asociaciones gremiales, participan las instituciones y participan incluso las autoridades como la Procuraduría.

Entonces, eso realmente hace que esas bases de coordinación para combatir el tema del ciber riesgo, pues estén la gente que deba de estar.

El siguiente tema que a lo mejor hoy o cuál sería hoy el estado o lo que sabríamos es que se generó este grupo de respuesta, este grupo de respuesta lo que hace es que recibe ante la ocurrencia de un incidente por parte de alguna institución recibe este señalamiento, evalúa si califica como tal y si sí es, lo contribuye o lo socializa con la idea de evitar alguna dispersión o de permitir que las prácticas de las demás vayan mejorando.

Y, finalmente, genera de alguna manera a las instituciones, les da el compromiso de generar también un grupo de gestión de esas respuestas.

Entonces, ¿cuál es el estado hoy real? Si el Consejo realmente tuvo una clarísima definición de la importancia de este riesgo, pues deberá estar como parte de todo su proceso de gestión.

Existen bases de colaboración donde lo que hoy tenemos son principios de comunicación.

Y lo único que sí hemos visto es que a la fecha realmente no tenemos muchos reportes de estos incidentes, lo que nos podría decir, a lo mejor confirmando cosas de las que se hablaban en la mañana, es que todavía el grueso de los ataques relacionados con temas cibernéticos, no se dan tanto en el país, sino probablemente más en Estados Unidos, ahí hay un tema que creo que el 90 por ciento de las primas que se emiten a nivel mundial relacionado con seguros para proteger la ciberseguridad se emiten en Estados Unidos, eso un poco nos dimensiona más o menos cómo están los niveles de conciencia, el 10 por ciento en el resto del mundo, entonces son un poco llamativos dónde están observando o dónde están dimensionando los riesgos.

Óscar Diez: Oye, Gerardo, y le iba a preguntar ahora a Miguel, que él como Director del Sistema de Pagos de Banxico y que ahora a partir hay un hito que para todos es clave en el SPEI, el evento del año pasado, ¿cómo has visto que han ido mejorando y en qué se ha tangibilizado desde el punto de vista de a partir de ahí con el G hito?

Miguel Díaz: Te cuento un poco las perspectivas y cómo fue evolucionando esto.

El Banco de México desde mediados de 2017 emite cierta regulación específica para los participantes del Spei, donde se establecen cuáles son los criterios mínimos de seguridad que deben cumplir los participantes en el sistema.

Entonces, esto se publica por ahí de julio, y se da un transitorio lo suficientemente largo para que las instituciones que participan en el sistema de pagos pudieran hacer estas modificaciones y cumplir para enero de 2018.

Estos ataques a las instituciones participantes en el sistema, porque es muy importante diferenciar entre un ataque al sistema de pagos centralizado en oposición a un ataque a los participantes del sistema. Digamos, este ataque se da en los participantes del sistema, como funciona el Spei es básicamente tenemos un núcleo centralizado de liquidación y los diferentes participantes desarrollan sus formas de conexión hacia este sistema.

Es en esos puntos de conexión en donde los hackers básicamente encontraron un punto de ataque exitoso.

Ahora, por qué mencioné un poquito el tema de que el Banco de México emitió regulación en 2017, porque después de hacer los análisis forenses de la situación que ocurrió por ahí de abril y mayo del año pasado nos dimos cuenta que si se hubieran cumplido a cabalidad todos los elementos regulatorios establecidos para los participantes del Spei, digamos los hackers hubieran tenido una situación más complicada para realizar los ataques. Es decir, no les puedo garantizar que no hubieran ocurrido, pero lo que sí les puedo garantizar es que hubiera sido mucho más complicado para los atacantes realizar esta situación.

Y esto un poco lo que nos ilumina mucho es un tema que tenemos muy problemático y que gracias a estos eventos significativos ha empezado a cambiar, que es la cultura de la ciberseguridad en el sector financiero.

Entonces, un poco lo que observamos nosotros es que hay como una percepción de a mí nunca me va a pasar, aunque le pase al de al lado a mí nunca me va a pasar.

Y lo que empezamos a ver es que, digamos, con este tipo de ataques, donde hay un contagio de una institución a otra y donde hay vectores de ataque que no son exactamente iguales, pero son parecidos, y las instituciones en el momento en el que reciben este tipo de ataques, la verdad es que se dan cuenta de esta falta de atención a cosas que se habían venido señalando ya de tiempo atrás por parte de las autoridades.

Entonces, creo que un elemento muy importante que nos hace falta en el país es ese cambio de cultura sobre la ciberseguridad. Derivado de los eventos de los participantes en el Spei sí hemos visto un poquito de cambio en la cultura, sobre todo a los niveles más altos. Entonces ya empezamos a ver que en consejos de administración se empieza a tocar, de vez en cuando algún tema de ciberseguridad que a los altos niveles directivos empiezan a platicar en algún momento de ciberseguridad posiblemente relacionado también con las discusiones internas en los foros financieros internacionales que se dan donde se toca muy a menudo el tema de ciberseguridad.

Sin embargo, es muy importante el ver que esta cultura de ciberseguridad permee en todos los niveles de las instituciones ¿por qué? Muchas veces los elementos de ciberseguridad no necesariamente están con nuestro equipo de TI, posiblemente están con un mail, con un fishing, con un tema muy sencillo que no necesariamente podemos corregir desde una perspectiva de herramientas de tecnologías de la información, sino con un tema de educación y de culturización de nuestros equipos.

Entonces, creo que el evento que sufrimos el año pasado, como sistema financiero, es un evento que puede generar un cambio de actitud hacia la ciber seguridad, y creo que tenemos que aprovecharlo.

Yo creo que hoy más que nunca, los consejos de administración y los altos directivos, están conscientes de que esto es una preocupación, de que es algo que viene creciendo, de que es algo que le tenemos que meter lana, porque al final del día, no se pierde nada más, no es un ataque de denegación de servicios, no son ataques que nos pueden sacar de actividad un par de horas, son ataques que tienen implicaciones financieras muy significativas.

Entonces, creo que estamos en un momento en el que podemos, digamos, poner nuestro granito de arena, empujar un poquito más, para que se hagan las inversiones, para que se tenga esta discusión y para que se tenga esta educación al interior de las entidades financieras.

Lo que hemos visto, un poquito respondiendo a la pregunta, es que sí hay un avance, sí hay consejos de administración que están aprobando presupuestos un poco mayores, quizá no los que se deberían de dar, pero yo creo que la tendencia es la correcta.

Yo creo que ahí nos toca a todos, desde la perspectiva de los conocedores de tecnologías de la información, y la gente que está perfectamente consciente que esto es un riesgo, no sólo tecnológico, sino financiero, de cómo podemos hacer para empujar las inversiones, cómo podemos hacer para empujar la cultura, y se empieza a ver, pese a que falta todavía un poco un camino significativo por recorrer.

Óscar Diez: Vamos a ver, en tu caso Silvia, que yo estoy de acuerdo con Miguel, que hay un tema cultural o de organización y en tu experiencia cuáles son las dificultades que tú te has encontrado desde el punto de vista de la organización, pues para vender y cómo las has podido vender internamente.

Y qué comparación establecerías entre México y otros países que también estás manejando.

Silvia Villanueva: Gracias por la pregunta y también quería darles las gracias por invitarme. La verdad es que para mí es un honor estar aquí con mis compañeros y con vosotros.

Yo creo que uno de los principales retos que tenemos en las organizaciones, y que yo creo que nuestros mayores comparten, es que defender es una labor mucho más difícil que atacar.

Decían los panelistas anteriores, que estaba escuchando con mucha atención, que evidentemente estas organizaciones trabajan dedicadas para encontrar una vulnerabilidad cuando nosotros trabajamos dedicados, para solucionar cien, miles, cientos de miles.

Otro de los temas importantes que yo creo que las aseguradoras tenemos como retos, es la digitalización, o sea, tenemos un negocio que data del siglo XIV y probablemente haya cambiado más en los últimos cinco años que los últimos siglos, con lo cual, pues es un reto que intentamos asumir, que intentamos afrontar y que, desde luego, para nosotros eso hace un día a día muy divertido.

Yo creo que la agilidad, la innovación.

Otro de los temas muy importantes que realmente hablamos dentro de las organizaciones aseguradoras y a nivel mundial, es una visión holística de seguridad.

Ahora, una de las cosas que comentaban mis compañeros, las amenazas están convergiendo, ya no son puramente amenazas ciber y esto es algo que requiere también un cambio de mentalidad y un cambio en la forma que nos aproximábamos a la seguridad.

Y yo creo que lo has mencionado muy bien antes y me han gustado muchísimo tus datos, para mí uno de los principales retos y uno de los principales trabajos que tenemos que hacer las organizaciones a nivel mundial es ayudar a paliar la carencia de profesionales de seguridad que tenemos.

Ahora mismo a nivel mundial hay más de un millón de profesionales de seguridad demandados por las organizaciones, con lo cual la verdad es que cuando tenemos el talento retenerlo, formarlo y hacer esa comunidad, creo que es algo clave y uno de los retos que tenemos cada una de las aseguradoras que estamos aquí sentados.

Óscar Diez: Oye, y hay veces que he vivido, Silvia, experiencias en esas donde me encuentro a responsables de una unidad de negocio, de un ramo con su visión del crecimiento, bien sea digital y la gente de ciber.

Entonces, si lo miras desde afuera te das cuenta que habitualmente veo que hablan dos lenguajes diferentes, uno está viendo cómo poner todas las trabas del mundo para que no se pueda hacer nada y el otro porque le tiene que poner trabas para poder vender.

Cuál es tu, diría, tu recomendación sería para que se entiendan cada vez más estas dos áreas, tanto del negocio del crecimiento, va a ser fundamental para todos, como la protección.

Silvia Villanueva: Yo voy a hablar por experiencia propia, nuestro presidente mundial dio una entrevista hace poco tiempo, quizás tres, cuatro semanas y habló de la ciberseguridad y de la seguridad con esa visión holística, como te digo, que creemos en AXA como una de nuestras prioridades y retos en AXA mundo, con lo cual yo creo que los profesionales de seguridad hemos hecho un esfuerzo para entender el lenguaje de los seguros, que no es fácil y los profesionales del negocio han hecho un esfuerzo por entender el lenguaje de ciberseguridad, con lo cual sinceramente yo percibo que al día de hoy tenemos un lenguaje bastante común, nos entendemos, sabemos que retos, porque incluso como individuos los vivimos día a día y yo creo que caminamos juntos, creo que hay mucha visión y todavía hay muchas percepciones, sobre todo cuando se acude a las ponencias, de que nuestros mayores no entienden el lenguaje de la ciberseguridad.

A mí me sorprende y es un mensaje que quiero trasladar lo bien que lo entienden, sobre todo las empresas de seguros, ¿por qué? Porque una empresa de seguros al final no deja de ser una empresa de riesgos, o sea, nosotros compramos, vendemos, transferimos riesgos, la ciberseguridad no es más que otro riesgo, con lo cual, para mí en el Minsait de nuestro *excom*, por supuesto es un lenguaje muy fácil de hablar y es un lenguaje que es fácil de transmitir.

Por supuesto, todavía yo coincido con Miguel y Gerardo que nos queda un gran camino por andar y desde luego, creo que es una ilusión de trabajar en este sector. No sé si lo comparten mis compañeros.

En esta línea, Gerardo, coincido contigo, decías la importancia de ese marco regulatorio, de actuación, los protocolos también de cómo serías capaz de tangibilizar o qué crees que podríamos estar midiendo dentro de un año, si nos juntásemos, para medir que realmente hemos ido progresando, al final esto es una progresión constante, pero para ti cuáles son los indicadores claves para decir: “vamos por buen camino dentro del mundo de los seguros”.

Gerardo Rubio: Lo primero y venir aquí representando al regulador, la verdad es que estoy seguro que este es un tema tan complejo; no logro yo identificar, creo más que el fraude, algún tema donde la aseguradora tenga algo que yo llame un adversario, algo que tenga una contraparte que la ataque con dolo, no identifico más que, insisto, fraude y los fraudes son de distintos niveles.

Entonces, al ser este un adversario, una contraparte, tiene la gran complejidad de que está en una adaptación constante, a diferencia, pensemos, de a lo mejor algún fenómeno natural, que si bien tiene una evolución, pues tiene una evolución llamémosle más estadística, entonces es una cosa como de una adaptación constante.

Entonces, ¿Qué creo que se tiene que hacer? La verdad es que lo primero que se tiene que hacer es que exista un genuino convencimiento de la institución y cuando hablo de la institución hablo desde, dijiste ese dato que me gustó mucho, la cantidad de recursos que se destina, eso me dice el nivel o la apreciación de riesgo que le ven a esto.

Si no existe un convencimiento real de un Consejo de Administración, de la importancia de gestionar su seguridad de la información, podemos hacer mucha regulación pero siento yo que va a pasar muchas, pueden volverse cuestiones cumplidas, pero realmente no asimiladas y es lo que yo a todo mundo le digo, eso en ese momento para mí se vuelve un costo regulatorio insuperable, pero siempre va a ser un costo, nunca es una adopción.

Dicho esto, lo que veo que tenemos que hacer, la Comisión está trabajando en ello y muy probablemente, más bien muy pronto vamos a buscar a las asociaciones para compartir esto. Sí es señalar cuestiones más específicas en la regulación, acerca de este tratamiento particular.

Como mencioné, a pesar de que existen cuestiones como de principios generales, lo que se ha observado a nivel mundial, dado la exponenciación en la exposición a este riesgo, cada vez hay más puntos de conexión a este riesgo y, por lo tanto, más riesgo, ha obligado a hacer menciones muy específicas.

Entonces, en realidad la idea va por ahí, es que para gestionar la seguridad de la información dado la ciberseguridad, pues primero a se haga a través desde una definición desde la alta esfera que involucren la totalidad a la institución, es decir, que sea una, como llaman *end to end*¸ de principio a fin.

Para que realmente desde, como dicen, los presupuestos, pero realmente la definición y la búsqueda de la institución vaya en fomentar esa protección.

Siguiente, y por lo que estoy escuchando es una dificultad, pues es traer a un experto en este tema, no es gestionarlo con gente que no es experta en este tema.

Entonces, por ejemplo, muchas de las cosas que se recomiendan es que es un experto en el tema, que tenga un alto nivel, es decir, que reporte directamente a la alta gerencia, que además sea independiente de las áreas de tecnología, que no sea juez y parte de este proceso.

Temas muy importantes, también que exista una trazabilidad de todas las operaciones, que se puedan rastrear, con la finalidad de poder encontrar vulnerabilidades, pero también de que en caso de que exista alguna violación poder encontrar responsables y generar soluciones.

Un proceso continuo de mejora, un proceso continuo de pruebas, de penetración, de análisis y demás. Cuestiones muy importantes obviamente, comunicaciones hacia el sector, hacia el regulador y demás. Un tema evidentemente de capacitación, capacitación en todos los niveles, un poco lo que decía Miguel, para que esto funcione tiene que estar perfectamente bien definido en todos los niveles de la institución.

Y a lo mejor aquí un poco lo que yo diría es que si este es un tema regulatorio, si bien esto puede ser una cuestión regulatoria cómo medirías, pues medirías observando que estas cosas se van cumpliendo, ese sería como el objetivo, observar que todo esté cumplido. Pero que a lo mejor desde el punto de vista de las instituciones individuales no lo vean como un costo regulatorio, sino que lo vean como un grado mínimo para que una institución opere en el mercado común, porque en realidad si bien una institución puede tener

algún percance y ser financieramente dañada, la verdad es que hay una cuestión comunitaria o de colectividad de todo el sector que lo que puede provocar es un tema más reputacional.

Entonces, es del interés desde mi perspectiva de todo el sector que no solo la institución por sí sola esté protegida, sino que el sector en realidad sea un sector confiable desde el punto de vista de protección de la información.

Óscar Díez: Miguel, tú que estás en el mundo de sistemas de pago, que yo creo que es uno de los mundos que más va, obviamente cada vez hay más transacciones, cada vez va a haber transacciones diferentes, va a ir cambiando, va a sr un mundo cambiante.

Y en general todas las instituciones hablan de multicanalidad. Bueno, se ha quedado corto ya eso, ya es omnicanalidad, es digital, es todos estamos con Wolet. Cada vez tenemos más puntos de contacto con los clientes más mundo digital.

¿Cuál sería tu recomendación desde la óptica de la ciberseguridad para entidades aseguradoras, bancos, para poder blindarnos en todo este esquema?

Miguel Díaz: Sí se vuelve un tema complicado al tener una evolución tecnológica exponencial y la estar tratando todos de ofrecer el mejor servicio a los clientes.

Muchas veces ponemos en la balanza esto que tú comentabas de una disyuntiva entre qué nivel de servicio voy a ofrecer y qué nivel de ciberseguridad tengo.

Pero algo que es bien importante, y tiene que ver con lo que decía al principio, y perdón que lo repita, pero es un tema de cómo fomentar la cultura de la ciberseguridad, es que no necesariamente tenemos que tener al cuate de ciberseguridad y al desarrollador sentados en la sala.

Es que nuestro desarrollador tiene que ser un experto en ciberseguridad a la vez que es un experto en ofrecer elementos de negocio.

Entonces, los desarrolladores tienen que tener una capacidad o tienen que tener una capacitación para introducir la ciberseguridad desde el principio, desde el desarrollo, desde el diseño, desde todo lo que hacemos tiene que tener esta perspectiva de ciberseguridad. Es decir, que esto no sea una fuerza externa que viene a presionar al desarrollador o que viene a presionar al de diseño.

Al final del día cuando lo ve uno desde una perspectiva de institución en su conjunto, pues digamos el tipo de negocio sí quiere vender más seguros, pero al final del día también debería ser responsable hasta cierto punto de si por ofrecer un servicio más sencillo tienes una vulnerabilidad, pues digamos eso también se tiene que introducir en los incentivos de la persona de negocio.

Entonces, es otra vez cómo le hacemos para que estos incentivos que desde una perspectiva la institución en su conjunto, están clarísimos, porque al final del día, sí quiero vender más seguros, sí quiero dar más servicios, pero no quiero que me ataquen y no quiero perder dinero.

Entonces, al final del día es cómo le hacemos para que el de negocio internalice el tema de ciber seguridad, cómo le hacemos para que desde que nace el producto sea un producto que tiene características específicas.

Entonces, yo creo que, digamos, un poco el cómo le hacemos, yo creo que es esto, y meter este tema de la ciber seguridad en la mente de todo el mundo.

Ahora, algo que preguntabas antes, y perdón que retome esa pregunta, de cómo puedo saber yo dónde estoy yo en un esquema de ciber seguridad, o si mi institución está lo suficientemente preparada, creo que hay cuatro preguntas que nos tenemos que hacer.

Primero, tengo algún esquema de alertamiento en tiempo real, es decir, tengo algún esquema donde alguien de mi institución esté verificando en el DIP web, a ver si hay elementos que me ponen preocupado, alguien de mi institución está revisando si tengo vulnerabilidades o si existen exploids en el DIP web a los que puedo estar susceptible.

Si nuestra respuesta es no, pues ahí tenemos un canal de trabajo que tenemos que hacer.

El segundo, detección. Tenemos a alguien que esté revisando nuestro sistema todo el tiempo, tenemos a una persona que esté dedicada a identificar los flujos de información que vienen desde y hacia nuestros servidores.

Si la respuesta es no, ahí hay otro canal de trabajo.

¿Tenemos bien definido un esquema de reacción ante un evento que pueda suceder? Es decir, sabemos exactamente quién tiene que hacer qué ante un evento de seguridad informática.

Si mañana le pegan a mi sistema o les pegan a mis servidores centrales sé qué es lo que voy a hacer, sé cómo voy a recuperar el modelo de negocio en tiempo real; tengo un plan de continuidad operativa diseñado para un evento de ciber seguridad.

Si la respuesta es no, ahí tenemos un tercer canal de trabajo.

Y finalmente, y porque no somos inmunes incluso haciendo todo lo anterior, no somos inmunes a un ataque que pueda deteriorar el servicio, que pueda generar una pérdida financiera, pero ante un evento, ante la realización de un evento, tenemos un protocolo de recuperación. Entonces, más que la reacción inmediata, cómo le vamos a hacer para recuperar nuestro modelo de negocio inicial.

Si logramos y decimos que sí a estas cuatro, la verdad es que tenemos un sistema ya relativamente robusto de ciber seguridad, pero lo que vimos en los eventos del año pasado es que no todas las instituciones tienen muy claro esto, pese a que, digamos, ahora se los cuento y la verdad es que suena como un tema muy razonable y muy sencillo.

Pero no todas las instituciones estamos preparados para tener estos cuatro elementos, digamos en marcha, en el momento adecuado.

Entonces, lo que sí es muy claro, es que el improvisar ante un evento de ciber seguridad, la verdad es que no da resultados muy positivos.

Y no sólo afecta a nuestros clientes, también afecta nuestro voto on line y, por lo tanto, creo que es bien importante, pegarle en estas cuatro dimensiones.

Óscar Diez: Oye, en esta línea que estás diciendo, que están muy bien esos indicadores o medidores, Silvia, tu experiencia desde el punto de vista, imagínate ya tienes por delante un proyecto no de transformación para meter un esquema de ciber seguridad y riesgos, y blindar la organización lo máximo posible.

¿Qué ha sido en tu experiencia lo que mejor te ha funcionado a la hora de priorizar las iniciativas? Porque al final supongo que cualquiera que se meta ahí le salen mil cosas, por dónde empiezo y cómo empiezo para que lo vaya haciendo y se note y la organización también perciba que esto, porque cuando tú te estás blindando, si no pasa nada es cuando la estás escogiendo, pero tiene ir notando todo esto.

¿Cuál ha sido?, ¿cómo priorizas tú los proyectos?

Silvia Villanueva: Bueno, como he dicho antes, las aseguradoras que estamos aquí somos empresas que conocemos los riesgos y para nosotros la seguridad tiene que seguir un enfoque de riesgos igualmente.

Evidentemente un programa de transformación de ciberseguridad, incluso un programa de ciberseguridad, como me estás preguntando, para un proyecto completo, es un proyecto complejo que hay que abordar desde todas las dimensiones.

Entonces, por supuesto, mi recomendación es, primero, hablar con el negocio, que esto parece una obviedad, pero muchas veces cuando en el pasado históricamente las organizaciones no entendían cuál era la finalidad del negocio, no éramos socios reales del mismo, con lo cual no éramos capaces de incorporar la seguridad desde el principio, que para mí es el clave, el negocio tiene que sentir que tú eres un folder más y que estás ahí.

Y luego tienes que hablar de seguridad en términos de criticidad, impacto, mitigación de riesgos y a partir de ahí puedes priorizar, puedes

priorizar tus iniciativas, tanto de una transformación general como en un proyecto concreto.

Después para nosotros la seguridad tiene que seguir una filosofía bastante completa de trabajo. Uno de los errores históricos mundiales de que tenían las organizaciones respecto a seguridad, es que intentábamos construir catedrales, planificar sus proyectos de seguridad hasta cinco, seis años vista, cuando la tecnología había cambiado tanto que cuando acabas los proyectos de seguridad realmente ya no protegían el inicio y la mentalidad que tenías en un primer momento.

Para mí dar realidad a la seguridad y hacerla simple, es uno de los retos que tenemos en el sector, si tú intentas hablar con un usuario y le dices que para acceder a su correo tiene que poner ocho factores de autenticación y además conectarse únicamente desde un punto completo y además hacer el fino puente que decimos en España para poder hacer seguridad.

Probablemente intente buscar cualquier alternativa para soslayar los controles. Yo creo que las cosas y los controles de seguridad deben ser realistas, deben ser efectivos, pero deben ser sencillos, además hay un tema muy clave cuando priorizas, cuando hacer un programa de transformación la seguridad tiene que ser por defecto, tú no puedes asumir que un desarrollador o que un usuario vaya a implementar seguridad por muy concienciado que esté, tienes que poner todos los mecanismos y todas las barreras posibles para que esto sea así.

De hecho, en seguridad siempre hablamos de varios conceptos que son como nuestros grandes principios, que son la defensa en profundidad. Es decir, un control puede fallar, pero tengo siete más que me están previniendo del ataque.

Óscar Díez: Oye, en esto que estabas hablando, que es indudable que tiene que encajar con el negocio, ¿Cómo juega lo canales, cómo juega el mundo de los agentes, los brókeres dentro de todo este engranaje?, al final es una cadena y las cadenas es donde.

Silvia Villanueva: Mira, perdonarme que lo trate así de simple, pero esta es la comparación que hago siempre con las aseguradoras y los bancos.

Típicamente, si tú ves la exposición de un banco, un banco tiene Unicommerce más o menos complejo, pero tiene uno y además luego usa un host tipo *rack F*¸ donde tiene establecido el 99,9 por ciento de sus controles; su administración de seguridad ha estado trabajando en el tiempo y han llegado una simplificación y unos controles de seguridad que le resultan efectivos.

Las aseguradoras partimos de una historia, como les decía, de hace muchos años, donde nuestros sistemas son complejos, son bastante heterogéneos y esto a la hora de aplicar seguridad nos implica un esfuerzo extra.

Entonces, este es uno de los grandes retos y grandes temas que tenemos en las aseguradoras, cuando más seamos capaces de homogenizar, cuando más somos capaces de simplificar, cuando más llevamos un camino concreto muy objetivo, o sea, con un objetivo claramente definido, más fácil es aplicar seguridad holística y ciberseguridad en este caso.

Óscar Díez: Bueno, creo que nos quedan cinco minutillos, entonces seguro que alguno de ustedes tiene alguna cuestión, pregunta, así que aprovechen.

¿Preguntas? Ahí al fondo.

Pregunta: Es para Gerardo. Desde el punto de vista del marco normativo y sobre todo teniendo en cuenta el modelo operacional de cualquier aseguradora, como tú lo sabes y lo hemos visto, yo vengo de bancos, me cuesta mucho trabajo saber en ocasiones cómo manejan o manejamos la información en la aseguradora versus banco.

¿A qué voy? De pronto tienes una fuerza de venta y esta fuerza de ventas vive fuera de la aseguradora, pero sin embargo tiene información de los asegurados. ¿Para qué? Para promover estos productos o servicios.

Entonces, es un poco preguntarte...

Gerardo Rubio: Perdón, te escuché la última parte.

Pregunta: Sí, que en este caso la fuerza de ventas, que son compañías, sociedades anónimas, tienen información de nuestros asegurados. ¿Por qué? Porque ellos al final del día tienen que hacer una labor de ventas.

Desde tu punto de vista, ¿qué otras cosas podemos hacer para que ellos también se concienticen y sepan qué clase de información tienen?, sobre todo porque tienen información restringida o altamente restringida, entonces ellos también deberían tener un espejo con los controles que se tienen de este lado; no sé si me explico.

Entonces, cómo poderles decir: ¿Sabes qué? Aquí ya hay vara y tienes tú que entregar evidencia de cómo está tu estado de salud.

Gerardo Rubio: Hoy, de hecho, esa es un de las cosas que ya se contemplan y, por otro lado, es uno de los temas que se están incluso discutiendo a nivel internacional, la contratación de servicios con terceros.

Hoy, otra vez, si tú piensas el marco normativo, tratando de resumir lo que dice contratación de servicios con terceros, es que el tercero es como tú, o sea, el tercero tiene que tener tus mismos controles, tiene que tener gobernanza, tiene que tener control interno, auditorías y demás; el tercero tiene que acceder a ser sujeto de supervisión de la Comisión, entonces en ese sentido te diría que de alguna forma lo que dice hoy la regulación es que tú debes de contratar con alguien un servicio que por algo tú decides no realizar, pero que ese alguien en realidad no tiene un detrimento en ninguna de las escalas en las que tú tienes que operar, calidad, responsabilidad y demás.

Entonces, hoy lo prevé, pero dicho esto otra vez, uno, por ejemplo, de las grandes cosas que se están preguntando es si, incluso, los contratos de terceros tendrían que auditarse, porque la verdad es que son sumamente complejo. O sea, ese tema que dices tú es sumamente complejo.

Ahora, por ejemplo, hay una discusión enorme con el tema de la nube. El tema de la nube genera una altísima concentración, ahí hay, yo lo voy a decir mal, porque son somos tres proveedores, nada más, o sea realmente fuertes de datos.

Entonces, incluso, se está hablando de hasta supervisar a los de la nube o que para obtener datos en la nube tengan que tener autorización, porque es de tal nivel la responsabilidad que está adquiriendo este tercero con respecto a la responsabilidad que trae la aseguradora hacia el asegurado que se vuelve un tema sumamente importante.

Entonces yo único que te diría es: o sea, hoy existe. Creo que lo importante como elección hacia una compañía es que esa compañía entienda que en esa contratación de tercero no es un as. O sea, lo está haciendo por una cuestión de optimización, pero nunca como una cuestión de deslinde de responsabilidades.

Óscar Díez: ¿Alguna otra pregunta?

Gerardo Rubio: ¿Me permitirías hacer una última reflexión?

Óscar Díez: Sí, venga, venga. Vamos.

Gerardo Rubio: Aquí estamos hablando de la aseguradora como el sujeto de riesgo. La aseguradora también es claramente el gestor en cualquier riesgo.

Si ustedes piensan que están todos los controles médicos, de autos, lo que ustedes quieran, cualquier riesgo, y la aseguradora en realidad es el último eslabón de esa cadena, es aquel que protege en caso de ocurrencia.

Lo que quería aquí un poco traer de reflexión es que identifico que puede haber dos tipos de formas en cómo las aseguradoras protejan la ciberseguridad de otros. Una clarísimamente es a través de seguros que están pensados un poquito más masivos, como el que te venden porque te dupliquen tu tarjeta, o el que te hagan algún fraude personal.

Pero también claramente están protegiendo de responsabilidad civil, de cuestiones muchísimo más complejas a grandes instituciones.

La reflexión que les quería hacer es que creo que este es también una gran oportunidad para que las aseguradoras tomen un papel mucho más activo no solamente como de un garante financiero, de un protector financiero sino en realidad de un asesor de riesgo.

Yo creo que una aseguradora no puede cubrir un riesgo tan complejo si no es capaz ella misma de gestionarlo, no lo puede dimensionar, no puede saber si realmente está aceptando un riesgo que le va a costar o que la va a quebrar o si están cobrando un riesgo que en realidad está bien gestionado.

Entonces, creo que este es un momento importante como que las aseguradoras piensen también en ese otro papel que las obliga a ellas mismas a hacer unos grandes gestores del riesgo, propio obviamente, pero que también los va a hacer asesores de riesgo al estar protegiendo a lo mejor a otras instituciones de este mismo tipo de tema.

Entonces, creo que es algo en lo cual se podría trabajar.

Óscar Díez: Sí, es lo que comentaba antes Silvia, que es un tema que encaja muy bien.

Ahora yo también quería hacer una reflexión. Comentabas tú antes, estoy de acuerdo que donde más impacta es el fraude, y creo que ahora puede ser así.

En breve el fraude serán peanuts, porque cuando tengamos la información de todos los clientes, cada vez tienen más información, tienen más cosas en la nube, los temas que tienen que ver desde el punto de vista reputacional, ya te da igual que te hayan robado un peso, que un millón o todo, va a tener muchísima más relevancia y el fraude va a pasar a un segundo término.

Yo creo que esto trasciende, es protegernos en todo. En cuanto más información, queremos tener mucha información de los clientes, y obviamente eso lo tenemos que tener muy blindado.

Bueno, yo creo que ya, no sé si tenemos el minuto de reflexión de Silvia y de Miguel.

Miguel Díaz: No quiero sonar repetitivo, pero al final del día esto es cómo metemos en el cerebro de cada uno de los que están y que tienen con nuestro negocio el tema de ciber seguridad, esto no es nada más de las áreas de TI, esto no es nada más de las áreas de control, esto tiene que ser de todos en la empresa.

Es decir, si tienen una idea esa es la idea que me gustaría que se quedara.

Silvia Villanueva: Simplemente para concluir, decirles que la ciber seguridad, es un bonito mundo, tenemos muchos retos por delante nuestro, lo sabemos.

Creo que el camino que llevamos andado, es muy positivo y la verdad es que a lo que los animo a todos es a formar parte de la protección, a formar parte de la solución, y a seguir avanzando para que todos creemos una comunidad, una sociedad, y un mundo mucho más seguro para nosotros, para nuestros clientes, para nuestras empresas y para nuestros gobiernos.

Creo que está en cada uno de nosotros ser parte del cambio.

Óscar Díez: Pues nada, muchas gracias a los panelistas, a la AMIS, por la invitación y obviamente a todos ustedes.

Muchas gracias.

- - -o0o- - -