Ciudad de México, 14 de mayo de 2019.

Versión estenográfica de la Sesión Especializada "Ciber riesgos en la transformación digital: de la amenaza a la oportunidad", en el marco de la 29 Convención de Aseguradores AMIS, llevada a cabo en el Salón Montejo 3, del Centro Citibanamex.

Moderador: En nombre de la Asociación Mexicana de Instituciones de Seguros y el Comité de Tecnologías de Información de la misma Asociación, les damos la más cordial bienvenida, es bueno verlos cada año, aquí en esta barra.

Daremos inicio y en este día, ahora las sesiones tienen una variante, en esta ocasión tendremos o compartiremos alguna de las sesiones directamente con el ramo de automóviles, por lo que tendremos dos participaciones o dos presentaciones, inicialmente de ciber seguridad.

Posteriormente tendremos un panel con la participación, tanto de la Comisión como BANXICO, y posteriormente se hará un poco del cambio, se abrirá la sala donde compartiremos otra serie de temas directamente con el ramo de automóviles.

Entonces, si les parece, voy a dar inicio, inicialmente con una presentación de Indra, en este caso nos acompaña Erick Moreno Sánchez.

Bienvenido, Erick.

Y como pequeño preámbulo, Erick es Director del Ciber Operation Center, de Minsait México, su experiencia incluye el diseño y definición de estrategias y productos de ciber seguridad, de ciber inteligencia, ciber defensa, así como implementaciones tecnológicas, diseño de arquitecturas de seguridad.

En los últimos años, se ha especializado en el diseño de la entrega de proyectos de ciber seguridad, contemplando nuevas amenazas, tecnologías en empresas nacionales y transnacionales.

Tiene experiencia en proyectos de análisis, de amenazas, gestión y respuesta de incidentes de seguridad, establecimiento de niveles de madurez y muchos temas más.

Cuenta con 15 años de experiencia, asesorando organizaciones en decisiones estratégicas, referente a seguridad, en múltiples industrias nacionales y transnacionales.

Le cedo la palabra a Erick.

Bienvenido.

Erick Moreno: Muchísimas gracias.

Muy buenas tardes a todos, agradezco mucho su presencia en esta sesión, en esta plática.

Vamos a hablar un poquito de los ciber riesgos, vamos a hablar del contexto que hoy en día aqueja a las instituciones de seguros, instituciones financieras, en sí al sector como tal y de cuáles son las tendencias de protección que estamos visualizando y a las cuales deberíamos de estar poniendo foco de atención.

Sin duda, los mecanismos de protección, deben de ir muy alineados y muy cambiantes acorde a las nuevas amenazas y a las amenazas cambiantes que también existen en el contexto, y esto pues obviamente va incrementándose conforme van ampliándose los canales de negocio que hoy en día tenemos.

Estamos viendo una situación de transformación digital, de omnicanalidad, o de apertura de nuevos canales de negocio; estamos frente a la presencia de nueva tecnología, tecnología en la nube, virtualización, temas de aplicativos móviles y todas estas nuevas tendencias tecnológicas implican nuevos riesgos, y es parte de lo que ahorita les voy a estar platicando.

Cómo enfrentar estos riesgos y cómo de estas amenazas, convertirlas en una oportunidad para nuestras organizaciones.

Hoy en día, sin duda, uno de los puntos importantes y de mayor relevancia que tienen las organizaciones, es el tema de los riesgos en términos de ciber seguridad.

Hemos visto en publicaciones recientes en medios de comunicación que, en instituciones de este sector, ciber seguridad está siendo ya el riesgo principal en términos de negocio y en algunas de las encuestas que se han realizado en el mercado, marca el 82 por ciento de los interesados en temas de estrategias de negocio, marcan que el riesgo de ciber seguridad es un riesgo de negocio y no un riesgo de TI.

Esto nos abre pautas hacia nuevos enfoques a que visualice el negocio que seguridad o ciber seguridad es un habilitador propio del negocio.

Sin embargo, de ese público que fue encuestado en este estudio, el 73 por ciento de los encuestados mencionan también que es muy difícil alinear negocio con seguridad.

Si hoy en día alinear negocio con TI es un reto bastante importante, sin duda, meterle la variable de ciberseguridad es un reto dos veces más grandes y bien, cómo hacer partícipe al negocio de los retos o de los riesgos a los cuales nos estamos enfrentando, siempre justificando con temas de negocio, las pérdidas transaccionales que pudiéramos estar teniendo, temas de fraude que pudiéramos estar teniendo también en las organizaciones si no implementamos los controles de seguridad adecuados con un enfoque de riesgos.

Y bien, a pesar de esta implementación de controles y podemos hablar de controles tecnológicos, podemos hablar de controles a nivel normativos, de políticas, de marcos regulatorios, podemos establecer toda una estrategia de gestión de riegos y aun así las organizaciones hoy día están siendo víctimas de incidentes de ciberseguridad.

¿Qué quiere decir esto? Que nuestra estrategia per se está siendo mal diseñado mal enfocada, ¿por qué? Porque no estamos protegiendo lo que comúnmente o digamos que banalmente nosotros decimos, la joya de la corona; es decir, desde un inicio aspectos totalmente fundamentales como identificar cuáles son nuestros activos críticos de información y con ello implementar los controles adecuados de seguridad de la información es de vital importancia, no todo lo tenemos

que proteger de la misma manera y lo vemos en casos del día a día de nuestra vida.

Sin duda, ustedes pueden ver en sus vidas propias que la cerradura quizá de la puerta que tienen de su casa no es la misma cerradura o el mismo nivel de seguridad que tienen quizá en sus habitaciones o en la habitación de sus niños o quizá tienen alguna caja fuerte dentro de su hogar y ese control de seguridad es todavía más fuerte que los otros controles de seguridad.

De igual forma, debemos de identificar los riesgos a los cuales está expuesta nuestra organización para poder identificar los controles adecuados y que las estrategias de costo-beneficio obviamente vayan acorde a los niveles de protección y ¿qué es lo que debemos de visualizar hoy en día en nuestras estrategias de ciberseguridad? Ya no nada más temas normativos, temas de definición de políticas, tema de definición de procedimientos y procesos totalmente establecidos.

Hoy día estamos viendo que las organizaciones deben de prepararse para poder ser resilientes ante un incidente de ciberseguridad. Sabemos que sí o sí vamos a ser víctimas de un incidente, ¿por qué? Porque los delincuentes están continuamente cambiando sus formas de ataque, porque no podemos anticiparnos a estas nuevas formas, a estas nuevas técnicas, porque nuestro negocio se está abriendo a nuevos canales de negocio, ¿qué es lo que debemos de hacer entonces? Garantizar o tratar de minimizar los impactos del negocio para poder recuperarnos de manera mucho más rápida y con el menor impacto hacia el negocio, evitar las pérdidas o la fuga de información, recuperar la operación de nuestro negocio en el menor tiempo posible y dar la certidumbre hacia nuestros clientes o usuarios finales de que somos una empresa totalmente responsable en la salvaguarda y en la protección de los datos sensibles de nuestros usuarios finales.

Es un punto muy importante y las tendencias hoy en día de protección y de ataque no están siendo ya hacia temas transaccionales, están siendo hacia el robo de información de nuestros clientes.

Si vemos, en el último año hay cifras engañosas con respecto a la disminución del número de incidentes que se presentan en la industria, dicen que 2018 ha disminuido el número de incidentes frente a 2017,

pero si vemos, si es una cifra engañosa, si vemos el número de datos que se han robado en el último año se va a duplicar versus los ataques que se hicieron en 2017.

Entonces, los ataques que hoy en día estamos siendo víctimas están siendo mucho más dirigidos, totalmente enfocados hacia nuestras organizaciones y no nos estamos dando cuenta d que estamos siendo atacados.

¿Por qué no nos estamos dando cuenta que estamos dando que estamos siendo atacados? Porque nuestros controles de seguridad no están puestos en lugar y en la forma adecuada, lo que les decía.

Nuevamente, hay que proteger la joya de la corona, hay que implementar controles que nos ayuden a recuperarnos en el menor tiempo posible.

Un punto importante es que no se tiene identificado esta joya de la corona, tenemos dependencia tecnológica 100 por ciento en nuestra estrategia de ciberseguridad, sin tomar en consideración aspectos importantes o relevantes del negocio.

Y estamos siendo muy tardíos o muy reactivos en la respuesta ante un incidente de ciberseguridad.

Más adelante verán algunas de las cifras que pongo y es impresionante la brecha de tiempo en términos de cuánto le lleva a un ciber atacante poder comprometer parte de nuestra infraestructura en términos de minuto versus cuánto nos lleva a nosotros como organizaciones poder visualizar o poder contener ese ataque.

Hemos visto en hechos recientes que a veces los atacantes se quedan uno, dos años, o quizá hasta más tiempo, no tenemos identificado cuánto tiempo se quedan en nuestra organización visualizando, monitoreando todos los flujos de información y a partir de ahí entonces determinan y estudian todos nuestros procesos de negocio para finalmente hacer toda una ex filtración de información y vemos casos en donde se han robado millones de registros y lo cual nos impacta en temas de multas, por temas de privacidad, temas de impacto reputacional frente a nuestros clientes y eso, obviamente, tiene un

impacto económico mucho más fuerte que el implementar controles preventivos en términos de seguridad.

¿Hacia dónde tenemos que focalizar? A incrementar nuestras capacidades de respuesta y detección con un enfoque de riesgos. Ese es el punto clave para la definición de una estrategia de ciberseguridad.

Alguno de los clientes en los cuales estamos atendiendo nos dicen: “Oye, hoy día estoy ampliando mis fronteras de protección. ¿Cómo le hago frente a estos nuevos retos?”, si antes tenía, por decir un número, mil equipos que proteger en mi red perimetral, hoy día estoy abriendo que esos equipos tengan trabajo en casa, que puedan estar en otras localidades, que no estén metidos en una política institucional de monitoreo, que las políticas de protección están solamente en mi corporativo, pero qué hago cuando esos equipos salen fuera de mi corporativo.

Para eso existen nuevas tendencias y nuevos mecanismos y controles tecnológicos para poder proteger todas esas nuevas fronteras a las cuales estamos enfrentándonos, y son tecnologías, como lo dice ahí, de detección y respuesta ante un incidente de ciberseguridad, en donde ampliamos el set de políticas que tenemos en términos de nuestro corporativo hacia ambientes no controlados, como puede ser un café internet, como puede ser quizá un hotel, un aeropuerto o localidades fuera del corporativo que tenemos hoy en día.

Y estas son las cifras o el *slide* que les tenía preparado. El 87 por ciento de las organizaciones les toma solamente minutos poder ser víctima de un ataque de ciberseguridad. Es decir, las capacidades que tienen hoy día los atacantes son mucho más potentes que nuestras capacidades de protección.

Y, ¿cuánto nos lleva a nosotros como organización poder detectarlo? Nos puede llevar hasta meses poder detectar este ataque.

¿Cómo se le llama a esta nueva tendencia, ya no tan nueva tendencia, de hecho, a este tema de ataques? Son ataques persistentes avanzados, en donde no nos cuenta que el atacante está estudiándonos internamente, para posteriormente materializar el riesgo cómo opera.

Puede ser un robo de información, puede ser un tema de transaccionalidad, un tema de fraude, independientemente del fin último el punto importante es cuánto tiempo se queda en nuestra organización.

¿Y por qué no podemos visualizarlo? Porque no tenemos las capacidades de monitoreo, porque no tenemos las capacidades de poder detectar comportamientos anómalos.

¿Cuáles son los dominios críticos para gestionar el riesgo digital, según el enfoque que hoy día tenemos en Minsait? El primer punto es gestión de riesgos. Una estrategia de ciberseguridad, una definición de un plan director de ciberseguridad debe de estar focalizado en riesgos.

Debemos de hacer un tratamiento de estos riesgos desde la identificación, el poder visualizar cuál va a ser su tratamiento y posteriormente la monitorización de este mismo riesgo, tenemos que tomarlo muy en cuenta para la definición de un plan director de ciberseguridad, de una estrategia de ciberseguridad.

Estas herramientas nos van ayudar a poder medir y poder cuantificar cuáles son los impactos que vamos a tener hacia la organización, y de qué tamaño van a ser los controles tecnológicos que vamos a implementar.

Con esto focalizamos los esfuerzos en lo que realmente debemos de proteger.

El segundo punto importante son las operaciones de seguridad, y por qué marco este tema como importante, porque debemos de estar monitoreando, debemos de tener las capacidades de respuesta y las capacidades de detección que tanto ahorita les he estado hablando.

¿Cómo hacer este control de operaciones de seguridad? Hoy las tendencias están apuntando a tercerizar este tipo de servicios, desarrollar una capacidad de respuesta de incidentes dentro de las organizaciones nos va a costar mucho trabajo.

Son años de experiencia que deben de tener los analistas, son meses para poder implementar correctamente un control tecnológico y con lo

cambiante que hoy día están las amenazas tenemos que estar desarrollando continuamente estas capacidades.

Por eso una de las tendencias principales es el cómo responder o estas capacidades de respuesta de incidentes tercerizarlo hacia un tercero.

Y el tercer punto importante en ambientes tecnológicos. Hoy día muchos de ustedes en sus organizaciones están contemplando subirse a la nube, o hay quienes ya tienen tecnología en la nube o hay quienes ya están utilizando tecnología en la nube híbrida, quizá con ambientes virtualizados de Big Data en donde el manejo de la información, obviamente es mucho más grande.

Aquí el punto fundamental es tener esta gestión de la identidad y del control de acceso, validar que las organizaciones, que validar que los usuarios tengan acceso solamente a la información que le corresponde tener.

¿Qué vamos a hacer con esto? vamos a minimizar la superficie de ataque ante la pérdida o ante la pérdida de información o la divulgación de información confidencial.

¿Cómo podemos hacer esto? Con controles tecnológicos que nos ayuden a gestionar este control de acceso, a gestionar estas identidades ¿por qué? Porque al final del día la seguridad perimetral va a estar a cargo de estos proveedores de la nube o de Big Data. Estamos cubiertos en temas tecnológicos, en temas perimetrales y hoy día debemos de focalizarnos en los permisos que tienen los usuarios hacia ciertas aplicaciones.

A partir de ahí se pueden elevar privilegios, nosotros hacemos algunos ejercicios de pruebas de seguridad, en donde a través de un usuario común y corriente, podemos elevar los privilegios de acceso a la información y podemos tener acceso a información que no corresponda a nuestras actividades diarias.

Entonces, éste es el tercer punto en donde nosotros debemos de poner un foco de atención.

¿Quién o qué tiene acceso a qué? Y guardar las pistas o la trazabilidad de hacia dónde se tuvo acceso.

Muchas veces nos hablan para decir: “Sabes qué, necesito que me apoyes, Erick en un tema de un análisis forense”, ¿por qué? Porque ya tuve un incidente de ciber seguridad.

Necesito que me traigas a tu equipo de respuesta de incidentes, o tu equipo de emergencia, para que me validen dónde estuvo la falla y sin ningún problema podemos llegar y cumplir con los niveles de servicio.

Sin embargo, en la mayor parte de las ocasiones, nos topamos con la misma problemática, llegamos y no hay trazabilidad de los hechos, no sabemos quién tuvo acceso a qué, de qué forma y mediante qué medios y es un punto fundamental.

Y aquí debemos de poner un punto medio, quizá también contra los requerimientos de negocio, porque muchas veces nos dicen: “Sabes qué, es que definir esas pistas de trazabilidad, definir esos blogs, hacer el almacenamiento de esta información, muchas veces le pega al performance de mi tecnología o muchas veces va en contra de la usabilidad, vuelve lentos los sistemas, y necesitamos darle atención pronta a ese cliente.

Y es aquí en donde nuevamente debemos de definir un punto medio. ¿Para qué? Para validar si realmente podemos tener ese apetito de riesgo y decir, aceptamos el riesgo de vivir sin unos logs, pero no vamos a poder dar trazabilidad a un incidente de ciber seguridad, o es importante o es mucho más importante dar atención a temas de incidentes de ciber seguridad, porque quizá la protección de la marca, porque quizá la información de nuestros clientes es altamente sensible, y no queremos enfrentarnos a una situación de este tipo.

Es ahí en donde viene mucho del filling de cada uno de ustedes, conocer el negocio, ver qué es lo que están protegiendo o qué es lo que se quiere proteger, para entonces determinar estos controles de seguridad.

Sin duda, los ataques se han estado incrementando en las últimas fechas, en los últimos años, y también hemos incrementado nuestras

medidas de control o de seguridad, pero muy seguramente no vamos acorde a ese incremento en términos de ataques.

Tenemos que hacer, de cierta forma y a veces lo digo a los clientes, magia con lo que tenemos, y es por eso que debemos de identificar, como primer punto, la gestión de riesgos.

A continuación, les voy a presentar un freimborg general de ciber seguridad que muchos de ustedes lo tienen en algunos de los flayers que tomaron en la entrada, y es una visión, digamos, que hoy en día de protección que se puede tener en las organizaciones.

Un punto importante y para Minsait y la joya de la corona es el Cyber Defense Center, que es las capacidades de respuesta de incidentes.

Debemos de asegurar que las organizaciones sean resilientes per sé ante la presencia de un incidente.

La organización debería de estar contemplando controles de seguridad para la parte de detección, para la parte de prevención, de respuesta y para la parte de protección ante un incidente de ciber seguridad.

Una de las tendencias de protección que hoy en día tienen las organizaciones, son los llamados weba o las soluciones basadas en comportamientos anómalos.

Sin duda, es una tendencia muy fuerte, que nos ayuda a incrementar la postura de seguridad que tenemos frente a las amenazas.

¿Cuál es el diferenciador versus otras tecnologías? Que aquí vamos a estar basados en comportamientos, es decir, no vamos a basar un incidente de seguridad en las reglas o en reglas previamente definidas.

¿Qué ventajas nos va a dar? Que los ataques nuevos no nos lo va a detectar un componente de tecnología basado en firmas en donde se actualizó, quizá, 24 horas antes, en donde quizá un ataque de día cero no va a estar actualizada en nuestros componentes basado en firmas.

Esta nueva tendencia de protección basada en comportamientos nos va a ayudar mucho a prevenir fraudes, nos va a ayudar mucho a prevenir

accesos no controlados o accesos indebidos de información y nos va a ayudar a tener una postura lo más madura en términos de seguridad.

Otro de los puntos importantes a considerar, sin dudas, son los dos habilitadores que marco ahí de nuestro ciber defencenter que es el tema del *red ten* y el tema *blue ten*.

Como decía, hoy debemos de desarrollar capacidades de respuesta a incidentes con nuestro blue ten, mi equipo de acción inmediata, ese equipo va a ser mi *swap*, por así decirlo, es el que voy a llamar cuando ya se presentó algún incidente de ciberseguridad y me va a ayudar a recuperarme en el menor tiempo posible.

Y el *red ten* lo que nos va a ayudar es a validar de manera preventiva todos aquellos controles de seguridad que tenga puesto en mi infraestructura, que tenga puesta en mi organización.

Es decir, tratar de anticiparme ante posibles escenarios de riego de un posible ataque, ante posibles escenarios de riesgo de una fuga de información.

Y existen controles complementarios que nosotros estamos visualizando aquí en términos, si ven, en la parte de arriba términos o controles que van asociados hacia el aseguramiento de los sistemas o nuestras aplicaciones desarrolladas en casa, un tema muy importante, contemplar seguridad desde el diseño de las aplicaciones, aquí contemplar metodologías y el punto de desarrollo seguro para no gastar nuevamente temas presupuestales en remediación de vulnerabilidades y temas de protección, temas o controles de protección que nos van a ayudar a incrementar hoy día la seguridad en las fronteras que tenemos identificadas.

Hoy día estamos también viendo el incremento en temas de aplicaciones móviles, cómo a través de estas aplicaciones móviles estamos haciendo nuevos negocios y tenemos que proteger a estas aplicaciones, sellarlas, blindarlas de usuarios malintencionados con el objetivo, pues obviamente, de prevenir algún posible fraude.

Finalmente, como tema principal y les digo, todos estos controles que pudiéramos estar teniendo en lugar o poniendo en algún lugar de

nuestra infraestructura, no tendría ningún sentido sin una estrategia, sin un plan directo de ciberseguridad y a veces soy muy repetitivo en este tipo de pláticas que damos, si no tenemos la estrategia no vamos a saber a dónde ir, una estrategia que contemple al negocio 100 por ciento, que ciberseguridad sea un habilitador de este negocio y que enfrentemos a los riesgos de la forma adecuada cuantificando las medidas de control que debemos de tener.

Es parte de la visión que hoy día estamos teniendo dentro de Minsait para las medidas de control, sin duda, se van a presentar amenazas, como pueden malware, como pueden ser ataques de *fishing*, como pueden ser ataques dirigidos totalmente o persistentes. Sería incontable la cantidad de ataques a las cuales podemos ser víctimas, no podemos protegerlos a cada uno de manera específica, necesitamos tener una estrategia de ciberseguridad que vaya acorde a un plan de negocio y de crecimiento hacia este tema.

Es parte de lo que hoy día estamos visualizando, uno de los puntos también importantes para ustedes es el tema de los ciberseguros y lo estamos viendo como una oportunidad para ustedes que puedan tener este tema de negocio importante y que ustedes puedan tener un habilitador o un *parner* tecnológico que les ayude a entregar. Eso es lo lógico para poder garantizar la continuidad de las operaciones de sus clientes, es una de las tendencias que hoy día se están marcando en este rubro, que, sin duda, temas geográficos, con Europa, principalmente en Londres, en Estados Unidos, están mucho más avanzados con respecto a este tema de cultura en temas de ciberseguros.

Y prácticamente es de lo que quería platicarles en esta pequeña charla, darles una pequeña visión de más allá de las tendencias de protección, más allá de las amenazas que pudiéramos estar teniendo, donde debemos de poder foco, es en nuestra estrategia de ciberseguridad.

No sé si tengan algún comentario. Quisiera igual, si alguien tiene alguna duda, algún comentario, dos comentarios igual, para hacer un poquito dinámica esta plática, y con gusto las resolveremos.

Moderador: Tenemos dos minutitos para preguntas, no sé si por ahí hay alguna.

Erik Moreno: Perfecto. Agradezco mucho estos minutos de esta pequeña charla, el objetivo era darles este pequeño *overview* y espero haya cumplido con las expectativas que tenían de la plática.

Cualquier cosa estoy aquí para servirles, con gusto podemos platicar más en corto de algunas dudas que pudieran tener y estoy a sus órdenes.

Muchísimas gracias.

Moderador: Muchas gracias Erik, en nombre de la Asociación te entregamos un pequeño reconocimiento por tu participación.

Erik Moreno: Muchísimas gracias.

Moderador: Si nos dan un minutito continuamos con la siguiente ponencia, ahora es interesante porque ahora vamos a ver un poquito del otro lado de lo que ya es una compañía asociada en la práctica, precisamente, de ciberseguridad.

Si nos dan dos minutos continuamos con el programa.

----- oo0oo -----