IAIS 25 YEARS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

a2ii 10 years
access to insurance initiative

Riesgo Cibernético en el Sector de Seguros

Informe sobre la Llamada de Consulta de la A2ii y la IAIS

SEP
2019

Las Llamadas de Consulta son organizadas conjuntamente por la Iniciativa de Acceso a los Seguros (A2ii) y la Asociación Internacional de Supervisores de Seguros (IAIS) para proporcionar a los supervisores una plataforma de intercambio de experiencias y lecciones aprendidas en la ampliación del acceso a los seguros.

Introducción

Las amenazas a la ciberseguridad están aumentando en todo el mundo, y existe una preocupación creciente sobre el impacto de los incidentes de ciberseguridad sobre el sector financiero como un todo, incluido el sector de los seguros. El Documento Temático de la IAIS sobre el Riesgo Cibernético para el Sector de Seguros (IAIS, 2016)[1] afirmó que "El riesgo cibernético presenta un reto creciente para el sector de seguros y uno que, según los Principios Básicos, los supervisores están obligados a abordar. Los aseguradores recopilan, almacenan y administran volúmenes sustanciales de información confidencial tanto personal como comercial. Al tener estos depósitos de datos, los aseguradores son los principales blancos de los ciberdelincuentes que buscan información que pueda ser utilizada más tarde para obtener ganancias financieras a través de la extorsión, el robo de identidad u otras actividades criminales. Además, dado que los aseguradores son importantes contribuyentes al sector financiero global, cualquier interrupción provocada por incidentes de ciberseguridad en sus sistemas pueden tener repercusiones de gran alcance."

En esta Llamada de Consulta las contribuciones de los expertos fueron preparadas y presentadas por Marcelo Ramella (vicedirector del Departamento de Estabilidad Financiera de la Autoridad Monetaria de las Bermudas[2]) en la llamada en español y la segunda llamada en inglés. Andrea Camargo (directora de Inspowering y Experta Técnica en la A2ii) presentó las aportaciones de los expertos en la primera llamada en inglés y la llamada en francés. Glory Kasasi (Principal Examinadora, ICT – Departamento de Supervisión de Pensiones y Seguros, Banco de la Reserva de Malawi[3]), Jennifer McAdam (Senior Counsel - Asociación Nacional de Comisionados de Seguros[4], EE. UU.) y Marcelo Adrián Borré (Coordinador de Evaluación Normativa, Superintendencia de Seguros de la Nación (SSN), Argentina) compartieron las experiencias de sus jurisdicciones.

1 Disponible en: https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

2 Bermuda Monetary Authority (BMA)

3 Reserve Bank of Malawi (RBM)

4 National Association of Insurance Commissioners (NAIC)

Definiciones

Los ataques cibernéticos son intentos, exitosos o no, por acceder a información, o sistemas de información sin autorización con el fin de robar o alterar la información o bloquear sistemas de información. **El riesgo cibernético** es la combinación de la probabilidad de que ocurra un ataque cibernético, con todos los daños que puede haber causado un ataque cibernético[5]. **Ciberseguridad**, por otra parte, "se refiere a las estrategias, políticas y estándares que abarcan toda la gama de reducción de las amenazas y la vulnerabilidad, así como la disuasión, el compromiso internacional, la respuesta a incidentes, la resiliencia y las actividades de recuperación y las políticas relativas a la seguridad de las operaciones realizadas por los aseguradores."[6]

Los ataques cibernéticos pueden causar una vasta gama de daños, que van desde la interrupción de los servicios y negocios, hasta la destrucción de datos y propiedades, el robo de datos, etc. y, en ciertos casos, la posibilidad de causar inestabilidad financiera. Los ataques cibernéticos pueden generar considerables perjuicios económicos (en 2018 se estimó que el costo global de los ataques cibernéticos ascendió a USD 800 mil millones[7]). Comparativamente hablando, el sector financiero ha recibido más ataques que otros sectores económicos.

5 FSB (2018) Cyber Lexicon. Disponible en https://www.fsb.org/wp-content/uploads/P121118-1.pdf

6 IAIS (2018) Application Paper on Supervision of Insurer Cybersecurity. Disponible en: https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

7 McAfee (2018) Economic Impact of Cybercrime. Disponible en: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Los ataques cibernéticos y el sector financiero

El sector financiero es particularmente vulnerable a los ataques cibernéticos porque, entre otras motivos, las empresas tienen en su poder valiosos datos personales de los consumidores y activos financieros. El informe sobre "El costo de la actividad cibernética maliciosa para la economía de los Estados Unidos[8]" destaca los eventos cibernéticos y su distribución en diversos sectores de la industria en los EE.UU. Entre otros sectores como la salud y la educación, en 2016 el sector financiero informó el mayor número de incumplimientos en el sector financiero, correspondientes a su contribución al Producto Interno Bruto (PIB) (pp. 19 – 20 Consejo de Asesores Económicos, 2018)

El Documento Temático de la IAIS sobre el Riesgo Cibernético para el Sector de Seguros (IAIS, 2016)[9] declara que "el sector de seguros enfrenta riesgos cibernéticos provenientes tanto de fuentes internas como externas, e inclusive a través de terceros. Los aseguradores recopilan, procesan y almacenan volúmenes sustanciales de datos, que también incluyen información de identificación personal. Los aseguradores están conectados con otras instituciones financieras a través de múltiples canales, que incluyen actividades de inversión, recaudación de capital y emisión de deuda. Los aseguradores ejecutan fusiones y adquisiciones y otros cambios en la estructura corporativa que pueden afectar la ciberseguridad. Los aseguradores subcontratan una variedad de servicios, que pueden aumentar, o en algunos casos disminuir, la exposición al riesgo cibernético." El documento temático destacó algunas de las consecuencias que resultan de los incidentes de ciberseguridad que ocurren en el sector de seguros. Estos incluyen:

- Pérdida de datos confidenciales – Los aseguradores son un blanco muy importante para los delincuentes debido a la información de identificación personal que recopilan.
- Interrupción del negocio – Los ataques cibernéticos pueden interrumpir las operaciones comerciales normales y requieren altos costos de recuperación.
- Daño reputacional – La confianza de los asegurados puede verse comprometida si ocurre un ataque cibernético que exponga la información confidencial del asegurado. Los ciberataques plantean un riesgo reputacional que puede afectar al sector de seguros en general.

Compartimos ejemplos extraídos del informe "El costo del ciberdelito" [10] para mostrar cómo se pueden manifestar los tipos y costos de los ciber ataques en el sector de seguros:

- Los análisis realizados en 11 países mostraron que los sectores bancario y de seguros continúan teniendo uno de los costos anuales promedio más altos en comparación con otras industrias[11]. En 2017, los costos anuales promedio de los ciberataques en el sector de seguros fue de USD 12,93 millones y USD 15.76 millones en 2018 (pp. 12, Accenture, 2019).

8 Disponible en : https://info.publicintelligence.net/US-MaliciousCyberActivityCost.pdf

9 Disponible en: https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

10 Disponible en: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

11 En comparación con los seguros, las 5 principales industrias que, entre las 16 industrias comparadas en el informe continúan teniendo el costo más alto causado por el ciberdelito están: banca, los servicios públicos, software, automotriz e industrias de alta tecnología (ver Pág. 12, Accenture, 2019)

- En lo que respecta a los tipos de ataques que puede enfrentar la industria financiera como un todo, el malware, los ataques basados en la web y los ataques de rechazo de servicio son causales del mayor número de En comparación con los seguros, las 5 principales industrias que, entre las 16 industrias comparadas en el informe continúan teniendo el costo más alto causado por el ciberdelito están: banca, los servicios públicos, software, automotriz e industrias de alta tecnología (ver Pág. 12, Accenture, 2019) incidentes que contribuyen a provocar la pérdida de ingresos (pp. 17, Accenture, 2019).

Regulación y supervisión del riesgo cibernético

Esta sección se basa en el Documento de Aplicación de la IAIS sobre la Supervisión de la Ciberseguridad del Asegurador (2018).[12] Varias organizaciones internacionales, nacionales y de la industria, tanto del sector público como del privado han desarrollado marcos y directrices de ciberseguridad de gran relevancia para la supervisión del seguro. Una fuente clave de orientación que los supervisores pueden usar como referencia son los Elementos Fundamentales de Ciberseguridad para el Sector Financiero[13] (G7FE).[14] El G7FE es un conjunto conciso de principios de ciberseguridad no vinculantes para entidades públicas y privadas que operan en el sector financiero, cuyo objetivo es ser útil tanto a las empresas como a los supervisores. Los ocho elementos fundamentales identificados por el G7 son:

1. Estrategia y marco de ciberseguridad
2. Gobernanza
3. Evaluación y control del riesgo
4. Monitoreo
5. Respuesta
6. Recuperación
7. Intercambio de información
8. Aprendizaje continuo

Según el Documento de Aplicación, los ocho elementos se discuten en el contexto del seguro y se asignan a los PBS[15] relevantes. A seguir, consta un breve resumen de cada elemento, su respectivo PBS y ejemplos suministrados durante la Llamada:

12 Disponible en: https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

13 G7 Fundamental Elements of Cybersecurity for the Financial Sector

14 Disponible en: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

15 Todas las referencias a PBS específicos mencionados en esta sección se basan en la versión de noviembre de 2018, disponible en: https://www.iaisweb.org/page/supervisory-material/insurance-core-principles-and-com frame/file/87203/all-icps-adopted-in-november-2018

G7FE 1 – Estrategia y marco de ciberseguridad

Este elemento requiere que los aseguradores identifiquen, administren y reduzcan sus riesgos cibernéticos en una manera integrada y exhaustiva. Este elemento del G7FE se relaciona directamente con el PBS 8.1, que urge a los supervisores a requerir que las aseguradoras establezcan un sistema de gestión de riesgo efectivo y sistemas de control internos que funcionen dentro de este marco. Ejemplos de cuestiones a tener en cuenta incluyen:

1. ¿Existe una estrategia y marco claros de seguridad cibernética?
2. ¿La estrategia y el marco de ciberseguridad determinan los objetivos de la seguridad cibernética y tolerancia al riesgo del asegurador, así como también de qué forma pueden mitigar y administrar sus riesgos cibernéticos?
3. ¿Los riesgos cibernéticos está sujetos a revisión bajo el marco de ciberseguridad del asegurador? ¿Cuándo se realizó la última revisión?

G7FE 2 – Gobernanza

Este elemento requiere que las instituciones financieras definan los roles y responsabilidades del personal necesario para implementar, gestionar y supervisar la estrategia de ciberseguridad. Además, los aseguradores deben proporcionar los recursos necesarios para implementar la estrategia y marco de ciberseguridad. Este principio es consistente con el PBS 7, que requiere que los supervisores exijan que los aseguradores establezcan e implementen marcos de gobernanza corporativos que respalden la administración y supervisión estable y prudente de las actividades realizadas por los aseguradores, y que reconozcan y protejan adecuadamente los intereses de los asegurados. Ejemplos de cuestiones a tener en cuenta incluyen:

1. ¿La Junta y la alta gerencia del asegurador participan en los temas de seguri dad cibernética del asegurador? Por ejemplo, en el establecimiento de la estrategia del asegurador, supervisando su tolerancia al riesgo cibernético.
2. ¿Existen políticas y procedimientos claros? ¿Se aplican?
3. ¿Hay suficientes recursos para implementar las políticas?
4. ¿Cuál es el presupuesto de ciberseguridad?

G7FE 3 – Evaluación y control de los riesgos

Este elemento exige que los aseguradores identifiquen las funciones, actividades y servicios (incluyendo los servicios subcontratados) sujetos a riesgos cibernéticos. Los aseguradores deben entender y evaluar los riesgos e implementar los respectivos controles. Este elemento es consistente con el PBS 8, que requiere que los supervisores exijan que los aseguradores tengan "como parte de su marco general de gobernanza corporativa, sistemas efectivos de gestión de riesgos y controles internos". El PBS 19.12 requiere que los supervisores exijan que los aseguradores e intermediarios cuenten con políticas y procedimientos establecidos para la protección y uso de la información del consumidor. Ejemplos de cuestiones a tener en cuenta incluyen:

1. ¿Cuál es el nivel de conocimiento del asegurador sobre sus riesgos cibernéticos? ¿Existe un registro de riesgos cibernéticos? ¿Se utiliza y actualiza?
2. ¿El riesgo cibernético forma parte del perfil de riesgo general del asegurador?
3. Nivel de protección para la información del consumidor.

G7FE 4 – Monitoreo

Este elemento requiere que los aseguradores tengan sistemas de monitoreo que les permitan detector rápidamente ataques cibernéticos. Ellos deben evaluar constantemente la efectividad de sus controles para los riesgos cibernéticos, incluyendo las simulaciones de ataques cibernéticos. Este elemento es consistente con el PBS 8.1, que requiere que los supervisores exijan que los aseguradores establezcan sistemas efectivos de gestión de riesgos que incluyan sistemas de alerta temprana y respuesta a los riesgos. También es consistente con el PBS 8.2, que requiere que los aseguradores exijan que los supervisores tengan sistemas de monitoreo para realizar pruebas regulares de efectividad.
Ejemplos de cuestiones a tener en cuenta incluyen:

1. ¿Existen sistemas de monitoreo permanente de las actividades de alto riesgo (por ejemplo, acceso a información confidencial)? ¿El monitoreo se realiza en tiempo real?
2. ¿Qué es lo que se monitorea (por ejemplo, hardware y software en riesgo)?
3. ¿Hay evidencia de simulaciones realizadas por el asegurador?
4. ¿Para qué se han usado los resultados de las simulaciones?

G7FE 5 y 6 – Respuesta y recuperación

Estos elementos requieren que los aseguradores respondan a los ciberataques con prontitud, tomando en cuenta la gravedad del ataque, reduciendo sus efectos, emitiendo notificaciones apropiadas a quien corresponda, y coordinando e implementado respuestas que les permitan volver a operar normalmente. El PBS 8.12 establece los elementos necesarios que los aseguradores deben tomar en consideración para responder efectivamente a la materialización de los riesgos, y en proporción al riesgo materializado.
Ejemplos de consideraciones incluyen:

1. ¿Qué políticas y procedimientos tiene el asegurador para mejorar la conciencia sobre los riesgos cibernéticos (por ejemplo, programas de capacitación del personal centrados en riesgos cibernéticos)?
2. ¿Existen planes explícitos con descripciones detallas sobre cómo responder a los ataques?
3. ¿Existen planes explícitos que expliquen cómo volver a operar normalmente?
4. ¿Existen políticas y procedimientos sobre notificaciones sobre ciberataques?
5. ¿Qué investigaciones fueron implementadas por el asegurador después de un ataque cibernético?

G7FE 7 – Intercambio de información

Este elemento requiere que los aseguradores brinden información sobre amenazas, debilidades, ataques y respuestas a los ataques para mejorar las respuestas a los ataques, limitar los daños, aumentar la concientización y promover el aprendizaje interno. Los aseguradores deben suministrar esta información tanto interna como externamente, incluyendo notificaciones a las autoridades gubernamentales. El PBS 8.1.2, especialmente en lo que respecta a los requisitos de planificación de contingencias, se aplica a este elemento. Con respecto al intercambio de información técnica, el PBS 16 (Gestión de Riesgos Empresariales para Propósitos de Solvencia), estipula cómo establecer los requisitos de gestión de riesgos empresariales para fines de

solvencia, exigiendo que los aseguradores aborden todos los riesgos materiales y relevantes. El PBS 3, PBS 25 y PBS 26 abordan el tema del intercambio de información y la cooperación entre los supervisores, que incluye también la cooperación en la gestión de crisis internacionales. Ejemplos de consideraciones incluyen:

1. ¿El asegurador pertenece a grupos especializados que intercambian información sobre riesgos cibernéticos?
2. ¿El asegurador intercambia información con sus proveedores de servicios externos sobre el marco de ciberseguridad para promover la comprensión mutua del enfoque utilizado por cada uno para asegurar sistemas que están vinculados o interconectados?

G7FE 8 – Aprendizaje continuo

Este elemento requiere que los aseguradores mantengan sus sistemas de gestión de riesgos cibernéticos bajo constante revisión para garantizar que se mantienen al día con los riesgos cibernéticos, al mismo tiempo que los dotan con recursos adecuados. El PBS 16.10 requiere que los supervisores exijan que el sistema de gestión de riesgo de los aseguradores integre un sistema de retroalimentación basado en información apropiada, procesos de gestión y una evaluación objetiva que les permita tomar las medidas necesarias de manera oportuna, en respuesta a los cambios ocurridos en el perfil de riesgo del asegurador. Ejemplos de controles incluyen:

1. ¿Hay indicios de la existencia de circuitos de retroalimentación en los sistemas de gestión de riesgos cibernéticos de los aseguradores? Caso afirmativo, ¿hay evidencia de que estos circuitos funcionan de manera efectiva (por ejemplo, se están utilizando)?
2. ¿Con qué frecuencia se revisan / actualizan los sistemas de gestión de riesgos? ¿Cuán exhaustivas son esas revisiones?

ESTUDIO DE CASO: MALAWI

El estudio de caso de Malawi fue presentado por Glory Kasasi del Banco de la Reserva de Malawi

El RBM es el único regulador del sector financiero en Malawi, que incluye a los seguros. En gran medida, el RBM aplica un enfoque de supervisión basado en el riesgo. Hace cinco años se realizó una encuesta sobre el panorama de la tecnología de la información entre los aseguradores, que demostró un uso significativo de la tecnología de la información y comunicación (TIC), incluyendo el uso de sistemas de gestión de la información, servicios móviles y portales de clientes en línea. A nivel nacional, la regulación cibernética consiste en una Ley de Ciberseguridad de 2016 y una Estrategia Nacional de Ciberseguridad de 2018. El reconocimiento de la ciberseguridad a nivel nacional ha reforzado positivamente la labor del RBM para abordar los problemas relacionados a la ciberseguridad.

En 2011, el RBM emitió una directriz sobre la gestión de riesgos para los aseguradores. Esta directriz establece que los aseguradores deben contar con medidas de gobernanza, estrategias, marcos, políticas y procedimientos efectivos para la gestión de riesgos. Además, el RBM tiene pautas más prescriptivas para la gestión de riesgos que proporcionan orientaciones específicas a las instituciones financieras (bancos y administradores de pensiones), especialmente para fortalecer su gobernanza de TI, establecer una gestión de riesgos de tecnología robusta y sólida, y fortalecer la seguridad, confiabilidad, resiliencia y recuperación del sistema.

En lo que respecta a las herramientas de supervisión de las TIC, el RBM utiliza solicitudes de preexamen, cuestionarios que contienen preguntas sobre los controles esperados utilizados para la supervisión en el sitio, así como un cuestionario para empleados de TI y oficiales de riesgo que está bajo prueba piloto. Entre las debilidades y desafíos observados por el RBM en este mercado se incluyen:

- La falta de comprensión del riesgo cibernético por parte de algunos aseguradores
- Actualmente no existe una visión general sobre el panorama de amenazas cibernéticas para el sector de seguros
- El RBM no cuenta con una estructura de respuesta cibernética
- Ausencia de una orientación formal sobre cómo deben comunicarse los incidentes en las instituciones reguladas a otras divisiones potencialmente afectadas dentro del RBM u otras autoridades relevantes en Malawi

Tomando en cuenta los actuales y futuros desarrollos, la misión de la Asistencia Técnica (AT) bilateral del Fondo Monetario Internacional (FMI) sobre Supervisión de Riesgos de la Información y Seguridad Cibernética tiene actualmente en curso el desarrollo de un marco de supervisión para el riesgo cibernético. El RBM también está actualizando sus directrices de gestión de riesgos de TI para que los bancos incorporen temas relativos a riesgos cibernéticos. En 2020 se emitirán las directrices de Gestión de Riesgos de Seguridad Cibernética para los bancos y, a continuación, se adaptarán para que sean aplicables a todas las instituciones financieras supervisadas. El RBM también pretende formalizar un plan de gestión de crisis cibernéticas, realizando ejercicios de crisis y estableciendo un mecanismo de notificación de incidentes cibernéticos para las instituciones supervisadas.

Para hacer preguntas o solicitar más informaciones sobre actividades relevantes del RBM, por favor entre en contacto con: gkasasi@rbm.mw

ESTUDIO DE CASO: EE. UU.

El estudio de caso de los EE. UU. fue presentado por Jennifer McAdam de la Asociación Nacional de Comisionados de Seguros

La Ley Modelo de Seguridad de Datos se comenzó a redactar en 2016, y sus miembros la adoptaron en 2017. La Ley Modelo de Seguridad de Datos de Seguros (No.668) fue elaborada en respuesta a las principales violaciones de datos en las que se vieron involucrados grandes aseguradores. En 2015 se descubrió una violación masiva de datos en una de las mayores empresas aseguradoras de salud, Anthem, que se abordó mediante inspecciones multiestatales previo a la adopción de la Ley Modelo de Seguridad de Datos de Seguros. Para abordar la violación de datos de Anthem, los comisionados de seguros de todos los EE. UU. colaboraron entre sí y con las autoridades policiales realizando inspecciones multiestatales para evaluar el ataque cibernético a Anthem y proteger los datos de los consumidores. Las inspecciones supervisaron las acciones correctivas destinadas a reparar los sistemas de Anthem y prevenir futuros ataques cibernéticos. Las inspecciones multiestatales impulsados por la colaboración formaron un punto de partida para discutir qué tipo de legislación modelo pueden usar los reguladores para enfrentar una violación similar en el futuro.

La ley modelo es consistente con la regulación cibernética que el Departamento de Servicios Financieros de Nueva York (*NYDFS*[16]) tiene para las compañías de servicios financieros. La Ley Modelo de Seguridad de Datos se aplica a los aseguradores, agentes y entidades debidamente licenciadas o que el departamento de seguros debe autorizar. Esto incluye el establecimiento de estándares para: la seguridad de los datos, investigación de "eventos de ciberseguridad", y la notificación de "cualquier evento de ciberseguridad" al comisionado de seguros. La ley NYDFS se basa más en normas que la ley modelo de seguridad de datos, basada más bien en principios. Además, La Ley Modelo de Seguridad de Datos establece requisitos adicionales sobre la seguridad de los datos, y otorga más poder a los reguladores para hacer cumplir las recomendaciones que dan a los aseguradores, incluyendo las notificaciones al comisionado en el caso de ocurrir algún evento cibernético o una violación de datos.

El componente más significativo de la ley modelo es la Sección 4, que esboza los requisitos del Programa de Seguridad de la Información del licenciatario.

El licenciatario debe designar a alguien para que se haga cargo del Programa de Seguridad de la Información.

Los licenciatarios deben realizar una evaluación de riesgos para identificar las probables amenazas a la seguridad de sus datos y los sistemas en los que se almacenan.

- Los licenciatarios deben evaluar estas amenazas potenciales de manera continua, y el Programa, anualmente.
- Es necesario que los licenciatarios mitiguen los riesgos identificados según su tamaño y complejidad, entre otros factores de riesgo que constan bajo la disposición de gestión de riesgos.

16 New York Department of Financial Services

La ley modelo es escalable al tamaño, complejidad y alcance de las actividades del licenciatario que puede, consecuentemente, determinar qué medidas de seguridad deben tomarse con base a su evaluación del riesgo. No obstante, según la ley modelo, existen algunos requisitos que el licenciatario debe cumplir:

- **Supervisión de la Junta:** La gerencia ejecutiva debe informar anualmente a la Junta, por escrito, sobre el estado general y el cumplimiento de esta ley.
- **Proveedores de servicios externos:** El licenciatario también debe ejercer la diligencia debida al seleccionar proveedores de servicios externos, asegurándose de que estos proveedores también implementen medidas administrativas, técnicas y físicas para proteger y mantener seguros los sistemas de información.
- Otras obligaciones incluyen:
  - El titular de la licencia debe monitorear, evaluar y ajustar su Programa de Seguridad de la Información para que sea consistente con los cambios en la tecnología, así como con sus propios arreglos de negocios cambiantes.
  - El licenciatario debe establecer por escrito un plan de respuesta a incidentes para responder a eventos cibernéticos, que debe ser evaluado y revisado en caso de que ocurra un evento.
  - Los aseguradores necesitan presentar anualmente una declaración escrita, garantizando que el asegurador cumple con los requisitos estipulados en la Sección 4 de la ley modelo.

Además, los reguladores realizan inspecciones in situ para evaluar la situación financiera general de los aseguradores, que también incluyen la evaluación de sus marcos de TI y de riesgo cibernético. El Manual del Examinador sobre la Situación Financiera (Manual del Examinador), suministra la orientación utilizada por los reguladores estatales como parte del proceso de inspección financiera, e incluye una revisión sobre si la aseguradora realmente está abordando su riesgo cibernético y cómo lo está haciendo. El Manual del Examinador fue actualizado recientemente para incorporar el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (*NIST*[17]) y sus cinco funciones: identificar, proteger, detectar, responder y recuperar.

Desde agosto de 2019 a la fecha, la ley modelo de seguridad de datos se ha implementado y adoptado en ocho estados. Aunque la ley no se ha adoptado en todos los estados de los EE. UU., los comisionados de seguros continúan teniendo el poder de realizar inspecciones en las compañías y hacer recomendaciones para actualizar sus prácticas de ciberseguridad.

Para hacer preguntas u obtener más información sobre actividades relevantes, por favor entre en contacto con: JMcAdam@naic.org

17 National Institute of Standards and Technology

ESTUDIO DE CASO: ARGENTINA

El estudio de caso de Argentina fue presentado por Marcelo Borré de la Superintendencia de Seguros de la Nación (SSN), Argentina

Recientemente, la SSN lanzó una mesa de innovación en Seguros e Insurtech (Mesa de Innovación). Esta mesa reúne a diferentes actores del sector tecnológico y la industria de seguros para dialogar, con el propósito de promover la innovación en la industria del seguro. La Mesa de Innovación es un espacio de colaboración público-privado que busca crear un entorno para dialogar sobre el uso de la tecnología para el sector de seguros. La mesa busca:

- establecer un canal de comunicación que sensibilice sobre nuevos modelos de negocio y tecnologías relacionados a los seguros,
- identificar desafíos regulatorios relacionados con los riesgos y las oportunidades de las InsurTechs,
- contribuir para aumentar la competitividad del sector de seguros, y
- promover la eficiencia y competencia en la industria de seguros.

La SSN está preparando directrices internas para la operación de la Mesa de Innovación, que pueden modificarse de acuerdo con los cambios que ocurran en el espacio InsurTech. Con este objetivo, la SSN establecerá las medidas necesarias para proteger los intereses de los asegurados ante la adopción de nuevas tecnologías, y garantizará el correcto funcionamiento del mercado asegurador.

La SSN reconoce que la implementación de la Mesa de Innovación tiene una importancia clave, ya que reforzará el crecimiento de soluciones y tecnologías innovadoras para beneficiar al sector de seguros y a los asegurados. Asimismo, la Mesa de Innovación contribuirá al cumplimiento de los PBS, analizando los nuevos comportamientos de mercado resultantes de la emisión de la Resolución SSN No. 219/2018, que ha permitido la emisión de seguros en formato digital.

La Mesa de Innovación también tiene un componente relacionado al riesgo cibernético, formado por miembros de aseguradoras, proveedores de servicios (por ejemplo, Big Techs, empresas de software), empleados de la SSN, el Ministerio de Modernización y expertos y consultores sobre riesgo cibernético. Sus objetivos consisten en desarrollar buenas prácticas de gestión de riesgo y medidas para prevenir los delitos cibernéticos.

Para preguntas o más información sobre actividades importantes de la SSN, por favor entre en contacto con: mborre@ssn.gob.ar o mesadeinnovacion@ssn.gob.ar para más información sobre la Mesa de Innovación en Seguros e InsurTech

Preguntas y discusión

¿Cómo mantiene el equilibrio entre gestionar el riesgo cibernético y permitir la innovación financiera? Tanto los riesgos cibernéticos como los riesgos asociados a la innovación deben considerarse bien distintos y, a su vez, relacionados entre sí. Los aseguradores deben acceder y determinar su tolerancia al riesgo de las ciberamenazas y su apetito de riesgo por la innovación, y dejar bien claro en sus declaraciones de riesgo cuánto riesgo están preparados a asumir, y cómo pretenden administrarlos. En general, los supervisores suelen interesarse en conocer la solidez de la evaluación y gestión de riesgos de los aseguradores, y la transparencia y gobernanza del proceso de decidir cuánto riesgo puede asumir el asegurador y cómo administrarlo. En última instancia, los supervisores deberían estar interesados en saber en qué medida estos compromisos realmente se cumplen en la práctica.

¿Cómo se estructuran las inspecciones / examinadores TIC dentro de las autoridades? ¿Existen diferentes especialistas para diferentes áreas TIC? En el RBM, hay tres departamentos diferentes responsables por distintas áreas de supervisión. Cada departamento tiene expertos en TIC responsables por realizar inspecciones TIC en su área. En la Comisión de Servicios Financieros de Gibraltar, el Director de Información introdujo la supervisión de los controles de las TIC, que incluyen la ciberseguridad, la seguridad de los datos, los sistemas de control y gobernanza, la continuidad del negocio y la recuperación ante los desastres en todas las industrias. La Comisión de Servicios Financieros de Gibraltar ha estado realizando esta tarea durante más de cuatro años. Este modelo ha funcionado para la autoridad y ha formado parte de sus procesos in situ y de supervisión, además de ser una parte integral de su proceso de autorizaciones.

Are there any past cases of cyber attacks in the insurance sector and how existing frameworks have helped to combat them? In Malawi, the RBM has not been made aware of any specific cyber attacks whether within the insurance or banking industry. However, it is key to have a response mechanism to deal with such attacks. In the US, prior to the adoption of the Insurance Data Security Model Law, the Anthem data breach of 2015 was addressed through collaboration-driven multi-state examinations. State regulators collaborated with the Anthem companies, the Federal Bureau of Investigation, and cybersecurity firms to evaluate the attacks and issue corrective actions.

¿Ha habido casos de ataques cibernéticos en el pasado en el sector de seguros, y cómo los marcos existentes han ayudado a combatirlos? En Malawi, el RBM desconoce si ha existido algún ciberataque específico en el sector asegurador o bancario. No obstante, es imprescindible contar con un mecanismo de respuesta para lidiar con este tipo de ataques. En los EE. UU., antes de la adopción de la Ley Modelo de Seguridad de Datos de Seguros, la violación de datos de Anthem en 2015 fue abordada mediante inspecciones multiestatales, impulsadas por la colaboración. Los reguladores estatales colaboraron con las empresas de Anthem, la Oficina Federal de Investigación y las empresas de ciberseguridad para evaluar los ataques y emitir acciones correctivas.

Con respecto a las ciberamenazas interconectadas o transfronterizas, ¿cómo pueden establecer los supervisores requisitos de seguridad para la supervisión en la nube [18] para lidiar con datos provenientes de diferentes sectores y países al mismo tiempo? A menudo los servicios de tecnología digital, tales como la tecnología en la nube, se subcontratan. Como la mayoría de estos desarrollos digitales aún no están regulados en muchos países, los supervisores no pueden depender actualmente de mecanismos transfronterizos. No obstante, es importante que los aseguradores sepan que estos riesgos existen y tengan marcos de respuesta adecuados para gestionar los riesgos.

¿Cuántas notificaciones se han hecho a la NAIC con respecto a ciberataques, y cuáles son los principales motivos que retrasan la adopción de una ley modelo en los distintos estados? Los aseguradores no están obligados a notificar a la NAIC, sino más bien directamente a los comisionados. Actualmente, no se han recopilado datos para dar cuenta de cuántas notificaciones se emitieron con respecto a los ataques cibernéticos. El principal desafío para garantizar una adopción uniforme de la Ley Modelo de Seguridad en todos los estados de EE. UU. ha sido la oposición presentada por los representantes de la industria. Sin embargo, la ley se está adoptando paulatinamente en todos los estados.

¿Cómo pueden lograr los supervisores una supervisión eficaz del riesgo cibernético en casos donde no hay expertos de TIC en el seno de la autoridad supervisora? Hay varias posibilidades que los supervisores pueden adoptar o aplicar en este sentido. El supervisor puede contar con la ayuda de expertos externos cuando sea necesario, incluso cuando el supervisor no tiene expertos internos y/o no tiene la masa crítica o presupuesto necesario para asegurar la experiencia interna. Es importante resaltar que el supervisor debe poder evaluar la solidez de la gestión del riesgo cibernético de la propia empresa, independientemente del "conocimiento técnico" del riesgo cibernético. Una analogía es la supervisión de los modelos actuariales internos que utilizan los aseguradores, que es probable que los supervisores no sean capaces de entender técnicamente en su totalidad o de forma cabal. Por ejemplo, en Canadá, la Oficina de la Superintendencia de Instituciones Financieras, está elaborando una nota de orientación para la supervisión de modelos internos con el propósito de determinar los requisitos de capital reglamentario (ver enlace http://www.osfi-bsif.gc.ca/Eng/Docs/e25-dft.pdf). La lógica subyacente también se aplica al riesgo cibernético.

18 Para más información sobre computación en la nube ver el documento del Instituto de *Financial Stability Institute* "Regulating and supervising the clouds: emerging prudential approaches for insurance companies" disponible en: https://www.bis.org/fsi/publ/insights13.pdf. Este documento fue presentado en la Llamada de Consulta de la A2ii-IAIS del 28 de noviembre de 2019. El informe de la llamada está en preparación.

Socio de Implementación:

IAIS 25 YEARS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Auspiciado por:

cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

Ministry of Foreign Affairs of the Netherlands

Acogidos por:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Iniciativa de Acceso a los Seguros
Patrocinada por el Sector del Proyecto
de Sistemas Financieros de GIZ
Enfoques para los Seguros
Deutsche Gesellschaft für Internationale
Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany

Teléfono: +49 61 96 79-1362
Fax: +49 61 96 79-80 1362
E-mail: secretariat@a2ii.org
Internet: www.a2ii.org

a2ii_org

Promoviendo el acceso a los seguros responsables e inclusivos para todos.