This Spanish translation is prepared by the Superintendencia de Valores y Seguros de Chile (SVS). It is not an official IAIS translation. Please visit www.iaisweb.org for the official English version.

Esta traducción al español fue preparada por la Comisión Nacional de Seguros y Fianzas de México (CNSF). No es una traducción oficial de la IAIS. Por favor, visite www.iaisweb.org para obtener la versión oficial en inglés.

DOCUMENTO TEMÁTICO SOBRE RIESGO CIBERNÉTICO PARA EL SECTOR AASEGURADOR

Agosto de 2016

Acerca de la IAIS

La Asociación Internacional de Supervisores de Seguros (IAIS) es una organización de membresía voluntaria de los supervisores de seguros y reguladores de más de 200 jurisdicciones de casi 140 países. La misión de la IAIS es promover una supervisión eficaz y coherente a nivel mundial de la industria de seguros con el fin de desarrollar y mantener mercados de seguros justos, seguros y estables para el beneficio y protección de los asegurados y de contribuir a la estabilidad financiera mundial.

Establecida en 1994, la IAIS es el órgano responsable del establecimiento de normas internacionales para desarrollar los principios, normas y otros materiales de apoyo para la supervisión de la industria de los seguros y para la entrega de asistencia respecto de su aplicación. La IAIS también proporciona un foro para que los miembros puedan compartir sus experiencias y comprensión de supervisión de seguros y de los mercados de seguros. Además de la participación activa de sus miembros, En las diferentes actividades organizadas la IAIS se beneficia de los comentarios, de observadores representantes de instituciones internacionales, asociaciones profesionales y empresas de seguros y reaseguros, así como consultores y otros profesionales.

La IAIS coordina su trabajo con otros responsables de políticas financieras internacionales y asociaciones de supervisores o reguladores, y ayuda en la formación de los sistemas financieros a nivel mundial. En particular, la IAIS es miembro de la Junta de Estabilidad Financiera (FSB), miembro y co-creador del Fórum Conjunto, junto con el Comité de Supervisión Bancaria de Basilea (BCBS) y la Organización Internacional de Comisiones de Valores (IOSCO) fundador, miembro del Consejo Asesor de la Junta de Normas Internacionales de Contabilidad (IASB), y socio de la Iniciativa de Acceso a Seguros (A2ii). En reconocimiento a su experiencia colectiva, la IAIS también es consultada habitualmente por los líderes del G-20 y otros organismos internacionales de normalización para la asesoría en temas de seguros, así como en asuntos relacionados con la regulación y supervisión del sector financiero mundial.

Los documentos temáticos proporcionan antecedentes sobre temas particulares, describen las prácticas actuales, ejemplos reales o estudios de caso relacionados con un tema en particular y / o identifican los asuntos y retos relacionados con la regulación y el control. Los documentos temáticos son principalmente descriptivos y no tienen la intención de crear expectativas sobre cómo los supervisores deben implementar el material de supervisión. Frecuentemente los documentos temáticos forman parte del trabajo preparatorio para el desarrollo de normas y pueden contener recomendaciones para el trabajo futuro de la IAIS.

Este documento fue preparado por el Grupo de Trabajo sobre Delitos Financieros (FCTF).

Esta publicación está disponible en el sitio web de la IAIS (www.iaisweb.org).

Contenido

I. Introducción 3
II. El panorama del riesgo cibernético 4
III. Amenazas cibernéticas al sector seguros 8
IV. Ejemplos de incidentes de ciberseguridad en el sector de los seguros. 10
V. Resistencia de Ciber Seguros 12
VI. Aplicabilidad de los Principios Básicos de los Seguros a la Seguridad Cibernética 14
VII. Respuesta de Supervisión al Riesgo Cibernético 18
VIII. Conclusión 28
Anexo I Resúmen de las respuestas de la Encuesta de la IAIS 30
Anexo II Glosario de términos 33
Anexo III Lectura adicional 35

I. Introducción

1. La preocupación por la ciberseguridad está creciendo en todos los sectores de la economía mundial, a medida que los riesgos cibernéticos han aumentado y los ciberdelincuentes se han vuelto cada vez más sofisticados. Para los aseguradores, los incidentes de seguridad cibernética pueden perjudicar la capacidad para emprender negocios, comprometer la protección de datos comerciales y personales, así como socavar la confianza en el sector. La IAIS ha observado que el nivel de conciencia de las amenazas cibernéticas y la ciberseguridad en el sector de los seguros, así como los enfoques de supervisión para combatir los riesgos, parecen variar entre las jurisdicciones.

2. Estos factores llevaron a la IAIS a considerar la creación de un área encargada de la seguridad cibernética en el sector de seguros, incluyendo la participación de supervisores de seguros en la evaluación y promoción de la mitigación del riesgo cibernético.

3. Aunque muchos de los incidentes de seguridad cibernética más ampliamente divulgados que afectan la información sobre consumidores han afectado a los minoristas, las empresas del sector de los servicios financieros, incluidas las aseguradoras, también han sido víctimas.

4. Todas las aseguradoras, independientemente del tamaño, la complejidad o las líneas de negocio, recogen, almacenan y comparten con terceras partes diversas (por ejemplo, proveedores de servicios, intermediarios y reaseguradores) cantidades considerables de información privada y confidencial de los asegurados, especialmente información relacionada con la salud. La protección

de la confidencialidad, integridad y disponibilidad de los datos de los aseguradores es de importancia fundamental. La información obtenida fraudulentamente de los aseguradores, mediante el delito cibernético, puede utilizarse para obtener ganancias financieras mediante la extorsión, el robo de identidad, la apropiación indebida de la propiedad intelectual u otras actividades delictivas. La exposición inadvertida o intencional de datos privados puede resultar en un daño severo y persistente para los asegurados afectados, así como daños a la reputación de los participantes del sector asegurador. Del mismo modo, los ataques cibernéticos maliciosos contra los sistemas críticos de una aseguradora pueden afectar o impedir su capacidad para realizar negocios.

5. En 2015, la IAIS consultó a sus Miembros acerca de su percepción sobre el riesgo cibernético en la industria de los seguros, su participación como reguladores en la lucha contra las amenazas cibernéticas y los enfoques de supervisión de la ciberseguridad que están en uso o en desarrollo. Este documento recoge las respuestas de los miembros a dicha encuesta. El documento también se nutre de consultas con varios Miembros, aseguradores, profesionales de la seguridad cibernética y otros expertos, así como la literatura citada en este documento. En el Anexo III se presentan fuentes adicionales.

6. El objetivo de este Documento Temático es sensibilizar a los aseguradores y supervisores de los desafíos presentados por el riesgo cibernético, incluyendo los enfoques de supervisión actuales y previstos para abordar estos riesgos. Como Documento Temático, proporciona antecedentes, describe las prácticas actuales, identifica ejemplos y explora los asuntos y retos relacionados con la regulación y la supervisión. Este artículo se centra en el riesgo cibernético para el sector de los seguros y la mitigación de tales riesgos. No se abordan los riesgos de seguridad de Tecnologías de la información (TI) más ampliamente, el ciber seguro (los aseguradores venden o suscriben ese tipo de productos de seguros) o los riesgos derivados de incidentes de ciberseguridad que involucran supervisores, temas importantes pero que no están dentro del alcance de este documento.

7. El documento es principalmente descriptivo y no pretende crear expectativas de supervisión. No obstante, el documento puede arrojar luz sobre la necesidad de desarrollar material de la IAIS adicional y más específico para apoyar a los supervisores en el abordaje del riesgo cibernético.

II. El panorama del riesgo cibernético

8. No existe una definición estandarizada del término "riesgo cibernético". El Foro deRiesgo Cibernético ha descrito ampliamente "riesgo cibernético" como: "Cualquier riesgo que emane del uso de datos electrónicos y su transmisión, incluyendo herramientas tecnológicas como Internet y redes de telecomunicaciones. También abarca los daños físicos que pueden ser causados por incidentes de ciberseguridad, fraude cometido por mal uso de datos, cualquier responsabilidad derivada del almacenamiento de datos y la disponibilidad, integridad y confidencialidad de la información electrónica, ya sea relacionada con individuos, compañías o gobiernos ".[1] Un grupo de trabajo del Comité de Pagos e Infraestructuras de Mercado y de la Organización Internacional de

[1] CRO Forum, The Cyber Risk Challenge and the Role of Insurance, paragraph 3 (December 2014), available at http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/.

Comisiones de Valores ha descrito el riesgo cibernético como sigue: "La combinación de la probabilidad de que ocurra un evento dentro del ámbito de los activos de información, cómputo y comunicación; y las consecuencias de ese evento para una organización".[2]

9. Este documento usa varios términos para describir los resultados adversos derivados del riesgo cibernético. Estos incluyen "ataque cibernético", definido por el Consejo Federal de Examinación de Instituciones Financieras de los Estados Unidos (FFIEC) como: "intentos de dañar, interrumpir u obtener acceso no autorizado a una computadora, sistema informático o red de comunicaciones electrónicas. Un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por una empresa, con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura de computación; o destruir la integridad de los datos o robar información controlada ".[3] Por otra parte, un" incidente cibernético "es definido por la FFIEC como" acciones tomadas a través del uso de redes informáticas que producen un efecto real o potencialmente adverso en un sistema de información o La información que allí reside".[4]

10. En este documento, la frase "incidente de ciberseguridad" se utiliza generalmente para incluir tanto los ataques cibernéticos como los incidentes cibernéticos.

11. En su Informe Global de Riesgos 2015, el Foro Económico Mundial identificó los riesgos tecnológicos, en forma de fraude de datos, incidentes de ciberseguridad o desglose de la infraestructura, como uno de los diez principales riesgos a los que se enfrenta la economía global. Entre las aseguradoras encuestadas (y la primera entre las aseguradoras estadounidenses y británicas) en un informe de 2015 sobre las percepciones del sector sobre el riesgo[5].

12. La aseguradora Allianz ha identificado las siguientes tendencias en el panorama del riesgo cibernético: [6]

- Aumentar la interconectividad y la "comercialización" de la delincuencia cibernética, generando una mayor frecuencia y gravedad de los incidentes, incluyendo las infracciones de datos;
- La legislación sobre protección de datos se endurecerá a nivel mundial. En el futuro se pueden esperar más notificaciones y multas significativas por incumplimientos de datos;

[2] Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016), available at https://www.bis.org/cpmi/publ/d146.htm.

[3] FFIEC, Cybersecurity Assessment Tool Glossary (June 2015), available at http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf.

[4] World Economic Forum, Global Risks 2015 (2015), available at http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.

[5] PWC and Centre for the Study of Financial Innovation, Insurance Banana Skins 2015: The CSFI Survey of the Risks Facing Insurers, paragraph 1 (July 2015), available at http://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/55dde0fce4b0dff05004146c/1440604412304/2015+Insurance+Banana+Skins+FINAL.pdf.

[6] Allianz Global Corporate & Specialty, A Guide to Cyber Risk (September 2015).

- Los riesgos de interrupción de negocio (IN), robo de propiedad intelectual y extorsión cibernética están aumentando. Los costos de IN podrían ser iguales o superiores a las pérdidas por infracción; y
- La vulnerabilidad de los sistemas de control industrial representa una amenaza significativa.

13. En lo que respecta al contexto, el resto de esta sección del Documento Temático describe los datos publicados recientemente sobre los tipos, la frecuencia, la gravedad y los costos de los incidentes relacionados con la seguridad cibernética.

Tipos de incidentes de seguridad cibernética

14. Los incidentes de ciberseguridad ocurren de diversas maneras, ejemplificados por las distintas formas en que ocurren los incumplimientos de datos, que es el tipo de incidente de ciberseguridad más divulgado.[7] En un informe de 2015[8], Verizon concluyó que la mayoría de las violaciones de datos surgieron por una o más de las siguientes causas: intrusiones en el punto de venta; Crimeware (cualquier tipo de software que se utiliza para cometer un delito); Ciberespionaje;[9] abuso de información privilegiada; y ataques a aplicaciones en la web. El resto de los incidentes de seguridad cibernética se debieron a errores diversos, robo o pérdida física, robo de identidad de tarjetas de crédito o denegación de servicio distribuida. Estos incidentes de seguridad cibernética, aunque a menudo están vinculados a violaciones de datos, también pueden dar lugar a otras formas de pérdida (por ejemplo, robo de propiedad intelectual).

15. La extorsión cibernética, generalmente realizada a través de una forma de crimeware conocida como "ransomware", es un incidente cada vez más común de ciberseguridad en el cual los hackers se infiltran en ordenadores pertenecientes a una empresa o a un individuo, encriptan los datos y luego demandan un pago para descifrarlo. "[10] Ciertos tipos de ransomware son muy efectivos, y las víctimas de tales ataques no pueden recuperar datos sin pagar rescate, a menos que hayan hecho una copia de seguridad de los datos almacenados en medios no sujetos al ataque de ransomware.[11]

Frecuencia, gravedad y costo de los incidentes de ciberseguridad

16. La frecuencia de los incidentes de ciberseguridad está aumentando. En el otoño de 2014, la encuesta anual de seguridad de la información global de ejecutivos corporativos de PricewaterhouseCoopers (PwC), que incluyó a 9,700 participantes, informó que casi 43 millones de incidentes de ciberseguridad detectados ocurrieron durante el año anterior - el equivalente a 100,000 ataques por día y un aumento del 48 por ciento sobre el número de incidentes reportados

[7] Data breaches are “security violations in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so.” See, e.g., U.S. Department of Health and Human Services, Administration for Children and Families, Information Memorandum: ACYF-CB-IM-15-04 (1 July 2015), available at http://www.acf.hhs.gov/programs/cb/resource/im1504.
[8] Verizon, 2015 Data Breach Investigations Report, page 32 (2015).
[9] Cyber espionage is defined as: “Unauthorised spying by computer. The term generally refers to the deployment of viruses that clandestinely observe or destroy data in the computer systems of government agencies and large enterprises.” PC Magazine, “Encyclopedia,” available at http://www.pcmag.com/encyclopedia/term/64376/cyber-espionage.
[10] Devlin Barrett, “Paying Ransom to Hackers Stirs Debate,” Wall Street Journal (9 November 2015).
[11] Ibid.

en la encuesta de 2013.[12] El número de incidentes de seguridad cibernética reportados en la encuesta PwC de 2015 aumentó un 38 por ciento respecto del año anterior.[13] Además, el número de incidentes de ciberseguridad no reportados o no detectados es probablemente mucho mayor. Los ataques a través del malware son cada vez más frecuentes: [14] se ha informado que, en todas las organizaciones a nivel mundial, ocurren cinco ataques de malware cada segundo de cada día, aunque no todos logran su propósito.[15]

17. Los incidentes de ciberseguridad ocurren en empresas de todos los tamaños. Las pequeñas empresas, sin embargo, pueden ser particularmente vulnerables. En una encuesta de NetDiligence de 2015, por ejemplo, las empresas de menos de 50 millones de dólares en ingresos reportaron la mayoría de los incidentes (29 por ciento), seguidos de cerca por negocios con menos de 2.000 millones de dólares en ingresos (25 por ciento) [16].

18. Las filtraciones de datos son la forma de incidente de ciberseguridad más reportada, y su gravedad varía según la jurisdicción. Entre los países y organizaciones cubiertos por un informe del Ponemon Institute (Ponemon), el número promedio de registros perdidos o robados por incumplimiento de datos oscila entre aproximadamente 19,000 y casi 30,000, con la experiencia de promedios más altos en Estados Unidos, India y países de la región árabe.[17]

---

[12] PwC, Managing Cyber Risk in an Interconnected World: Key Finding from The Global State of Information Security Survey 2015, paragraph 7 (September 2014), available at http://www.pwccn.com/home/eng/rcs_info_security_2015.html.

[13] PwC, Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security Survey 2016, paragraph 2 (September 2015), available at http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

[14] "[El malware está diseñado para acceder secretamente a un sistema informático sin el consentimiento informado del propietario. La expresión es un término general (abreviación de software malicioso) que se utiliza para designar una variedad de formas de software o código de programa hostil, intrusivo o molesto. Malware incluye virus informáticos, gusanos, caballos de Troya, spyware, adware deshonesto, ransomware, crimeware, la mayoría de los rootkits y otros programas o programas maliciosos y no deseados. Tomado de FFIEC, Glosario de la Herramienta de Evaluación de la Seguridad Cibernética.

[15] El informe Verizon 2015, sobre costo de las filtraciones de datos señala que muchos de estos ataques de malware son detenidos por "controles como firewalls, sistemas de detección de intrusiones (IDS) / sistemas de prevención de intrusiones (IPS), filtros de spam, etc."
Verizon, 2015 Data Breach Investigations Report, page 21. The Verizon report notes that many of these malware attacks are stopped by “controls like firewalls, intrusion detection systems (IDS)/intrusion prevention systems (IPS), spam filters, etc.”

[16] Net Diligence, 2015 Cyber Claims Study, página 22 (2015).

[17] Ponemon Institute, 2015 Estudio del costo de la violación de datos: análisis global, página 8 (mayo de 2015). En el estudio participaron 350 empresas de los siguientes 11 países: Estados Unidos, Reino Unido, Alemania, Australia, Francia, Brasil, Japón, Italia, India, Emiratos Árabes Unidos, Arabia Saudita y Canadá. Las organizaciones participantes experimentaron filtraciones de datos que oscilaban entre un mínimo de aproximadamente 2.200 y un poco más de 101.000 registros comprometidos. Como se describe en la siguiente sección, el costo "por registro" de responder a las filtraciones de datos también varía según el país.

19. Los incidentes de seguridad cibernética también son costosos. El Centro de Estudios Estratégicos e Internacionales y McAfee, por ejemplo, ha estimado que el delito cibernético cuesta a la economía mundial más de 400,000 millones de dólares cada año.[18]

20. Recientemente, Lloyd's y el Centro de Estudios de Riesgos de la Universidad de Cambridge publicaron un informe analizando las pérdidas financieras asociadas con un hipotético ataque cibernético en la red eléctrica estadounidense. El informe prevé pérdidas totales de entre 243,000 millones de dólares y más de 1 billón de dólares, con pérdidas aseguradas de entre 21,400 y 71,100 millones de dólares, según la gravedad del corte de electricidad[19].

21. Ponemon ha llegado a la conclusión de que el costo medio global de una infracción de datos en 2014 fue de 3.79 millones de dólares, con un costo medio global de 154 dólares por cada registro perdido o robado. Estos costos varían geográficamente. Por ejemplo, el costo promedio por registro en los Estados Unidos fue de $ 217, mientras que en la India el costo fue $ 56 por registro. Los costos también varían según la industria, en firmas relacionadas con la salud ($ 363 / registro), firmas de educación ($ 300 / registro), firmas farmacéuticas ($ 220 / registro) y firmas financieras ($ 215 / registro) El costo promedio de la industria minorista por alteración ha aumentado dramáticamente año tras año, de $ 105 / registro en 2014 a $ 165 / registro en 2015.[20]

22. Según Ponemon, estos costos pueden considerarse comprendidos en una de cuatro categorías: (i) detección y escalada; ii) notificación; iii) respuesta ex post; Y (iv) pérdida de negocio. En 2013, 2014 y 2015, la pérdida de negocio -que incluye la rotación inesperada de clientes, las pérdidas de reputación y la disminución de la plusvalía- fue el componente de costo más grande asociado con las brechas de datos.[21]

III. Amenazas cibernéticas al sector seguros

23. En general, el sector de los seguros se enfrenta a un riesgo cibernético tanto por fuentes internas como externas, incluso a través de terceros. Las aseguradoras recogen, procesan y almacenan volúmenes sustanciales de datos, incluyendo información de identificación personal. Las aseguradoras están conectadas a otras instituciones financieras a través de múltiples canales, incluyendo inversiones, captación de capital y actividades de emisión de deuda. Las aseguradoras

[18] Centro de Estudios Estratégicos e Internacionales y McAfee, Pérdidas Netas: Estimación del Costo Global del Delito Cibernético (junio de 2014), disponible en http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[19] Lloyd's of London, Emerging Risk Report: Business Blackout – The Insurance Implications of a Cyber Attack on the U.S. Power Grid (July 2015), available at https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf. El informe (que asume que la Ley de Seguro de Riesgo de Terrorismo de los EE.UU. no se activaría) señala que las cifras de pérdidas aseguradas llevan incertidumbre de $ 5 mil millones o más debido a ambigüedades en torno a la cobertura y exclusiones bajo diversas líneas de negocio.

[20] Ponemon Institute, 2015 Costo del estudio de la brecha de datos: análisis global, páginas 1, 2 y 9 (mayo de 2015). Estos resultados se basan en una encuesta Ponemon de empresas que experimentan infracciones de menos de aproximadamente 100.000 registros.

[21] Ponemon Institute, 2015 Estudio del costo de la violación de datos: análisis global, párrafo 17 (mayo de 2015).

realizan fusiones y adquisiciones y otros cambios en la estructura corporativa que puedan afectar a la ciberseguridad. Los aseguradores externalizan una variedad de servicios, que pueden aumentar, o en algunos casos disminuir, la exposición al riesgo cibernético.

Ejemplos de debilidades de seguridad cibernética con aseguradoras recientemente observadas por los miembros de la IAIS

Falta o incompleta Visión general del paisaje informático

Aunque todos los aseguradores deben tener un inventario de hardware de TI y software con licencia, incluso aquellos que mantienen tales registros en una base actualizada pueden no tener identificado el flujo de datos entre esos sistemas de TI, aplicaciones y componentes. Si existen flujos de datos entre sistemas con altos niveles de protección y sistemas con niveles de seguridad más bajos, los ciberdelincuentes pueden tener acceso a sistemas, que de otro estarían seguros.

Proceso de control inadecuado en relación con los privilegios del usuario

Típicamente hay dos tipos de problemas asociados con la gestión de identidad de usuario: (1) el fallo de los controles dentro del proceso de asignación de derechos de usuario, es decir, permitiendo a los usuarios tener privilegios de sistema superiores a los garantizados; y (2) la falta de actualización cuando una cuenta deja de necesitar ciertos privilegios del sistema. Ambos tipos de fallas podrían conducir al abuso de información privilegiada y a la exposición a riesgos cibernéticos. Existen productos de software que pueden realizar verificaciones de gestión de identidad de forma automatizada.

Acceso incorrecto a cuentas de superusuario

El acceso directo de los empleados a las cuentas de "superusuario" (cuentas con niveles de privilegio muy superiores a los apropiados para la mayoría de los usuarios) sin que existan controles suficientes, presenta riesgos para las aseguradoras. En primer lugar, si un hacker obtuvo acceso a cualquiera de las cuentas de los empleados con privilegios de superusuario, el hacker podría controlar eficazmente todo el sistema a través de la cuenta del superusuario (incluyendo el ocultamiento de actos delictivos, modificando o eliminando archivos de registro o desactivando los mecanismos de detección). En segundo lugar, el uso común de cuentas de superusuario podría conducir a errores no deseados que afecten a todo el sistema.

24. Las consecuencias potencialmente adversas derivadas de los incidentes de ciberseguridad en el sector de los seguros, pueden incluir, por ejemplo: pérdida o corrupción de datos confidenciales de empresas, consumidores o terceros; Interrupción del negocio; pérdida física (por ejemplo, daño al hardware); perdidas financieras; y daños a la reputación. Algunos de ellos se destacan a continuación.

Pérdida de datos confidenciales

25. La información personalmente identificable recolectada y almacenada por los aseguradores, incluyendo información de salud personal de los asegurados y, en algunos casos, de terceros, puede

incluir nombres, fechas de nacimiento, números de seguridad social, direcciones de correo electrónico y de domiciulio, números de identificación social y datos de empleo. Los registros privados de salud pueden ser particularmente valiosos en los mercados negros, como herramientas para la extorsión, el fraude y el robo de identidad, lo que hace que los aseguradores que recopilan ese tipo de información representen objetivos de alto valor para los criminales.

26. Para los titulares de pólizas comerciales, las aseguradoras pueden recopilar información confidencial de negocios que podría ser valiosa para espías corporativos y extranjeros. En el caso de los productos de ciberseguridad, por ejemplo, los aseguradores pueden poseer información sobre los controles de seguridad de la red de un asegurado y otra información de resistencia cibernética que podría ser valiosa para hackers y otros ciberdelincuentes. Además, la pérdida de información confidencial podría perjudicar los derechos de propiedad intelectual de un asegurado.

Interrupción de los negocios

27. No todos los incidentes de seguridad cibernética incluyen infracciones de datos; algunos ataques cibernéticos pueden provocar interrupciones en las operaciones comerciales normales. El incidente de ciberseguridad de Sony Pictures, por ejemplo, habría destruido toda la red de la compañía, incluyendo correos electrónicos, directorios telefónicos, correo de voz y registros comerciales como plantillas de contrato.[22] Tal ataque malicioso contra una aseguradora podría resultar en un daño significativo a la empresa con sustanciales costos de recuperación.

Daño de Reputación

28. El negocio de seguros se basa en la confianza de los asegurados: confían en que la información recolectada por los aseguradores estará protegida y en que las reclamaciones se pagarán de manera oportuna. Si un asegurador sufre una violación de sus datos, por la que su información confidencial se expone, esa confianza puede ser sacudida. De manera similar, si un asegurador sufriera un incidente de ciberseguridad que le hiciera incapaz de hacer pagos puntuales de reclamaciones o que de otra manera interrumpiera sus operaciones, también se mina la confianza. El riesgo de reputación podría extenderse al sector de los seguros en su conjunto y afectar negativamente la confianza de los consumidores, asegurados, inversionistas, agencias calificadoras y socios comerciales.

IV. Ejemplos de incidentes de ciberseguridad en el sector de los seguros.

29. En los últimos años el sector de los seguros ha experimentado una variedad de incidentes de seguridad cibernética, incluyendo la afectación de datos en varias aseguradoras de salud estadounidenses. A continuación se ofrecen algunos ejemplos de estos incidentes de ciberseguridad.

[22] Amanda Hess, "Inside the Sony Hack," Slate (22 de noviembre de 2015), disponible en http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

30. En 2015, Anthem Blue Cross Blue Shield y Premera Blue Cross experimentaron filtraciones de datos, comprometiendo los relativos a tarjetas de crédito, la información de identificación personal, y datos de salud.[23] Las infracciones potencialmente expusieron la información personal de hasta 91 millones de asegurados, una cuarta parte de la población en los Estados Unidos.[24] Las aseguradoras tuvieron que reaccionar rápidamente para mitigar el daño a la reputación y minimizar los costos de los litigios, aunque actualmente se desconoce la cantidad de pérdidas en que los aseguradores incurrirán en última instancia debido a esta violación.

31. En otro ejemplo reciente, un servidor de datos operado por el estado de Dakota del Norte vio comprometida su seguridad, exponiendo potencialmente una variedad de información personal relacionada con los reclamantes de compensación de trabajadores - incluyendo 43,000 informes de incidentes y 13,000 informes de nómina que habían sido archivados en línea por trabajadores y empleadores. Según se supo, la información médica y los expedientes de reclamación no fueron expuestos, pero se dijo que los datos en riesgo incluían nombres de individuos, números de seguridad social, fechas de nacimiento, descripciones de lesiones, descripciones de incidentes, nombres y direcciones de empleadores.[25]

32. Un grupo de extorsionistas cibernéticos conocido como el "DD4BC" ha estado apuntando a una gama de empresas incluyendo instituciones financieras en Europa, Australia, Canadá y los Estados Unidos con amenazas de ataques de denegación de servicio (DDoS)[26] para solicitarles dinero. DD4BC ha exigido rescates de cantidades variables, que se pagarían en bitcoins (cripto-moneda), amenazando con lanzar ataques DDoS a menos que el objetivo pague el rescate en un plazo especificado. Dos grupos alemanes de seguros experimentaron este tipo de ataque a mediados de 2015, recibiendo amenazas de un ataque DDoS en los servidores web de la empresa, a menos que pagaran 40 bitcoins. Los aseguradores se negaron, ya que consideraron que los extorsionistas sólo habrían causado daños menores en esos casos, pero estos incidentes podrían haber sido mucho más graves si los ataques se hubieran concentrado en sistemas más críticos.

33. En 2015, las pruebas de penetración realizadas por el equipo de auditoría interna de una aseguradora en Francia encontraron que se había producido un acceso no autorizado a las herramientas de contabilidad. Aunque en este caso no hubo más consecuencias, este incidente de

[23] Anthem, Inc., Declaración relativa al ataque cibernético contra "Anthem", disponible en https://www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem; Premera Blue Cross, Premera Targeted by Cyberattack (17 marzo 2015), disponible en https://www.premera.com/wa/visitor/about-the-cyberattack/?WT.z_redirect=www.premera.com/cyberattack/.

[24] NAIC, Cybersecurity Breach Response HQ, disponible en http://www.naic.org/index_security_breach.htm.

[25] La seguridad y el seguro de la fuerza de trabajo de Dakota del Norte, el ataque cibernético contra el servidor estatal pueden afectar la información de WSI (julio de 2015), disponible en https://www.workforcesafety.com/news/news-item/cyber-attack-on-state-server-may-impact-wsi-information.

[26] En un ataque DDoS, un adversario dirige una avalancha de solicitudes de servicio ilegítimas para abrumar la computadora o red de destino en un intento de hacer que el recurso no esté disponible para los usuarios deseados, capturando así el control de múltiples sistemas infectándolos con malware. Véase Comité de Pagos e Infraestructuras de Mercado, Cyber Resiliencia en Infraestructuras de Mercados Financieros (noviembre de 2014), disponible en http://www.bis.org/cpmi/publ/d122.pdf.

ciberseguridad podría haber tenido un impacto sustancial no sólo en la empresa sino también en los socios, proveedores de servicios y asegurados.

34. Como un recordatorio de que los incidentes de ciberseguridad también pueden incluir actos de parte de personas de su entorno, se identificó un fraude interno en 2012 en una compañía mutualista de seguros francesa. Este fraude, como resultado de un robo interno de datos en un entorno replicado con información confidencial de los clientes, condujo a un caso de robo de identidad y afirmaciones falsas.

35. Recientemente en los Países Bajos, una aseguradora fue sometida al denominado "hack CEO", una forma específica de ataque cibernético de phishing.[27] Pretendiendo ser el CEO de un importante y conocido cliente comercial de la aseguradora, los criminales intentaron persuadir a los empleados del asegurador, para que transfiriera dinero a una determinada cuenta. Al parecer, los delincuentes habían investigado ciertos detalles operativos de la aseguradora.

36. Un informe reciente de PwC identificó varios incidentes adicionales de seguridad cibernética experimentados por aseguradores en múltiples jurisdicciones, incluyendo ataques contra líneas personales, viajes, salud y aseguradoras marinas.[28]

V. Resistencia de Ciber Seguros

37. Los diversos desafíos d el riesgo cibernético deben ser enfrentados con una respuesta amplia de paste de los aseguradores. Es necesaria una atención de alto nivel de la administración, así como una estructura de gobierno eficaz, capaz de comprender, prevenir, detectar, responder y abordar los incidentes de ciberseguridad. Además, debe establecerse un programa de gestión de riesgos que funcione correctamente y que esté en consonancia con las mejores prácticas de resistencia cibernética y se verifique mediante una revisión supervisora. Como se describe a continuación, este nivel de respuesta es consistente con los Principios Básicos de Seguros.

38. Para ser eficaz, es necesario abordar la ciberseguridad a todos los niveles de una institución y con respecto a las disposiciones pertinentes de terceros. En general, un programa eficaz de gestión del riesgo cibernético incluye mejoras continuas de procesos y control, procedimientos de gestión de incidentes tales como respuesta y recuperación de desastres, políticas y procedimientos de red apropiados, administración y control riguroso de privilegios de usuario, guía de configuración segura, monitoreo de los procedimientos de trabajo en el hogar, y las iniciativas continuas de concientización y educación para todo el personal.

39. Generalmente las mejores prácticas para la resistencia cibernética incluyen:[29]

---

[27] Este tipo de ataque cibernético se ha convertido en una amenaza emergente. Véase, por ejemplo, la Oficina Federal de Investigación de los Estados Unidos, "Compromiso de correo electrónico empresarial - una amenaza global emergente" (28 de agosto de 2015), disponible en https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise.

[28] PwC, Under the Lens: Threats to the Insurance Sector (November 2015).

[29] Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), Marco para mejorar la ciberseguridad de las infraestructuras críticas (febrero de 2014), disponible en http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf; FFIEC, Cybersecurity Assessment Tool (June 2015), disponible en, https://www.ffiec.gov/cyberassessmenttool.htm; Committee

• Gobierno

Junto con el compromiso de la Junta Directiva y la Alta Dirección, un marco adecuado de resistencia cibernética contribuye a la mitigación del riesgo cibernético. Por ejemplo, la Alta Dirección debería incluir a un funcionario con acceso a la Junta, que fuera responsable de desarrollar e implementar el marco de la ciberresistencia.

• Identificación

Detectar aquellas funciones y procesos empresariales que deben protegerse contra compromisos. Los activos de información (incluida la información personal sensible) y el acceso al sistema conexo deben ser parte del proceso de identificación. Las revisiones regulares y las actualizaciones son factores clave, ya que el riesgo cibernético está en constante evolución y pueden surgir "riesgos ocultos". Las entidades conectadas forman parte del cuadro completo; La importancia de los riesgos que plantean no es necesariamente proporcional a la importancia del servicio en particular. Por ejemplo, el bien conocido ataque cibernético contra el minorista Target implicaba la entrada a través de un proveedor de servicios de ventilación.[30]

• Proteccion

La resistencia puede ser proporcionada por el diseño. La protección integral implica la protección de las interconexiones y otros medios de acceso a las amenazas internas y externas a la institución. Al diseñar la protección, se debe tener en cuenta el "factor humano". Por lo tanto, la formación también es una parte esencial de la red de seguridad contra el riesgo cibernético. Los controles deben estar en línea con las principales normas técnicas, ya que los sólidos controles de TI contribuyen a la protección.

• Detección

El monitoreo continuo y completo de la seguridad cibernética es esencial para detectar posibles incidentes cibernéticos. Llevar a cabo análisis de seguridad también ayuda a detectar y mitigar incidentes cibernéticos.

• Respuesta y recuperación

No siempre es posible detectar o prevenir incidentes cibernéticos antes de que sucedan, incluso con los mejores procesos instalados. Por esta razón, la planificación de respuesta a incidentes es de gran importancia. La reanudación de los servicios (si se interrumpen) se debe lograr dentro de un plazo razonable, dependiendo del impacto de los incidentes y de la importancia del servicio. La planificación de contingencia, el diseño y la integración empresarial, así como la integridad de los datos (también en el caso de los acuerdos de intercambio de datos) son factores clave para una rápida reanudación. Para que la planificación de contingencia sea efectiva, debe someterse a

on Payments and Market Infrastructures and International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016), disponible en http://www.bis.org/cpmi/publ/d146.htm.

[30] SANS Institute, Estudio de Caso: Controles Críticos que Podrían Evitar la Violación de los Objetivos (5 de agosto de 2014), disponible en http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

pruebas periódicas. Los pasos para prevenir el contagio pueden mitigar otros riesgos. Debería establecerse una política de divulgación para mejorar la comunicación en caso de crisis. Por último, pero no menos importante, la preparación forense es esencial para las investigaciones de inmersión profunda. Estos elementos deben ser considerados en la planificación de la continuidad del negocio.

• Pruebas

Los programas de pruebas, las evaluaciones de vulnerabilidad, las pruebas basadas en escenarios, las pruebas de penetración y las pruebas en equipo rojo son las piedras angulares en la fase de pruebas. Las pruebas de seguridad cibernética deben incluirse cuando los sistemas se especifican, desarrollan e integran.

• Conciencia de la Situación

La conciencia contribuye a la identificación de amenazas cibernéticas. En consecuencia, el establecimiento de un proceso de inteligencia de amenazas ayuda a mitigar el riesgo cibernético. En este sentido, los aseguradores deberían considerar participar en iniciativas establecidas de intercambio de información.

• Aprendiendo y evolucionando

Los aseguradores deben reevaluar continuamente la eficacia de la gestión de la seguridad cibernética. Las lecciones aprendidas de los eventos cibernéticos y los incidentes cibernéticos contribuyen a mejorar la planificación. Los nuevos desarrollos en tecnología deben ser monitoreados.

VI. Aplicabilidad de los Principios Básicos de los Seguros a la Seguridad Cibernética

40. Aunque los Principios Básicos de Seguros (PBS) no abordan específicamente el riesgo cibernético y la resistencia cibernética, proporcionan una base general para que los supervisores aborden el sector de los seguros con respecto al riesgo cibernético y a la resistencia cibernética, exigiendo el manejo de riesgos significativos y controles internos relacionados.

41. Los PBS que pueden ser más relevantes para la supervisión del riesgo cibernético en el sector de los seguros incluyen:[31]

• PBS 7 (Gobierno Coorporativo)

• PBS 8 (Administración de riesgos y Controles Internos)

• PBS 9 (Revisión y Reporte de Supervisión)

• PBS 19 (Conducta de mercado)

• PBS 21 (Combate al fraude en seguros)

[31] También pueden ser relevantes otros PCS, como los PCS 16 (Gestión del riesgo empresarial para fines de solvencia) y 18 (Intermediarios).

Especialmente en lo que respecta al intercambio de información y la cooperación en materia de supervisión, también son pertinentes los siguientes PBS:

- PBS 3 (Intercambios de Información y Requerimientos de Confidencialidad)
- PBS 25 (Cooperación y coordinación en materia de supervisión)
- PBS 26 (Cooperación y coordinación transfronterizas en la gestión de crisis).
- PBS 7 – Gobierno Coorporativo

42. El PBS 7 fue revisado en noviembre de 2015. En virtud de dicho PBS, se espera que las aseguradoras puedan demostrar la eficacia de los sistemas y controles y el marco de gobierno corporativo. La Guía para este PBS establece: "Es responsabilidad de la Junta asegurarse de que la aseguradora tiene sistemas y funciones apropiados para la administración de riesgos y controles internos y para proveer la supervisión que asegure que estos sistemas y las funciones que los supervisan estén operando efectivamente y según lo planeado. "Identificar y abordar el riesgo cibernético debe ser una parte integral de la gestión del riesgo de una aseguradora.

PBS 8 - Administración de riesgos y Controles Internos

43. El PBS 8 fue revisado en noviembre de 2015. Este PBS requiere que un asegurador tenga, como parte de su marco general de gobierno corporativo, sistemas efectivos de gestión de riesgos y controles internos, incluyendo funciones efectivas para la gestión de riesgos, cumplimiento, asuntos actuariales y auditoría interna.

44. La Guía del PBS 8 enumera un conjunto mínimo de categorías que debe cubrir el sistema de gestión de riesgos. En lo que respecta al riesgo cibernético, la orientación es relevante, ya que se refiere a la "gestión del riesgo operacional", "la conducción de negocios" y "otras técnicas de mitigación del riesgo". Todos los riesgos materiales razonablemente previsibles y relevantes, incluidos los riesgos actuales y emergentes.

45. La Guía también describe los componentes típicos de un sistema de control interno eficaz. Bajo las "políticas y procesos" que se enumeran como uno de estos componentes, la guía describe dicho sistema de control interno como tener "controles apropiados para todos los procesos y políticas empresariales", incluyendo "funcionalidades críticas de TI", "acceso a bases de datos" "Sistemas de TI por parte de los empleados". Esto abarca claramente el riesgo cibernético.

46. Adicionalmente esta guía considera necesario el contar con recursos suficientes para las funciones de control, incluidos los sistemas de información de TI / gestión adecuados.

47. Finalmente, la guía del PBS 8 establece que la función de auditoría interna debe proporcionar garantías independientes a la Junta, y a la Alta Dirección, respecto de cuestiones como la capacidad y la adaptabilidad de la arquitectura de TI, para proporcionar información contable, financiera y oportuna.

48. Al entrar o revisar un acuerdo de subcontratación, el Directorio y la Alta Dirección deben considerar en qué medida el perfil de riesgo y la continuidad del negocio de la aseguradora se verán afectados por la contratación externa. Esto puede aplicarse a la gestión de los proveedores de servicios, la gestión de riesgos y los controles internos con respecto al riesgo cibernético.

PBS 9 - Revisión y Reporte de Supervisión

49. El PBS 9 se ocupa de los procesos y procedimientos generales que deberían tener los supervisores con respecto a la revisión y la presentación de informes. Estos procesos incluyen analizar el marco de supervisión para revisión e informes, ello para asegurar que se preste la debida atención a la naturaleza, escala y complejidad de los riesgos que pueden presentar los aseguradores y de los riesgos a los que pueden estar expuestos los aseguradores. En virtud de este PBS, el marco de supervisión debe exigir que un asegurador informe con prontitud cualquier cambio o incidente importante que pueda afectar la condición del asegurador o los clientes. En la actualidad se está examinando el PBS 21, en la parte de supervisión in situ, los supervisores deben obtener información suficiente para evaluar y analizar los riesgos a los que está expuesta una aseguradora y sus clientes y revisar la efectividad de la administración de los riesgos por parte de la aseguradora. El PBS 9 está siendo revisado.

PBS 19 - Conducta de mercado

50. Los requisitos para la conducción de negocios de seguros incluyen disposiciones relativas a la protección de la privacidad en virtud de las cuales las aseguradoras y los intermediarios están autorizados a recopilar, mantener, utilizar o comunicar información personal de los clientes a terceros.

51. Los requisitos para la conducción de negocios de seguros incluyen disposiciones relativas a la protección de la privacidad en virtud de las cuales las aseguradoras y los intermediarios están autorizados a recopilar, mantener, utilizar o comunicar información personal de los clientes a terceros.

ICP 21 – Combate al fraude en seguros

52. En virtud del PBS 21, los supervisores exigen que los aseguradores e intermediarios tomen medidas eficaces para disuadir, prevenir, detectar, informar y remediar el fraude en los seguros

Los PBS 3, 25 y 26 - Intercambio de Información y Cooperación Supervisora

53. El PCI 3 (Intercambio de Información y Requisitos de Confidencialidad) es relevante ya que, dada la naturaleza del riesgo cibernético, es posible que más de una jurisdicción estuviera involucrada en la identificación, administración y mitigación de tales riesgos. Actualmente dicho principio se está revisando.

54. La capacidad de compartir información con otras jurisdicciones -como se establece en el PBS 25 (Cooperación y coordinación en materia de supervisión) - es una herramienta importante para los supervisores, habida cuenta de la posibilidad de que un incidente cibernético tenga repercusiones transfronterizas. La habilidad de los supervisores para actuar rápidamente, identificar, administrar y mitigar los riesgos, será mejorada al contar con un mecanismo eficiente para compartir información. Dichos mecanismos podrían incluir memoranda de entendimiento bilaterales o multilaterales, como el Memorando de Entendimiento Multilateral de la AIFI (la norma mundial para el intercambio de información entre supervisores de seguros) u otros acuerdos de cooperación, como los establecidos, por ejemplo, en relación con los colegios de supervisión. Además, los resultados de la encuesta de la IAIS descritos en este documento sugieren que la mayoría de las

jurisdicciones pueden beneficiarse compartiendo iniciativas regulatorias y de supervisión relacionadas con la ciberseguridad, especialmente en temas como educación y capacitación cibernética y tratamiento del riesgo cibernético con respecto a la subcontratación. Actualmente se está examinando el PBS 25.

Ejemplos de trabajo de ciberseguridad de otras organizaciones que establecen normas del sector financiero mundial

Comité de Pagos e Infraestructuras de Mercado (CPMI) y Organización Internacional de Comisiones de Valores (IOSCO)

En junio de 2016, el Grupo de Trabajo Conjunto sobre la Resistencia Cibernética de la CPMI y la IOSCO publicó la "Orientación sobre la Resistencia Cibernética ante infracciones de los Mercados Financieros" .[32] Esta guía tiene como objetivo mejorar la capacidad de las infraestructuras del mercado financiero (IMF) para prevenir ataques cibernéticos, y responder efectivamente a ellos, así como lograr objetivos de recuperación más rápidos y seguros. La orientación no establece normas adicionales para las IMF que vayan más allá de las ya establecidas en los Principios para las infraestructuras de los mercados financieros (PIMF), pero apunta a elaborar información sobre los PIMF.[33]

Comité de Supervisión Bancaria de Basilea (BCBS)

En octubre de 2014, el BCBS publicó "Revisión de los Principios para una Gestión Segura del Riesgo Operacional" [34], que revisa la implementación de los Principios para la Gestión Racional del Riesgo Operacional publicados en 2011.[35] El informe aborda las prácticas de gestión del riesgo operacional de 60 aspectos sistemáticamente de importantes Bancos, y observa que algunos bancos han desarrollado escenarios relacionados con eventos catastróficos, como el ataque cibernético.

55. Bajo el PBS 26 (Cooperación y coordinación transfronterizas en materia de gestión de crisis), el supervisor colabora y coordina con otras autoridades pertinentes, de manera que una crisis transfronteriza que afecte a un asegurador o grupo específico pueda gestionarse eficazmente. Por consiguiente, se espera que los supervisores cooperen y coordinen con otras autoridades pertinentes con respecto a una crisis transfronteriza que implique la ciberseguridad de un asegurador o grupo específico. La planificación anticipada para una coordinación y gestión oportuna y coherente de una crisis transfronteriza (incluidas las medidas de política, las decisiones de respuesta a las crisis y las comunicaciones externas) es un componente de la gestión eficaz de las crisis. Actualmente se está examinando el PBS 26.

[32] Disponible en http://www.bis.org/cpmi/publ/d146.htm (29 de junio de 2016). Por invitación del grupo de trabajo conjunto, el Presidente de la FCTF actuó como observador durante el desarrollo de esta guía.
[33] CPMI y IOSCO, Principios para las infraestructuras de los mercados financieros (abril de 2012), http://www.bis.org/cpmi/publ/d101a.pdf.
[34] Disponible en http://www.bis.org/publ/bcbs292.htm.
[35] Disponible en http://www.bis.org/publ/bcbs195.htm.

56. Para ayudar a los supervisores a implementar prácticas de supervisión consistentes y sólidas; y para ayudar a las aseguradoras a implementar prácticas apropiadas de seguridad cibernética, podría ser necesario más material de la IAIS específico en el área.

VII. Respuesta de Supervisión al Riesgo Cibernético

57. Esta sección considera el papel de los supervisores, incluye un resumen de la encuesta de 2015 de los Miembros de la IAIS sobre la lucha contra el riesgo cibernético y proporciona ejemplos de respuestas de supervisión en curso y en evolución, a cuestiones de ciberseguridad.

58. La misión de la IAIS incluye el desarrollo y mantenimiento de mercados de seguros justos, seguros y estables para el beneficio y la protección de los asegurados. En este contexto, los supervisores de seguros tienen un rol en el abordaje de los riesgos (incluyendo el riesgo cibernético) que podrían plantear amenazas a la seguridad, estabilidad y confianza en los mercados de seguros y que podrían comprometer a los asegurados.

59. El supervisor puede abordar el riesgo cibernético mediante la regulación apropiada y el proceso de supervisión. Las áreas de supervisión que pueden tener una relevancia particular para el riesgo cibernético y la resistencia cibernética incluyen:

- La seguridad de la información privada de los aseguradores e intermediarios;
- La delincuencia financiera a través de medios cibernéticos; y
- Planificación de la continuidad del negocio y la recuperación de desastres - para aseguradores e intermediarios individuales y potencialmente, para el sector de seguros en su conjunto.

60. Además, la cooperación transfronteriza e intersectorial de supervisión puede ser importante para abordar el riesgo cibernético, ya que este tema es de naturaleza global.

Encuesta de IAIS sobre Riesgos Cibernéticos y Prácticas Supervisoras

61. Durante los meses de enero y febrero de 2015, la IAIS llevó a cabo una encuesta entre sus miembros para obtener información sobre los actuales enfoques de supervisión del riesgo cibernético. Específicamente, la encuesta tenía por objeto ayudar a la Fuerza de Trabajo sobre Delitos Financieros (FCTF) a comprender la percepción de los miembros sobre el riesgo cibernético, su participación en la lucha contra las amenazas cibernéticas y los enfoques de supervisión que utilizan o están en desarrollo en esta esfera. Aproximadamente 30 miembros respondieron. Las respuestas recibidas de la encuesta, muestran que las prácticas de supervisión y las opiniones sobre ciberseguridad varían ampliamente entre los miembros de la IAIS. A continuación se presentan algunas tendencias notables observadas en las respuestas a la encuesta. En el anexo I figura un resumen de los resultados de la encuesta.

62. La mayoría de los encuestados indicaron que han establecido o establecerán requisitos reglamentarios o de supervisión para el gobierno corporativo de los aseguradores con respecto a la ciberseguridad. Aunque muchos de los encuestados aún no han definido disposiciones específicas sobre seguridad cibernética, esperan que las aseguradoras puedan hacer frente al riesgo cibernético bajo requisitos regulatorios y de supervisión más amplios, es decir, a través de actividades de gestión de riesgos empresariales. Además, algunos de los encuestados informaron de la adhesión a

las normas pertinentes, en particular la norma ISO para la gestión de la seguridad de la información[36], así como el marco del Instituto Nacional de Estándares y Tecnología (NIST) para mejorar la infraestructura.[37] Algunos encuestados han publicado directrices de seguridad cibernética aplicables a las instituciones financieras.

63. Sin embargo, la resistencia cibernética no parecía percibirse como una prioridad reglamentaria para la mayoría de los encuestados. Las razones dadas incluyen la etapa actual de desarrollo de TI, la falta de requisitos reguladores específicos para la resistencia cibernética y la confianza en las autoevaluaciones de los aseguradores. Además, la mayoría de los encuestados parecían tener limitaciones en el personal con responsabilidad y experiencia en el monitoreo y supervisión de la seguridad cibernética.

64. Los resultados de la encuesta indicaron que hay una variedad de enfoques de supervisión de la resistencia cibernética. Por ejemplo, algunos encuestados evalúan la naturaleza y la escala del riesgo cibernético enfrentado por una aseguradora a través de inspecciones in situ. Algunos esperan adoptar ejercicios de autoevaluación o inspecciones temáticas centradas en la resistencia cibernética de los aseguradores. Otros no se centran específicamente en el riesgo cibernético, pero pueden evaluar la seguridad cibernética como parte de un plan de continuidad de negocio o marco de gestión de riesgos de una aseguradora. Además, una minoría de los encuestados define el tipo o la gravedad de los incidentes cibernéticos que un asegurador debe informar a su autoridad supervisora, mientras que la mayoría de los encuestados no tienen requisitos específicos para la notificación y algunos dependen de los informes anuales de auditoría.

65. Aunque el número de respuestas de la encuesta fue limitado, las respuestas de los miembros que respondieron, y otra información descrita en este informe demuestra que no existe una práctica uniforme entre los miembros de la IAIS con respecto a la supervisión en materia de ciberseguridad.

Ejemplos de respuestas de supervisión al riesgo cibernético

66. Además de sus respuestas a la encuesta, algunos miembros de la IAIS proporcionaron ejemplos de algunas iniciativas de riesgo cibernético emprendidas en las jurisdicciones de los estados miembros, incluidas, en algunos casos, la cooperación público-privada y los enfoques de todo el mercado. Estos ejemplos se describen a continuación.

67. Francia. La Autoridad de Control Prudencial y de Resolución (ACPR) categoriza la supervisión relacionada con el riesgo cibernético bajo el control del Sistema de Información (SI). La ACPR estableció los siguientes cuatro criterios para la supervisión de la seguridad cibernética: (1) Confidencialidad: La información es accesible sólo a aquellos que están autorizados a accesarla. La información está protegida a lo largo de su ciclo de vida; (2) Integridad: Los datos almacenados son precisos y consistentes. No hay necesidad de alteración entre los registros de datos; (3)

[36] Las normas ISO 27000 ayudan a las organizaciones a mantener seguros los activos de información. ISO / IEC 27001 es el estándar que proporciona los requisitos para un sistema de gestión de la seguridad de la información. Organización Internacional de Normalización, ISO / IEC 27001 - Gestión de la Seguridad de la Información, disponible en http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.
[37] NIST, Marco para la mejora de la ciberseguridad de las infraestructuras críticas (12 de febrero de 2014), disponible en http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Disponibilidad: La información es accesible por las personas autorizadas en el momento adecuado con el rendimiento adecuado; Y (4) Auditabilidad: El acceso e intentos de acceso a SI o las actividades en SI se registran y se almacenan. Los archivos registrados no deben modificarse o eliminarse. Con estos criterios, la ACPR estudia las siguientes áreas: gobernabilidad; Identificación y evaluación de los riesgos de SI; respuestas a los riesgos de SI; y la evaluación de los controles, la gestión del riesgo y la actividad de seguimiento.

68. Alemania. El examen de supervisión de la gestión del riesgo cibernético suele realizarse a través de inspecciones in situ. El procedimiento exacto depende del tamaño y los riesgos de la empresa particular y del tamaño del equipo de supervisores. Para las pequeñas empresas, el Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) aborda este aspecto en el contexto de la gestión de riesgos. Para las empresas grandes, a menudo organiza una reunión centrada en cuestiones de seguridad de la información. Durante una reunión de este tipo, el equipo discute los aspectos de la seguridad cibernética y la gestión de riesgos de TI que son de gran importancia. Otras áreas de la seguridad cibernética se pueden abordar al examinar más de cerca otros aspectos relacionados con TI, como el proceso de desarrollo de software o la gestión de la identidad.

69. Unión Europea. La Comisión Europea realizó la propuesta de Directiva[38] relativa a medidas para garantizar un alto nivel común de seguridad de las redes y de la información en toda la Unión. El 7 de diciembre de 2015, el Parlamento Europeo y el Consejo llegaron a un acuerdo sobre las medidas propuestas por la Comisión para aumentar la seguridad en línea en la UE. Esta Directiva es la primera pieza de la legislación europea sobre ciberseguridad. Sus disposiciones tienen por objeto hacer el entorno en línea más fiable y, por tanto, apoyar el buen funcionamiento del mercado único digital de la UE. Las nuevas normas: 1) mejorarán las capacidades de ciberseguridad en los Estados Miembros; (2) mejorar la cooperación de los estados miembros en materia de ciberseguridad; Y 3) obligar a los operadores de servicios esenciales en los sectores de la energía, el transporte, la banca y la salud, así como a los proveedores de servicios digitales clave como los motores de búsqueda y la nuve de almacenamiento de datos, a adoptar medidas de seguridad apropiadas y a denunciar los incidentes a las autoridades nacionales. [39]

70. El 24 de mayo de 2016 entró en vigor un proyecto de reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y será aplicable a partir del 25 de mayo de 2018.[40] Este texto incluye disposiciones

[38] Propuesta de Directiva sobre medidas para garantizar un alto nivel común de seguridad e información en la red en la Unión - 2013/048 (denominado SRI o NIS).

[39] Directiva sobre la seguridad de las redes y la información de la Comisión Europea: los co-legisladores acuerdan la primera legislación a escala europea sobre seguridad cibernética (9 de diciembre de 2015), disponible en http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation.

[40] El Parlamento Europeo y el Consejo de la Unión Europea, el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos, Y que deroga la Directiva 95/46 / CE (Reglamento General de Protección de Datos) (4 de mayo de 2016), disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

sobre notificación de incidentes de seguridad relativas a datos personales, y faculta a los comisionados nacionales de datos para imponer multas significativas.

71. Países Bajos. Uno de los resultados de las investigaciones temáticas del banco central de los Países Bajos (el De Nederlandsche Bank o DNB) es proporcionar a las instituciones financieras individuales un punto de referencia con el que se comparan en cada sector (por ejemplo, aseguradores, bancos y Fondos de pensiones) basándose en los resultados de las investigaciones. Las instituciones financieras individuales pueden ver dónde están posicionadas en comparación con el promedio de cada sector. Esto se aplica a la gestión del riesgo cibernético.

72. El DNB también supervisa grandes aseguradores internacionales conjuntamente con supervisores de otras jurisdicciones. Se han llevado a cabo varios proyectos conjuntos de investigación para la supervisión de estos grupos. Además, durante las investigaciones, dos grupos de personas de diferentes autoridades de supervisión han trabajado juntos en un equipo. A través de esta cooperación, el DNB tiene la intención de obtener información sobre la gestión del riesgo cibernético dentro de los grupos de seguros. Además, algunas unidades dentro de un grupo prestan servicios internamente para entidades de varios grupos, mientras que las entidades individuales del grupo pueden estar sujetas a regulaciones financieras separadas aplicables en cada jurisdicción. El DNB tiene la intención de obtener una mejor visión de estas unidades desde una perspectiva de todo el grupo a través de ese trabajo. Un buen ejemplo de este tipo de cooperación de supervisión incluye la supervisión centrada en la gestión de activos en todo el grupo y en los sistemas informáticos.

Iniciativas de Intercambio de Información del Sector Privado en los Países Bajos

En los Países Bajos, el banco central (De Nederlandsche Bank, o DNB) ha encontrado que las aseguradoras reconocen el peligro que representa el riesgo cibernético y están dispuestas a cooperar entre sí. La Asociación Holandesa de Aseguradores cuenta actualmente con dos grupos de trabajo activos en el campo de los riesgos de TI y un grupo de consulta separado formado por directores de TI de aseguradoras. Los dos grupos de trabajo se enfocan respectivamente en Seguridad de la Información (SI) y Gestión de la Continuidad del Negocio (GCN). En estos dos grupos, los especialistas de las mayores aseguradoras intercambian información sobre sus experiencias, lo que están haciendo y cómo aprender unos de otros. Los grupos de trabajo se reúnen de tres a cuatro veces por año. El DNB ha hecho presentaciones a ambos grupos y ha observado que el proceso de intercambio de información aún tiene margen de mejora. Por ejemplo, la información sobre los ataques a los aseguradores podría ser compartida más ampliamente.

73. Singapur. La Autoridad Monetaria de Singapur (MAS), junto con la Asociación de Bancos de Singapur, organiza un ejercicio trianual en toda la industria, para permitir a las instituciones financieras practicar y mejorar la coordinación con los principales socios gubernamentales para minimizar el impacto de una crisis derivada de un incidente cibernético. El ejercicio Raffles IV de 2014, incluyó la participación unas 141 instituciones financieras, incluyendo bancos, compañías financieras, compañías de seguros, firmas de administración de activos y casas de valores participaron en un ejercicio de medio día, donde se mostró la respuesta de los participantes ante un incidente masivo de ciberseguridad en la industria financiera. Las instituciones financieras y las infraestructuras de mercado se enfrentaron a una combinación de incidentes simulados de

ciberseguridad, incluido el robo de información; compromiso de los sistemas centrales de las instituciones financieras; Cortes de cajeros automáticos, interrupciones en los servicios en línea; y la corrupción del sitio web. Los ataques simulados requerían que las instituciones financieras evaluaran el impacto de los ataques en los negocios de las instituciones en cinco grandes categorías: cliente, reputacional, regulador y legal, financiero y operacional.[41]

74. Reino Unido. Las autoridades financieras del Reino Unido[42] han emprendido una serie de proyectos para comprender y tratar de mitigar el riesgo cibernético. En 2005, 2007 y 2009, las autoridades financieras del Reino Unido emprendieron proyectos para evaluar la resistencia operativa del sector financiero del Reino Unido.[43] En 2012, las autoridades respondieron a las amenazas cibernéticas y la retroalimentación del sector y se centraron en el desarrollo de encuestas más pequeñas y más específicas Para profundizar en el tema de la tecnología y la resistencia cibernética. Esto llevó a un ejercicio de escritorio en 2013 para probar la respuesta del sector bancario mayorista a un ataque cibernético sostenido e intensivo.[44]

75. El Comité de Política Financiera (CPF) recomendó que HM Treasury, en colaboración con los organismos gubernamentales pertinentes y las demás autoridades financieras, debería trabajar con el sistema financiero británico central y su infraestructura para establecer un programa de trabajo para mejorar y probar la resistencia ante el riesgo cibernético. En respuesta, las autoridades emitieron un cuestionario de gestión del riesgo cibernético dirigido a las principales empresas del Reino Unido y los temas de esta encuesta se han utilizado para identificar las áreas de trabajo futuro. Sobre la base de esta evaluación, las capacidades necesarias para abordar el riesgo cibernético pueden dividirse en tres categorías: capacidades defensivas, capacidades de recuperación y gobernabilidad efectiva. El programa de trabajo resultante se articula en torno a cuatro temas: (1) mejorar la comprensión de la amenaza para el sector financiero; (2) fortalecer el trabajo para evaluar la resistencia actual del sector al riesgo cibernético; (3) desarrollar planes para probar la resistencia del sector; y, (4) mejorar el intercambio de información.

76. En junio de 2015, el CPF recomendó además que el Banco de Inglaterra, la Autoridad Reguladora Prudencial (ARP) y la Autoridad de Conducta Financiera (ACF) trabajen con las empresas en el núcleo del sistema financiero del Reino Unido para asegurar que completen las pruebas CBEST (un marco para poner a prueba las vulnerabilidades cibernéticas) y adoptar planes de acción individuales de resistencia cibernética. El Banco, la ARP y la ACF también deben establecer arreglos para que las pruebas CBEST se conviertan en un componente de la evaluación regular de la resistencia cibernética dentro del sistema financiero del Reino Unido. En agosto de 2015, la ARP y la ACF iniciaron un proyecto para evaluar la resistencia del sector de los seguros.[45]

---

[41] Asociación de Bancos en Singapur, "El Sector Financiero Responde a los Ataques Cibernéticos en el Cuarto Ejercicio de Continuidad del Negocio de la Industria" (21 de noviembre de 2014), disponible en http://abs.org.sg/docs/library/mediarelease_20141121.pdf.

[42] Antes del 1 de abril de 2013, las autoridades financieras eran el Banco de Inglaterra, la Autoridad de Servicios Financieros y HM Treasury.

[43]Banco de Inglaterra: http://www.bankofengland.co.uk/financialstability/fsc/Pages/bcinformation.aspx.

[44] Ibid

[45] Autoridad de Regulación Prudencial, Banco de Inglaterra: http://www.bankofengland.co.uk/pra/Documents/about/insuranceletter100815.pdf.

Medidas adicionales de supervisión y cooperación en el Reino Unido

El gobierno del Reino Unido considera los ataques cibernéticos junto con amenazas terroristas, como un riesgo de alto nivel para la seguridad nacional. En consecuencia, ha establecido una serie de iniciativas para ayudar a prevenir los ciberataques, entre ellos.

- Cyber Essentials[46] - un estándar básico de higiene cibernética lanzado en 2014 para ayudar a las organizaciones a protegerse contra ataques cibernéticos comunes
- Una Unidad Nacional de Delitos Cibernéticos dentro de la Agencia Nacional del Crimen
- Una asociación de intercambio de información cibernética para permitir que el gobierno y la industria intercambien información sobre amenazas cibernéticas[47]
- Un único sistema de información para que las personas denuncien el delito cibernético motivado por la financiación mediante Fraude de Acción[48], un Equipo Nacional de Respuesta a Emergencias Informáticas del Reino Unido (CERT) para mejorar la coordinación nacional de incidentes cibernéticos49.
- Un nuevo esquema de Respuesta a Incidentes Cibernéticos en la Central de Comunicaciones del Gobierno para ayudar a las organizaciones a recuperarse de un ataque cibernético
- Una red de Centros de Excelencia para la Investigación de la Seguridad Cibernética dentro de las universidades del Reino Unido en 2013, para ayudar a proporcionar investigación confiable y actualizada y proezas académicas.

77. Estados Unidos. Hay varias iniciativas y programas en los Estados Unidos que se centran en la resistencia cibernética del sector financiero, incluyendo las aseguradoras. Estos incluyen, pero no se limitan a, lo siguiente.

78. Comité de Infraestructura Financiera y Bancaria. El Departamento de Hacienda de los Estados Unidos preside al Comité de Infraestructura de Información Financiera y Bancaria (FBIIC), que es un comité de 18 reguladores federales y estatales y organizaciones relacionadas, incluyendo la Junta de Gobernadores del Sistema de la Reserva Federal y Reguladores del seguro estatal. El FBIIC fue fundado para enfocarse en: (1) mejorar la coordinación y la comunicación entre los reguladores

[46] Gobierno del Reino Unido, Departamento de Negocios, Innovación y Habilidades y Oficina del Gabinete, Orientación - Esquema de Cibernética Esencial (abril de 2014), disponible en https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[47] Gobierno del Reino Unido, Oficina del Gabinete, Departamento de Negocios, Innovación y Habilidades, Oficina de Relaciones Exteriores y de la Commonwealth y Seguridad Nacional e Inteligencia, Documento de Política - 2010 a 2015 Política Gubernamental: Seguridad Cibernética (febrero de 2013), disponible en https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/establishing-a-cyber-security-information-sharing-partnership.

[48] El Fraude de Acción es el centro nacional de informes de delitos de fraude y internet de Reino Unido. Información disponible en: http://www.actionfraud.police.uk/about-us.

[49] CERT-UK (https://www.cert.gov.uk/) es el Equipo Nacional de Respuesta a Emergencias Informáticas del Reino Unido, formado en marzo de 2014 en respuesta a la Estrategia Nacional de Seguridad Cibernética (noviembre de 2011), disponible en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf).

financieros; (2) mejorar la resistencia del sector financiero; y (3) promover la asociación público-privada. El Tesoro coordina los esfuerzos de seguridad cibernética del sector financiero de los Estados Unidos a través del FBIIC. Para cumplir con su misión el FBIIC: (1) identifica los activos críticos de infraestructura, junto con sus ubicaciones y vulnerabilidades potenciales, y prioriza su importancia para el sistema financiero de los Estados Unidos; (2) establece una capacidad de comunicación segura entre los reguladores financieros y protocolos para comunicarse durante una emergencia; y (3) asegura que exista personal suficiente en cada organización miembro que cuente con las autorizaciones de seguridad adecuadas para manejar información clasificada y de coordinación en una emergencia.[50]

79. Poder para las Sanciones Federales. El 1 de abril de 2015, el Presidente firmó la Orden Ejecutiva 13694, Bloqueando la propiedad de ciertas personas que participan en Actividades Cibernéticas Maliciosas Significativas. Esta Orden Ejecutiva autoriza al Secretario de Hacienda, en consulta con el Procurador General y el Secretario de Estado, a imponer sanciones a las personas o entidades que participan en ciertas actividades cibernéticas malintencionadas significativas.[51]

80. Marco del NIST. El marco para mejorar la seguridad cibernética de las infraestructuras críticas (Marco NIST) fue publicado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos en febrero de 2014. El Marco NIST fue creado mediante la colaboración entre la industria y el gobierno y establece un sistema voluntario, Y un enfoque rentable para la gestión de la ciberseguridad.[52] Aunque originalmente se creó para aplicabilidad a la infraestructura crítica (es decir, servicios esenciales que sustentan la economía, la seguridad y la salud de EE.UU.). El Marco NIST fue creado a través de la colaboración entre la industria y el gobierno y establece un sistema voluntario, Aunque se creó originalmente para aplicarse a la infraestructura crítica (es decir, servicios esenciales que sustentan la economía, la seguridad y la salud de los Estados Unidos), el Marco del NIST también fue diseñado para ser utilizado por empresas de todos los tamaños y de todos los sectores y jurisdicciones. Las autoridades de los Estados Unidos continúan promoviendo la adopción generalizada de mejores prácticas de ciberseguridad, mediante el uso del Marco NIST con el objetivo de ampliar la comprensión del riesgo cibernético y mejorar la ciberseguridad colectiva.[53]

81. La herramienta de Evaluación de la Seguridad Cibernética FFIEC. Aunque diseñada específicamente como una herramienta de autoevaluación voluntaria para los bancos, la Herramienta de Evaluación de la Seguridad Cibernética (Evaluación) desarrollada por el Consejo

[50] Comité de Infraestructura Financiera y Bancaria: https://www.fbiic.gov/index.html.
[51] Oficina Ejecutiva del Presidente, Orden Ejecutiva: Bloquear la Propiedad de Ciertas Personas que Participan en Actividades Cibernéticas Maliciosas Significativas (1 de abril de 2015), disponibles en https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.
[52] NIST, Marco para la mejora de la ciberseguridad de las infraestructuras críticas (12 de febrero de 2014), disponible en http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[53] Casa Blanca, Esfuerzos de la Administración en la Seguridad Cibernética: El Año en Revisión y Esperando hacia 2016 (2 de febrero de 2016), disponible en https://www.whitehouse.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016.

Federal de Examinación de Instituciones Financieras (FFIEC)[54] en 2015 ofreció un enfoque lógico para la gestión del riesgo cibernético, aspectos que podrían ser considerados por otras instituciones financieras, incluidas las aseguradoras. La evaluación está diseñada para proveer a las instituciones financieras dentro de su área de acción un "proceso repetible y mesurable" para informar a la Alta Dirección y las Juntas Directivas de las instituciones sobre el riesgo cibernético y la seguridad cibernética.[55] La Evaluación puede utilizarse para (1) determinar el perfil de riesgo inherente de la institución, o su riesgo cibernético global; (2) evaluar el vencimiento de la ciberseguridad de la institución en cinco dominios separados y si esa preparación para la seguridad cibernética está alineada con el riesgo inherente de la institución; y (3) identificar prácticas o controles de gestión de riesgos específicos que son necesarios para mejorar la seguridad cibernética.

Medidas federales adicionales de supervisión y cooperación en los Estados Unidos

Compartir información cibernética. En diciembre de 2015, el Presidente firmó la Ley para Compartir la Información Cibernética de 2015 (CISA), que establece un sistema para que las compañías privadas compartan voluntariamente con agencias federales la información sobre amenazas cibernéticas. Las compañías que comparten esa información reciben protecciones específicas de responsabilidad. La información personalmente identificable no directamente relacionada con una amenaza debe ser eliminada antes de compartir los datos.[56]

Plan Nacional de Seguridad Cibernética. El 19 de febrero de 2016, el Presidente solicitó a las agencias del Departamento Ejecutivo, implementar un Plan de Acción Nacional de Seguridad Cibernética (CNAP) que toma medidas a corto plazo y pone en marcha una estrategia a largo plazo para mejorar el conocimiento y protección de la seguridad cibernética, proteger la privacidad y mantener la seguridad pública. Así como la seguridad económica y nacional, y capacitar a los estadounidenses para mejorar el control de su seguridad digital. Además de establecer la Comisión sobre el fortalecimiento de la ciberseguridad nacional para desarrollar una hoja de ruta de acciones futuras, El CNAP hace un llamado a los aseguradores de salud y los interesados en el cuidado de la salud para tomar medidas significativas que mejoren sus prácticas de administración de datos, y garantizar que los datos sensibles de sus consumidores están confiablemente seguros.[57]

Centro de Análisis e intercambio de información sobre Servicios Financieros. El sector privado estableció el Centro de Análisis e intercambio de Información sobre Servicios Financieros (FS-ISAC) para compartir información sobre amenazas, vulnerabilidades e incidentes, incluyendo reportes anónimos de instituciones miembros y varias autoridades públicas. Varias agencias recomiendan la membresía del FS-ISAC, incluyendo la FFIEC, sus agencias miembros, el Departamento de Seguridad

[54] El FFIEC es un organismo oficial interinstitucional estadounidense facultado para prescribir principios uniformes, estándares y formularios de informes para el examen federal de instituciones financieras por parte de ciertos reguladores bancarios estadounidenses. Vea el sitio web de FFIEC: http://www.ffiec.gov/.

[55] Consejo de Examen de las Instituciones Financieras Federales (FFIEC), Glosario de la Herramienta de Evaluación de la Seguridad Cibernética (junio de 2015), disponible en https://www.ffiec.gov/cyberassessmenttool.htm.

[56] Ley de Asignaciones Consolidadas, 2016, Pub. L. 114-113 (Dec. 15, 2015).

[57] Comunicado de prensa de la Casa Blanca, Hoja Informativa: Plan de Acción Nacional de Seguridad Cibernética (9 de febrero de 2016), disponible en https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Nacional y el Departamento de Hacienda. La Directiva Presidencial 7 (2003) define el papel del gobierno federal como proveedor de información de amenaza sobre vulnerabilidad de información a FS-ISAC y a entidades del sector privado que operan infraestructura crítica, lo cual ayuda a la protección de infraestructura crítica a través de asociaciones público- privadas y el papel de coordinación del Tesoro.[58] Además, las empresas privadas de infraestructura crítica del sector de servicios financieros formaron el Consejo de Coordinación del Sector de Servicios Financieros (FSSCC) para coordinar las actividades de protección de las infraestructuras críticas para el sector financiero, incluida la respuesta a los incidentes y los problemas conexos.[59] Los aseguradores están involucrados tanto en el FS-ISAC como en el FSSCC.

83. Iniciativas Cibernéticas de la Asociación Nacional de Comisionados de Seguros (NAIC). La NAIC está llevando a cabo varias iniciativas en respuesta a amenazas cibernéticas emergentes. Los reguladores de seguros estatales sirven en el FBIIC y en el Foro de Seguridad Cibernética para Reguladores Independientes y Ejecutivos, donde trabajan con los reguladores federales para desarrollar las mejores prácticas y discutir enfoques comunes a los desafíos de ciberseguridad. A finales de 2014, la NAIC formó el Grupo de Trabajo de Seguridad Cibernética (EX) para coordinar los esfuerzos de los reguladores de seguros en abordar las cuestiones de ciberseguridad. Poco después de su constitución, el Equipo de Tareas estableció 12 Principios para una Guía efectiva de ciberseguridad para reguladores de seguros, los cuales establecen un marco para que los reguladores evalúen los esfuerzos de los aseguradores, productores y otras entidades reguladas para proteger la información del consumidor.[60] Estos principios fueron revisados y adoptados por el Comité Ejecutivo / Plenario de la NAIC en junio de 2015. El Grupo de Trabajo desarrolló entonces el Suplemento de Cobertura de Seguridad Cibernética y Robo de Identidad para los estados financieros de aseguradoras, con el objeto de recopilar información de desempeño financiero sobre aseguradores que suscriben cobertura de seguridad cibernética. El Comité Ejecutivo y el Comité Plenario de la NAIC adoptaron el suplemento revisado en agosto de 2015 y las presentaciones comenzaron en el primer trimestre de 2016.[61] El Grupo de Trabajo también colabora con el Grupo de Trabajo sobre Examen de Tecnología de la Información de la NAIC y el Grupo de Trabajo sobre Normas de Examen de Conducta del Mercado, para desarrollar y actualizar protocolos para su inclusión como guía en el Manual de Examinadores de la Condición Financiera y el Manual de Regulación del Mercado, respectivamente; ello a medida que las amenazas cibernéticas continúan evolucionando. Finalmente, el Grupo de Trabajo también desarrolló la Hoja de Ruta de NAIC para las Protecciones de Ciberseguridad del Consumidor, en el que se describen las protecciones que la NAIC cree que los consumidores tienen derecho a recibir de las compañías de seguros, Agentes y

[58] Centro de Análisis e intercambio de información sobre Servicios Financieros (https://www.fsisac.com/about).

[59] Consejo de Coordinación del Sector de Servicios Financieros para la Protección de la Infraestructura Crítica y la Seguridad de la Patria (https://www.fsscc.org/).

[60] NAIC, Principios para una Ciberseguridad Efectiva: Guía de Regulación de Seguros (abril de 2015), disponible en http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[61] NAIC, Ciberseguridad y Robo de Identidad (junio de 2015), disponible en http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_cyber_id_theft_ins_suplement.pdf.

otros negocios, cuando estas entidades recopilan, mantienen y usan información personal.[62] Adoptada por primera vez por el Equipo de Tareas en octubre de 2015, la Hoja de Ruta fue adoptada por el Comité Ejecutivo / Plenario de la NAIC en diciembre de 2015. Estas protecciones se incorporarán en las actualizaciones de leyes y reglamentos pertinentes de la NAIC, así como en una nueva "Ley Modelo de Seguridad de Datos sobre Seguros" que fue expuesta en marzo de 2016 y que puede ser considerada para adopción en 2016.

84. Función del Supervisor Estatal de los Estados Unidos. En general, en caso de incumplimiento de un asegurador nacional, el estado principal puede utilizar su autoridad reguladora de las siguientes maneras: (1) coordinar las llamadas con el asegurador para determinar: cuando se produjo el incumplimiento; quien se ve afectado por tal incumplimiento y, utilizando esa información, determinar qué reguladores necesitan ser informados del impacto de la falla en los residentes del estado; y de cómo se notificará a las personas afectadas (por ejemplo, por correo postal, correo electrónico, anuncios en los periódicos, etc.); (2) garantizar que el asegurador adopte medidas apropiadas en respuesta a la violación (por ejemplo, protección contra robo de identidad, etc.); (3) comunicarse con los reguladores estatales / federales según corresponda; y (4) determinar si un examen dirigido es necesario / apropiado y, en caso afirmativo: coordinar la selección del proveedor para realizar el examen de ciberseguridad; Coordinar la ejecución de los procedimientos de examen; Determinar el alcance del trabajo utilizando los conceptos del Manual de Examinadores de la Condición Financiera cuando sea apropiado; Comunicar los resultados del examen; y determinar si es necesaria una acción reguladora. Los reguladores de seguros estatales pertinentes han adoptado los exámenes de conducta de mercado de múltiples estados, después de violaciones de datos del asegurador, examinando, entre otras cosas, los detalles de las infracciones, las respuestas de los aseguradores a las infracciones y el impacto financiero de los incumplimientos tanto de los asegurados como de los aseguradores .

85. Departamento de Servicios Financieros de Nueva York. En noviembre de 2015, el Departamento de Servicios Financieros de Nueva York (DFS) emitió una carta a los miembros de la FBIIC indicando que estaba considerando una nueva regulación de seguridad cibernética para las instituciones financieras. La carta establece propuestas clave de regulación que el DFS considera como parte de esas regulaciones, e invita a la retroalimentación. Entre otras disposiciones, las regulaciones potenciales requerirían que las instituciones financieras adopten políticas y procedimientos escritos de ciberseguridad supervisados por un Oficial Principal de Seguridad de la Información designado (CISO) sobre: (1) seguridad de la información; (2) gobierno y clasificación de datos; (3) controles de acceso y gestión de identidad; (4) planificación y recursos para la continuidad del negocio y recuperación de desastres; (5) planificación de capacidad y rendimiento; (6) preocupación de operaciones y disponibilidad de sistemas; (7) seguridad de sistemas y redes; (8) desarrollo de sistemas y aplicaciones y garantía de calidad; (9) seguridad física y controles ambientales; (10) privacidad de los datos del cliente; (11) gestión de proveedores y terceros proveedores de servicios; y (12) respuesta a incidentes, incluyendo el establecimiento de roles claramente definidos y

[62] NAIC, Ciberseguridad y Robo de Identidad (junio de 2015), disponible en http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_cyber_id_theft_ins_suplement.pdf.http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf

autoridad para tomar decisiones. Además, se exige a las instituciones que apliquen y mantengan políticas y procedimientos para garantizar la seguridad de los datos, o sistemas sensibles que sean accesibles a terceros proveedores de servicios o que estén en su poder, y que las políticas y procedimientos incluyan requisitos internos mínimos, términos preferidos que se incluirán en los contratos con terceros proveedores de servicios que aborden los riesgos de seguridad de la información. Además, el CISO deberá presentar al DFS un informe anual, revisado por la Junta, que evalúe el programa de ciberseguridad y el riesgo cibernético para la institución. La iniciativa de Nueva York permanece en la fase de propuesta.

VIII. Conclusión

87. El riesgo cibernético representa un desafío cada vez mayor para el sector de los seguros, que los supervisores están obligados a abordar en virtud de los PBS. Las aseguradoras recolectan, almacenan y administran volúmenes sustanciales de información personal y comercial confidencial. Debido a estos depósitos de datos, los aseguradores son l objetivo principal de los ciberdelincuentes que buscan información que más tarde pueda ser utilizada para obtener ganancias financieras a través de la extorsión, robo de identidad u otras actividades delictivas. Además, debido a que las aseguradoras son contribuyentes significativos al sector financiero mundial, las interrupciones de los sistemas de las aseguradoras debido a incidentes de ciberseguridad pueden tener implicaciones de largo alcance.

88. El sector de los seguros enfrenta un riesgo cibernético tanto de fuentes internas como externas, incluso a través de interconexiones con terceros. Los incidentes de ciberseguridad en el sector de seguros pueden resultar en daños graves y de largo plazo para los asegurados afectados y costos legales, regulatorios y operacionales significativos, incluyendo daño a la reputación. Además, el sector de los seguros en su conjunto puede verse afectado por una pérdida de confianza pública. Debido a la creciente frecuencia y gravedad de los incidentes de ciberseguridad en todas las entidades comerciales, la resistencia cibernética debe ser alcanzada por todas las aseguradoras, independientemente de su tamaño, especialidad, domicilio o alcance geográfico.

89. Dada la escala mundial del riesgo cibernético es necesario abordar estos riesgos a nivel global, existen ejemplos de este trabajo en curso a nivel internacional, incluso por organismos normativos del sector financiero como CPMI y IOSCO. Una cooperación y coordinación transfronterizas eficaz es un componente importante de la respuesta de supervisión al riesgo cibernético.

90. Los supervisores de seguros tienen un papel importante en la mejora de la resistencia cibernética en el sector de los seguros. La naturaleza del riesgo cibernético requiere un mayor escrutinio por parte de los supervisores y una mayor cooperación e intercambio de información, con salvaguardias apropiadas, entre y entre los sectores público y privado para mejorar la resistencia cibernética.

91. Aún y cuando los PBS no abordan explícitamente el riesgo cibernético o la resistencia cibernética, los términos de las declaraciones principales, así como de las normas y directrices que lo acompañan abarcan todas las cuestiones que presentan estos riesgos. En consecuencia, los PBS proporcionan una base general para la supervisión del sector de seguros con respecto a la ciberseguridad. Además,

de conformidad con su mandato, en 2016-17 la FCTF investigará si - y en caso afirmativo, cómo - el PBS 21 debería ampliarse para abordar específicamente los elementos de la ciberseguridad.

92. Los Miembros de la IAIS tienen una gran diversidad y sofisticación en cuestiones relacionadas con el cibercrimen. Algunos supervisores de seguros han tomado medidas significativas para abordar la resistencia cibernética de las aseguradoras bajo su jurisdicción. Sin embargo, con base en los resultados de la encuesta de la IAIS 2015 sobre el riesgo cibernético, entre otras indicaciones existe una gran variación en el grado en que los supervisores priorizan el riesgo cibernético y las herramientas disponibles para abordar esos riesgos.

93. Dada la experiencia pasada y las tendencias pronosticadas, los riesgos cibernéticos y el impacto de los incidentes cibernéticos seguirán creciendo. Los supervisores deben tratar de aumentar su comprensión del riesgo cibernético y sus capacidades de supervisión en relación con la resistencia cibernética del sector de seguros. Este enfoque de supervisión podría incluir apropiadamente, pero no limitarse a, la conciencia de los aseguradores sobre el riesgo cibernético y la resistencia cibernética, y el desarrollo e implementación de políticas, procedimientos y tecnología por parte de los aseguradores para aumentar la resistencia cibernética. -parte conexiones sobre la resistencia cibernética.

94. La IAIS monitoreará iniciativas y asuntos relacionados con el riesgo cibernético a medida que éste continúa evolucionando. Otros materiales de apoyo de la IAIS que aborden las mejores prácticas de resistencia cibernética de acuerdo con los PBS pueden ser útiles para los supervisores y las aseguradoras. A este respecto, de conformidad con su mandato, la FCTF recomienda que la IAIS considere la posibilidad de seguir desarrollando este Documento Temático, con uno o más documentos de aplicación que exploren más a fondo estos temas. Las orientaciones para los supervisores en materia de ciberseguridad serían útiles para las siguientes facetas del sector de los seguros: 1) prácticas de examen para los supervisores; Y (2) prácticas de gestión de riesgos para los aseguradores.

Anexo I Resúmen de las respuestas de la Encuesta de la IAIS

Durante el período de enero a febrero de 2015, la FCTF realizó una encuesta a los Miembros de la IAIS sobre el tema del delito cibernético. La encuesta tenía por objeto ayudar al Equipo de Tareas a comprender la percepción de los miembros sobre estos riesgos, su participación en la lucha contra las amenazas cibernéticas y los enfoques de supervisión que se utilizan o están desarrollandose en esta esfera. Aproximadamente 30 miembros respondieron. Esta sección presenta los principales puntos de las respuestas, establecidos de acuerdo con los temas principales de la encuesta.

Contexto normativo y de supervisión

i) El riesgo cibernético se considera dentro del ámbito del riesgo operacional y se aborda dentro del marco regulatorio de la TI, ya sea a través de directrices de riesgo operacional o estándares especificados de TI. En general, los encuestados consideran que las amenazas cibernéticas están aumentando dentro de su jurisdicción. Sin embargo, la mayoría no percibió que la resistencia cibernética fuera una prioridad regulatoria. Algunos de los factores para no dar prioridad a la resistencia cibernética incluyen la etapa actual de desarrollo de su propio sector de seguros, la falta de un marco regulatorio y la confianza en las autoevaluaciones de los aseguradores.

Expectativas de Supervisión

ii) Algunas autoridades proporcionaron retroalimentación suponindo que sus marcos regulatorios a actualizarse en un futuro próximo ya están en vigor; mientras que otros describen cómo sus marcos regulatorios que ya abordan el riesgo operacional o el de TI, pueden abordar el riesgo cibernético. En general, la mayoría de los encuestados esperan incluir los requisitos de gobernanza dentro de su propio marco cibernético, particularmente en lo que respecta a las funciones en relación con las tres líneas de defensa.[63] Sin embargo, las respuestas en otras áreas, como el monitoreo de incidentes cibernéticos, o la capacitación y concientización del personal, hacen dudar si estas áreas se están abordando dentro del marco cibernético de la reglamentación.

iii) Por ejemplo, mientras que más de la mitad de los encuestados indicaron que supervisan al asegurador, incluyendo sus entregables y planes de acción, para remediar las causas de los incidentes cibernéticos, otros indicaron que no tienen un marco específico para monitorear los proyectos que abordan incidentes cibernéticos. Algunas autoridades, sin embargo, indicaron que si identifican las debilidades de un asegurador al tratar con un incidente cibernético, durante una visita in situ o en otras ocasiones, evaluarán y monitorearán las acciones de seguimiento del asegurador para abordar esas debilidades y sus desarrollos.

[63] Las prácticas comúnmente observadas en el sector de la gobernanza del riesgo sólido a menudo se basan en tres líneas de defensa: (i) gestión de la línea de negocio, (ii) una función independiente de gestión de riesgos operativos corporativos y (iii) una revisión de auditoría independiente. Por ejemplo, véase Comité de Supervisión Bancaria de Basilea, Buenas Prácticas para la Gestión y Supervisión del Riesgo Operacional (junio de 2011).

Revisión y evaluación supervisora

iv) Algunos encuestados no contaban con personal específicamente dedicado a la vigilancia de la ciberseguridad, mientras que algunos habían experimentado equipos de especialistas en TI que continuamente recibían capacitación sobre cuestiones de ciberseguridad. Entre estos extremos, la mayoría de los encuestados parecían tener limitaciones en el número de funcionarios responsables de la vigilancia de la seguridad cibernética.

Gobernanza

v) Dos tercios de los encuestados informaron que ellos verifican si se producen informes periódicos a la Junta y a la Alta Dirección sobre el riesgo cibernético y las evaluaciones de control. La misma proporción informó que verifican la validación de la función de auditoría del marco de seguridad cibernética. Un poco más de la mitad de los encuestados confirmaron que los supervisores revisan la alineación de la gestión del riesgo cibernético con la estrategia organizacional.

Ambiente de Control de Riesgos Cibernéticos

vi) La mitad de los encuestados parecían contar con disposiciones reglamentarias y prácticas de supervisión para evaluar el entorno de control de riesgos cibernéticos de los aseguradores. Sin embargo, muchos de ellos no han definido disposiciones específicas sobre ciberseguridad, sino que han seguido las amenazas cibernéticas mediante actividades de gestión de riesgos y, en particular, mediante evaluaciones de riesgos de TI. Algunos encuestados basaron sus respuestas en informes de auditoría periódicos para supervisar la vigilancia de la seguridad cibernética de los aseguradores, mientras que otros incluyen disposiciones sobre ciberseguridad como parte de los requisitos de licencias.

Gestión de riesgos de amenazas y vulnerabilidades

vii) Un tercio de los encuestados indicó claramente que evalúan la gestión del riesgo cibernético por parte de los aseguradores, incluido el uso de herramientas de seguridad de software por parte de los aseguradores. Alrededor de la misma proporción confirmaron que se mantienen al día con los últimos acontecimientos en la gestión del riesgo cibernético. Para aquellos que no siguen estas prácticas, algunos indicaron que sólo esperan ser informados cuando los aseguradores están sujetos a amenazas cibernéticas importantes, mientras que otros se basan en los informes de auditoría interna de los aseguradores apoyados por conclusiones de especialistas externos en TI.

Abordar los incidentes de ciberseguridad

viii) Más de dos tercios de los encuestados no tienen requisitos específicos para notificar a las autoridades de incidentes cibernéticos. Sin embargo, algunas autoridades esperan ser informadas por los aseguradores de cualquier incidente que tenga un impacto significativo en los asegurados bajo los requisitos reglamentarios para proteger la información personal o con respecto a los principales incidentes de riesgo operacional, o esperan ser informados por otra agencia gubernamental responsable de la información Protección en general, pero no directamente reportados por los aseguradores. Existe claramente un margen para seguir desarrollando la recolección de estadísticas sobre el número de incidentes de ciberseguridad.

ix) Además, más de la mitad de los encuestados indicaron que supervisan cómo un asegurador realiza un seguimiento de un incidente cibernético, incluyendo sus entregables y planes de acción, para remediar las causas de orígen de los incidentes cibernéticos. Otros indicaron que si identifican cualquier debilidad de una aseguradora al tratar con un incidente cibernético a través de una visita in situ, evaluarán y monitorearán las acciones de seguimiento de la aseguradora para abordar las debilidades.

x) Además, con respecto a la continuidad de los negocios relacionados con incidentes cibernéticos, una gran mayoría de los encuestados indicaron que evaluaban la efectividad de los planes de continuidad de negocio de los aseguradores después de un incidente cibernético. Los enfoques varían entre los encuestados. Varios consideran un plan de continuidad de negocio o un marco de gestión de crisis desde una perspectiva más amplia donde la resistencia cibernética es parte del plan o marco.

Medidas de Supervisión

xi) Aunque la mayoría de los encuestados indicó que no existe un requisito reglamentario que se refiera específicamente al riesgo cibernético, la mayoría de ellos indicó que hay una serie de medidas de supervisión disponibles. Estos incluyeron una carta de advertencia, una solicitud de reporte adicional, un plan de remediación, multa o suspensión de negocios. Más de la mitad de los encuestados informaron no haber utilizado medidas de supervisión para hacer frente a las debilidades y deficiencias en las prácticas de seguridad cibernética de los aseguradores, en los últimos cinco años.

Enfoques de supervisión y otras iniciativas para abordar el riesgo cibernético

xii) Los enfoques de supervisión varían por una serie de razones, incluida la prioridad dada a las iniciativas de seguridad cibernética en comparación con otras categorías de riesgo. Los enfoques de supervisión también varían en función del nivel de madurez de las infraestructuras de TI y de telecomunicaciones de los aseguradores. Cabe señalar que las directrices y otros documentos a que se hace referencia en esta sección se consideran de beneficio potencial para la mayoría de las jurisdicciones, aunque podría haber otros de nivel similar o incluso mejor de detalle y claridad. Teniendo esto en cuenta, los enfoques observados se han subdividido en las siguientes secciones:

xiii) Cumplimiento de las normas. Los resultados de la encuesta indicaron claramente que la mayoría de las jurisdicciones asocian la ciberseguridad con el cumplimiento de las normas. Aunque las prácticas de ciberseguridad están en constante evolución, ciertas normas son pertinentes y aplicables a la mayoría de las organizaciones. Una norma de este tipo es la norma ISO 27001, una norma internacional con el objetivo de proporcionar requisitos para una gestión racional de la seguridad de los sistemas de información.[64] Más específicamente relacionado con la ciberseguridad es el "marco para mejorar la infraestructura crítica" publicado por el Instituto Nacional de Estándares y Tecnología)[65], que se centra en utilizar los impulsores empresariales para guiar las

[64] Organización Internacional de Normalización, ISO / IEC 27001 - Gestión de la Seguridad de la Información.
[65] NIST, Marco para mejorar la seguridad cibernética de las infraestructuras críticas.

actividades de seguridad cibernética y considera los riesgos de seguridad cibernética como parte de los procesos de gestión de riesgos de una organización.

xiv) Directrices e inspecciones in situ. Algunos encuestados señalaron haber publicado directrices específicas para la ciberseguridad. Por ejemplo, la NAIC de los Estados Unidos ha publicado principios para una orientación normativa efectiva específica para la industria de seguros. En otros casos, las directrices se han concebido para ser aplicables a todo tipo de organizaciones, como el sistema "Cyber Essentials" del Reino Unido, mientras que otras son específicas de las instituciones financieras, como en el caso de la guía de autoevaluación cibernética del OSFI en Canadá , o la verificación de ciberresistencia de ASIC en Australia.

xv) Aún y cuando la mayoría de las jurisdicciones sólo han desarrollado documentos sobre mejores prácticas, algunas jurisdicciones ya están en proceso de implementar marcos de examen actualizados, como el desarrollado por el Departamento de Servicios Financieros del Estado de Nueva York.

Anexo II Glosario de términos

Las definiciones de algunos de los términos clave utilizados en el documento son las siguientes:[66]

Ataque cibernetico

Intenta dañar, interrumpir u obtener acceso no autorizado a una computadora, sistema informático o red de comunicaciones electrónicas. Un ataque, a través del ciberespacio, dirigido al uso del espacio cibernético de una empresa con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura de computación; o destruir la integridad de los datos o robar información controlada.[67]

Incidente cibernético

Medidas adoptadas mediante el uso de redes informáticas que tengan como consecuencia un efecto real o potencialmente adverso sobre un sistema de información o la información que en él se encuentre.[68]

Riesgo cibernético

Cualquier riesgo que emane del uso de datos electrónicos y su transmisión, incluyendo herramientas tecnológicas como Internet y redes de telecomunicaciones. También abarca los daños físicos que pueden ser causados por incidentes de ciberseguridad, fraude cometido por mal uso de datos, cualquier responsabilidad derivada del almacenamiento de datos, y la disponibilidad, integridad y

[66] Al proporcionar estas definiciones, se reconoce que hay una estandarización limitada y por lo tanto se pueden encontrar definiciones alternativas para algunos términos en otras fuentes.
[67] Consejo de Examen de las Instituciones Financieras Federales (FFIEC), Glosario de la Herramienta de Evaluación de la Seguridad Cibernética (junio de 2015), disponible en http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf.
[68] Ibid

confidencialidad de la información electrónica - esté relacionada con individuos, compañías o gobiernos.[69]

Resistencia cibernética

La capacidad de anticipar, soportar, contener y recuperarse rápidamente de un ataque cibernético.[70]

Seguridad cibernética

El término se refiere a estrategias, políticas y estándares que abarcan toda la gama de reducción de amenazas, reducción de la vulnerabilidad, disuasión, compromiso internacional, respuesta a incidentes, resistencia, actividades de recuperación, y políticas relacionadas con la seguridad de las operaciones de una aseguradora.[71]

Incidente de ciberseguridad

En este documento, la frase "incidente de ciberseguridad" se utiliza generalmente para capturar tanto los ataques cibernéticos como los incidentes cibernéticos.

Amenaza cibernética

Una circunstancia o evento con el potencial de explotar, intencionalmente o no, una o más vulnerabilidades del sistema resultando en una pérdida de confidencialidad, integridad o disponibilidad.[72]

Violaciones de datos

Las violaciones de seguridad en las que los datos confidenciales son copiados, transmitidos, vistos, robados o utilizados por una persona no autorizada para hacerlo.[73]

Malware

El malware está diseñado para acceder secretamente a un sistema informático sin el consentimiento informado del propietario. La expresión es un término general (abreviación de software malicioso) que se utiliza para designar una variedad de formas de software o código de programa hostil, intrusivo o molesto. El malware incluye virus informáticos, gusanos, troyanos, spyware, adware

[69] CRO Forum, The Cyber Risk Challenge and the Role of Insurance (December 2014), disponible en http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/.
[70] Comité sobre Pagos e Infraestructuras de Mercado y Organización Internacional de Comisiones de Valores, Orientación sobre la Resistencia Cibernética para las Infraestructuras de los Mercados Financieros (junio de 2016), disponible en http://www.bis.org/cpmi/publ/d146.htm.
[71] Comité de Pagos e Infraestructuras de Mercado, Resistencia Cibernética en Infraestructuras de Mercados Financieros (noviembre de 2014), disponible en http://www.bis.org/cpmi/publ/d122.pdf. De acuerdo con la definición utilizada en el glosario.
[72] Ibídem. De acuerdo con la definición utilizada en el glosario.
[73] Departamento de Salud y Servicios Humanos de los Estados Unidos, Administración de Niños y Familias, Memorando de Información: ACYF-CB-IM-15-04 (1 de julio de 2015), disponible en http://www.acf.hhs.gov/sites/default /files/cb/im1504.pdf.

deshonesto, ransomware, crimeware, la mayoría de los rootkits y otros programas o programas malintencionados o no deseados.[74]

Marco NIST

Instituto Nacional de Estándares y Tecnología, Marco para mejorar la seguridad cibernética de las infraestructuras críticas, febrero de 2014.[75]

Anexo III Lectura adicional

Atlantic Council and Zurich Insurance Group, Risk Nexux – Beyond Data Breaches: Global Interconnections of Cyber Risk (April 2014), disponible en http://www.atlanticcouncil.org/publications/reports/beyond-data-breaches-global-interconnections-of-cyber-risk.

Atlantic Council, Frederick S. Pardee Center for International Futures and Zurich Insurance Group, Risk Nexus - Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures (September 2015), disponible en http://publications.atlanticcouncil.org/cyberrisks/.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, Principles for Financial Market Infrastructures: Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers (December 2014), disponible en http://www.bis.org/cpmi/publ/d123.htm.

Council of Europe, Convention on Cybercrime (November 2001), disponible en http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Deborah Bodeau and Richard Graubart, “Cyber Resiliency Assessment: Enabling Architectural Improvement,” MITRE Technical Report MTR120407 (May 2013), disponible en http://www.mitre.org/publications/technical-papers/cyber-resiliency-assessment-enabling-architectural-improvement.

European Commission, “Cyber Security,” Special Eurobarometer 390 (July 2012), disponible en http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

Angelia Herrin, “Meeting the Cyber Risk Challenge,” Harvard Business Review (27 November 2012), disponible en https://hbr.org/webinar/2012/12/meeting-the-cyber-risk-challen.

International Cyber Security Protection Alliance, “Project 2020 -Scenarios for the Future of Cybercrime,” disponible en https://www.icspa.org/wp-content/uploads/2015/03/ICSPA_Project_2020_-_Scenarios_for_the_Future_of_Cybercrime.pdf.

International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, Broadband Commission for Digital Development, The State of Broadband 2012:

[74] FFIEC, Glosario de la Herramienta de Evaluación de la Seguridad Cibernética.

[75] Disponible en http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Achieving Digital Inclusion for All (September 2012), disponible en http://broadbandcommission.org/documents/bb-annualreport2012.pdf.

International Telecommunication Union, “Cybersecurity Guide for Developing Countries,” disponible en http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf.

International Organization for Standardization, ISO 31000: 2009, Risk management -- Principles and guidelines (November 2009), disponible en http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170.

- ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management (June 2011), disponible en http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742.

- ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity (July 2012), disponible en http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375.

- ISO/IEC 27000:2016, Information technology - Security techniques -- Information security management systems - Overview and vocabulary (February 2016), disponible en http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435.

International Organization of Securities Commissions, Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity, (December 2015), disponible en http://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf.

Information Systems Audit and Control Association, Control Objectives for Information and Related Technology, disponible en http://www.isaca.org/COBIT/Pages/default.aspx.

Organisation for Economic Co-operation and Development, Future Global Shocks, Improving Risk Governance (September 2011), disponible en http://www.oecd.org/governance/48329024.pdf.

- Cybersecurity Policy Making at a Turning Point, Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy (2012), disponible en http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

- The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines (April 2011), disponible en http://www.oecd-ilibrary.org/science-and-technology/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy-guidelines_5kgf09z90c31-en.

- “Information security and privacy,” disponible en http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm.

Rohini Tendulkar, “Cyber-crime, securities markets and systemic risk,” Joint Staff Working Paper, International Organization of Securities Commissions Research Department and World Federation of Exchanges, (July 2013), disponible en http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.

SANS Institute, CIS Critical Security Controls - Version 6.0 (January 2013), disponible en http://www.sans.org/critical-security-controls/.

Securities Industry and Financial Markets Association, Principles for Effective Cybersecurity Regulatory Guidance (October 2014), disponible en http://www.sifma.org/issues/item.aspx?id=8589951691.

UK National Computer Emergency Response Team, Cyber-security Risks in the Supply Chain (February 2015), disponible en https://www.cert.gov.uk/resources/best-practices/cyber-security-risks-in-the-supply-chain/.

United Nations, Creation of a Global Culture of Cybersecurity, Resolution 57/239 adopted by the General Assembly (January 2003), disponible en http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

United Nations Office on Drugs and Crime, Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector (February 2013), disponible en http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

U.S. Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity (October 2011), disponible en https://www.sec.gov/divisions/corpfin/cfdisclosure.shtml.

World Economic Forum, Building Resilience in Supply Chains (January 2013), disponible en http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.

- Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience (May 2012), disponible en http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.

- Partnering for Cyber Resilience – Towards the Quantification of Cyber Threats (January 2015), disponible en http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.