Recuadro. Gestión de la SFC coordinando el Sub-Grupo de Trabajo de Ciberseguridad de la Alianza del Pacífico

Introducción

La Alianza del Pacífico (AP) se constituyó como un mecanismo para fortalecer el desarrollo, la articulación política, económica, la cooperación e integración, con el propósito de impulsar el crecimiento y la competitividad de las cuatro economías que la integran: Chile, Colombia, México y Perú. Cada año los presidentes de los países revisan y actualizan los mandatos o lineamientos en materia de integración financiera, innovación y digitalización financiera, manejo de riesgos catastróficos y ciberseguridad, entre otros temas, sobre los cuales se deben formular y desarrollar iniciativas que contribuyan al logro de los objetivos planteados. La presidencia de la AP se rota cada año entre los países miembros.

En 2021 Colombia ejerció la Presidencia Pro Tempore (PPT) de la AP y la Superintendencia Financiera de Colombia asumió la coordinación del Sub-Grupo de Trabajo de Ciberseguridad (SGT-CS), constituido con el propósito de fortalecer la seguridad cibernética de los sistemas financieros y mercados de capitales de los países miembros de la AP. Durante la gestión de la Superintendencia se desarrollaron cinco iniciativas.

1. Guía para la gestión de incidentes en arquitectura Cloud.

La computación en la nube es una de las tecnologías de más rápida adopción en los últimos años por parte de todo tipo de entidades, en particular, las financieras, y su uso conlleva beneficios, pero también desafíos para su adecuada administración. Gestionar la seguridad en este ambiente, que interactúa con plataformas locales, ampliando el tamaño y la complejidad de la infraestructura de las organizaciones, requiere de especialistas en la materia y de metodologías que contemplen sus particularidades.

El reto al que se ven enfrentadas las entidades usuarias de la nube también lo tienen los supervisores, que necesitan ingenieros especializados y herramientas que orienten sus labores. Por tal razón, y partiendo del contexto de cada jurisdicción sobre el uso de la nube, la gestión de los supervisores en la evaluación de los incidentes cibernéticos y la regulación expedida sobre la materia, se desarrolló la "Guía de supervisión de incidentes en arquitecturas *Cloud*", que facilita la evaluación de los protocolos de gestión de las entidades vigiladas y su efectividad.

2. Simulación de incidentes cibernéticos.

La acelerada transformación digital que el sector financiero está experimentando, gracias a los desarrollos tecnológicos y a las nuevas exigencias del consumidor financiero, ha aumentado la superficie de exposición de las entidades a incidentes cibernéticos relacionados con campañas de *phishing*, ataques a la cadena de suministro, ataques de ingeniería social, *ramsomware*, entre otros.

Para hacerle frente a esta situación las entidades financieras han adoptado sistemas de gestión de la seguridad de la información y la ciberseguridad, cuentan con equipos especializados y el apoyo de terceros expertos en la materia, han implementado diferentes herramientas para fortalecer la gestión y realizan simulacros internos para hacerle frente a posibles incidentes cibernéticos. Sin embargo, para consolidar este ambiente de control es necesario realizar ejercicios que simulen ataques simultáneos a diferentes entidades y evaluar la manera como el sistema financiero se articula con otros agentes, como las superintendencias, los organismos nacionales

encargados de la seguridad digital, los ministerios de finanzas, los medios de comunicación y los consumidores financieros, entre otros grupos de interés.

Para contribuir con el cumplimiento de este objetivo y con el apoyo del Banco Interamericano de Desarrollo (BID), se adelantó la selección de una firma especializada que diseñará y liderará un ejercicio en cada uno los países de la AP, para evaluar el grado de coordinación del sector bancario de cada país con otras entidades o grupos de interés de su jurisdicción, en la atención de incidentes cibernéticos, identificando oportunidades de mejora. Los ejercicios se desarrollarán en 2022.

3. Plataforma única para el reporte de incidentes cibernéticos.

Las amenazas cibernéticas son cada vez más complejas y por lo tanto más difíciles de gestionar. El intercambio de información y el trabajo conjunto entre las entidades de supervisión, los equipos de respuesta de las entidades financieras y de los distintos CERT/CSIRT, facilitan la generación de una inteligencia global que mejora la capacidad de actuar de forma preventiva.

Para ello, es necesario que los entes públicos y privados establezcan mecanismos que faciliten la coordinación y cooperación entre los distintos actores promoviendo el intercambio, la recopilación, el almacenamiento y la distribución de la información necesaria para actuar de forma rápida y eficaz contra las ciber-amenazas, generando un conocimiento común. Aunque es clara la conveniencia de compartir información, normalmente considerada de alta confidencialidad, es necesario superar la desconfianza, fijar criterios para anonimizarla, adoptar estándares para el intercambio y armonizar la legislación a nivel internacional.

Para contribuir con este objetivo, con el apoyo del BID, se elaboraron los términos de referencia para contratar o desarrollar una “Plataforma Única para el Reporte de Incidentes Cibernéticos e Intercambio de Información”, que contempla los requisitos funcionales, técnicos y operativos.

Adicionalmente, se realizó un análisis comparativo de las plataformas existentes en el mercado, que se podrían usar para tal propósito. Considerando los requerimientos identificados; se planteó la arquitectura de la plataforma y se presentó una propuesta de acuerdos para el intercambio de información entre las entidades de los países miembros.

Esta iniciativa continuará durante la PPT de México en 2022.

4. Metodología para identificar infraestructuras críticas cibernéticas.

Un aspecto importante de la seguridad nacional y la defensa de un país es garantizar una alta disponibilidad de la infraestructura crítica empleada para la prestación de los servicios esenciales, por lo tanto, es necesario identificar, catalogar y priorizar la Infraestructura Crítica Cibernética (ICC) para formular políticas y estrategias para su protección.

La infraestructura crítica de un país incluye empresas de energía, transporte, bancos y pagos, telecomunicaciones, alimentos, atención médica, servicios públicos, entre otras, que son estratégicamente importantes para el funcionamiento de la economía y la seguridad de la nación.

Las instituciones financieras, especialmente aquellas que puedan considerarse sistémicas y estratégicamente importantes, son consideradas parte de la infraestructura crítica del país.

Dada la variedad de los productos y servicios ofrecidos por los distintos tipos de instituciones financieras, no existe un enfoque metodológico universal para la identificación, clasificación y priorización de las que pueden considerarse ICC. De otra parte, cada entidad gestiona su sistema de seguridad de la información y ciberseguridad como un proyecto único, aplicable a dicha organización, sin considerarlo como parte de un ecosistema ni contemplar la

manera como debe interactuar con los sistemas de gestión de otras organizaciones.

Por tal razón, se desarrolló una metodología para que los países de la AP puedan identificar las entidades del sector financiero que se pueden considerar ICC, cuya afectación por incidentes cibernéticos puede poner en peligro el funcionamiento de los servicios esenciales. Estas entidades deberán contar con los más altos niveles de madurez en la gestión de la ciberseguridad y contar con el apoyo prioritario de los organismos de seguridad nacional para recuperar los servicios esenciales ante la ocurrencia de incidentes cibernéticos. Adicionalmente, se hizo un resumen del estado actual de los países de la AP en el desarrollo de estrategias nacionales de ciberseguridad y en la identificación, clasificación y priorización de sectores críticos nacionales.

5. Jornadas de capacitación y sensibilización.

La pandemia del COVID-19 aceleró la transformación digital en el sector financiero planteando un reto para las entidades que no estaban preparadas para gestionar la mayor parte de su operación en teletrabajo y prestar un mayor número de servicios de manera digital en forma acelerada. La adaptación a este nuevo ritmo implica cambios culturales en las organizaciones, inversiones, asumir una mayor competencia, atender consumidores más exigentes, afrontar ajustes en la regulación y una mayor presión para mejorar la eficiencia, entre otros factores.

Por estas razones y las planteadas en las otras iniciativas, es importante que los supervisores, la alta gerencia y las juntas directivas de las entidades financieras se mantengan actualizadas con las tendencias en materia de ciberseguridad.

Para contribuir a este objetivo, con el apoyo del BID, se realizaron dos eventos con panelistas expertos en la materia; uno orientado a fortalecer los conocimientos de los supervisores de la región, denominado “Encuentro AP-21: Supervisión a la Vanguardia en Ciberseguridad”, donde se presentó la evolución, técnicas y mecanismos de protección frente a los troyanos bancarios móviles; la importancia de la criptografía homomórfica, las amenazas y el riesgo de seguridad en la nube. El evento contó con la participación de más de 80 asistentes.

El segundo evento estuvo dirigido a la alta gerencia y la junta directiva de los establecimientos bancarios de los países de la AP denominado “Encuentro AP-21. Ciberseguridad: reflexiones de un riesgo sistémico, emergente y disruptivo”, donde se presentó el estado global del ciber riesgo y por qué la ciberseguridad es clave para una transformación digital sostenible, las macrotendencias para atender los riesgos emergentes de la era post Covid y las nuevas responsabilidades de las juntas directivas y la alta gerencia en la gestión del ciber riesgo y la ciber seguridad. El evento contó con la participación de más de 300 asistentes.

Conclusión

Las actividades desarrolladas por el SGT-CS en 2021, bajo la coordinación de la Superintendencia Financiera de Colombia, sin duda contribuirán a fortalecer la seguridad cibernética de los sistemas financieros y mercados de capitales de los países miembros de la AP.

La coordinación del SGT-CS continuará en 2022 bajo la PPT de México.