UNIVERSIDAD DE BUENOS AIRES

FACULTADES DE CIENCIAS ECONÓMICAS, CIENCIAS EXACTAS Y NATURALES E INGENIERÍA

CARRERA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO FINAL

ANÁLISIS DE LAS REGULACIONES DE CIBERSEGURIDAD PARA LA INDUSTRIA *FINTECH* DE LATINOAMÉRICA

AUTOR: LIC. ALAN ISAAC MESRI

TUTORA DEL TRABAJO FINAL: LIC. MARA MISTO MACÍAS

COHORTE 2019

Declaración jurada de contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

_____

Alan Isaac Mesri
DNI: 37.948.357

Agradecimientos

A mis padres, José y Karina, y a mi hermano, Joan, por apoyarme en todo lo que hago.

A mis abuelos Isaac, Alegra, Leonardo y Clara, por su cariño infinito.

A mi tutora, Mara Misto Macías, y al coordinador del posgrado, Pedro Hecht, quienes fueron una guía indispensable para la confección de este trabajo.

Resumen

El presente trabajo se propone analizar y comparar los marcos regulatorios para las compañías fintech de América Latina en relación a la seguridad de la información, haciendo foco en Brasil, Chile y México. Se analizará la industria para comprender su importancia y el impacto que un potencial problema de seguridad de la información podría tener en la vida del usuario financiero y se revisarán sus leyes y las regulaciones de sus respectivos Bancos Centrales, así como también el análisis de bibliografía relacionada. Posteriormente, se analizaran posibles implementaciones en la República Argentina.

Durante el desarrollo de este trabajo se hará hincapié en la gestión de los riesgos, la gestión de las terceras partes y la gestión de incidentes y se describirá la importancia y el impacto de una buena gestión en estas tres áreas en el mundo Fintech. Se analizarán los requisitos que una compañía Fintech precisa para lograr un nivel de cumplimiento adecuado en estas áreas en función de las regulaciones locales de cada país mencionado.

En la conclusión se brindará una opinión sobre las normas vigentes en los países analizados y se sugerirán actualizaciones o modificaciones, al mismo tiempo que se establecerán paralelismos para comparar la coyuntura en la República Argentina con el objeto de sugerir aportes a la legislación local.

Palabras Clave: Fintech, Regulaciones, Ciberseguridad

Tabla de contenidos

Tabla de Ilustraciones

Nómina de abreviaturas

Bacen: Banco Central Del Brasil.

BCRA*: Banco Central de la República Argentina*

ARR*: Actividades de Recuperación y Respuesta*

Bigtech*: Compañías más grandes y dominantes en la industria de las tecnologías de la información*

CMBV*: Comisión Nacional Bancaria y de Valores de México*

CMF: Comisión para el Mercado Financiero de Chile

Fintech*: Financial Technology*

FSB*: Financial Stability Board*

Iaas: *Infrastructure As a Service*

Insurtech*: Insurance Technology*

PaaS: *Platform as a Service*

PCI-DSS*: Payment Card Industry – Data Security Standard*

RAN*: Recopilación Actualizada de Normas*

SaaS: *Software as a Service*

SBIF*: Superintendencia de Bancos e Instituciones Financieras de Chile*

Introducción

La industria *FinTech* (del inglés *Financial Technology*) está comprendida por aquellas compañías que aplican las nuevas tecnologías a actividades financieras y de inversión de activos. Las *FinTech* están marcando una nueva era en la evolución de los servicios financieros y sirven de tierra fértil para la innovación, tanto para las grandes empresas como para los nuevos emprendimientos que están comenzando a ofrecer servicios y productos financieros con enfoques claramente disruptivos respecto de los proveedores tradicionales.

La seguridad de la información en las *FinTech* es un asunto de extrema seriedad dado el potencial impacto de un incidente sobre la información de los usuarios, comprometiendo información financiera, su privacidad y su seguridad, además de, dependiendo del tamaño de la Fintech, poder provocar un potencial problema a la estabilidad financiera local.

En esta línea, la industria *FinTech* no debería estar ajena al control y aplicación de las regulaciones, en parte por ser un sector de la industria con una impronta distintiva que requiere toda la atención de las autoridades, quienes deberían emitir regulaciones especialmente diseñadas para aplicarse sobre este sector. Sin embargo, el nivel vertiginoso con el que estas compañías evolucionan -del cual depende gran parte de su éxito- hace extremadamente complicado para las agencias gubernamentales poder mantener un marco regulatorio constantemente actualizado.

En América Latina, países como Brasil, Colombia, Chile y México ya han hecho grandes avances en el largo camino de la regulación de las *FinTech* y dedican un espacio al cuidado de la seguridad de la información de éstas*,* mientras que la República Argentina, por otro lado, aún no ha desarrollado un marco regulatorio específico para esta clase de empresas.

A efectos de este trabajo, comenzaremos haciendo un análisis sobre la industria Fintech en el mundo en general y en América Latina en particular, para luego enfocar el alcance de nuestro análisis en la gestión del riesgo, la gestión de las terceras partes y la gestión de incidentes, que, como se

desarrollará a lo largo del trabajo, son tres aspectos críticos para cualquier organización de base tecnológica y especialmente necesarias a la hora de manejar la resiliencia operativa.

1. ¿Qué son las Fintech?

Si bien es un término que comenzó a usarse hace unos 30 años, la palabra Fintech se popularizó durante la última década. El término *fintech* procedente de las palabras en inglés Finance and Technology, hace referencia a todas aquellas actividades que impliquen el empleo de la innovación y los desarrollos tecnológicos para el diseño, oferta y prestación de productos y servicios financiero Estos servicios pueden ser típicamente, servicios de pago, gestión de finanzas personales, financiación alternativa tal como, créditos online, financiación participativa (*crowdfunding*), gestión de criptoactivos, identificación online de usuarios billeteras electrónicas, entre otras categorías.

Las actividades realizadas por las fintech, al igual que las realizadas por las entidades tradicionales, tienen sus riesgos. De hecho, este tipo de empresas se enfrentan a riesgos específicos al utilizar tecnologías que pudieran no estar todavía suficientemente maduras o al ofrecer modelos de negocio disruptivos.

En las actividades realizadas por empresas fintech, es de suma importancia la seguridad de los datos almacenados de sus clientes. Por este motivo, estas empresas deben contar con las medidas de protección suficientes.

Si bien, los servicios prestados por estas instituciones resultan muy atractivos porque ofrecen entornos sencillos y fáciles de utilizar y en algunos casos simplifican la gestión de las finanzas personales, el uso de sus servicios debe ir acompañado del correspondiente conocimiento del servicio o producto que se desea contratar y de las ventajas y riesgos asociados al mismo. Los avances tecnológicos no deben considerarse como un sustituto de la educación financiera.

En efecto, el motor de estos servicios es el uso de la tecnología para facilitar la vida del usuario financiero, el objetivo es que cada usuario financiero

pueda realizar sus actividades de manera online, a través de su computadora, su celular o *Tablet*, ahorrando tiempo y esfuerzo en trámites presenciales de la manera mas sencilla posible. Es por eso que las Fintech suelen prescindir de sucursales de atención al público. [1]

Estas instituciones están creciendo a niveles vertiginosos generando niveles de innovación pocas veces vistos.

Para el año 2017, el 25% de las inversiones de capital de riesgo en el sector de Tecnologías de la Información en América Latina y el Caribe estuvo destinado a las Fintech. [2] Todo esto genera una disrupción que supone un gran desafío para la industria financiera tradicional, pues deberían adaptar sus productos y los servicios que ofrecen para mejorar la experiencia del usuario y la forma en la operan.

Este fenómeno mundial, en Latinoamérica tiene un pilar importante, dado que es específicamente en Argentina donde se originaron 5 de los 11 unicornios digitales latinoamericanos y es también Argentina el tercer país con mayor cantidad de Fintech de origen nacional, por detrás de México y Brasil.

2. ¿Por qué es importante que se protejan las Fintech?

Las actividades realizadas por las Fintech, se enfrentan a riesgos específicos al utilizar tecnologías que, en principio, pudieran no estar todavía suficientemente maduras o al ofrecer modelos de negocio disruptivos. Asimismo, esta expansión de los servicios implica también mayor uso de tecnología e interconexión de los servicios financieros, aumentando el campo de exposición a los ciberataques.

Según un relevamiento realizado en el año 2018, el 80% de las Fintech de América Latina y el Caribe identificaban a los ciberataques como una amenaza para su modelo de negocio. Al mismo tiempo, menos de la mitad (47%) tenían un plan de contingencia en caso de incidentes y el 32% tiene el objetivo de implementarlo en el futuro. Solo un 4% contaba con un seguro de ciberseguridad.

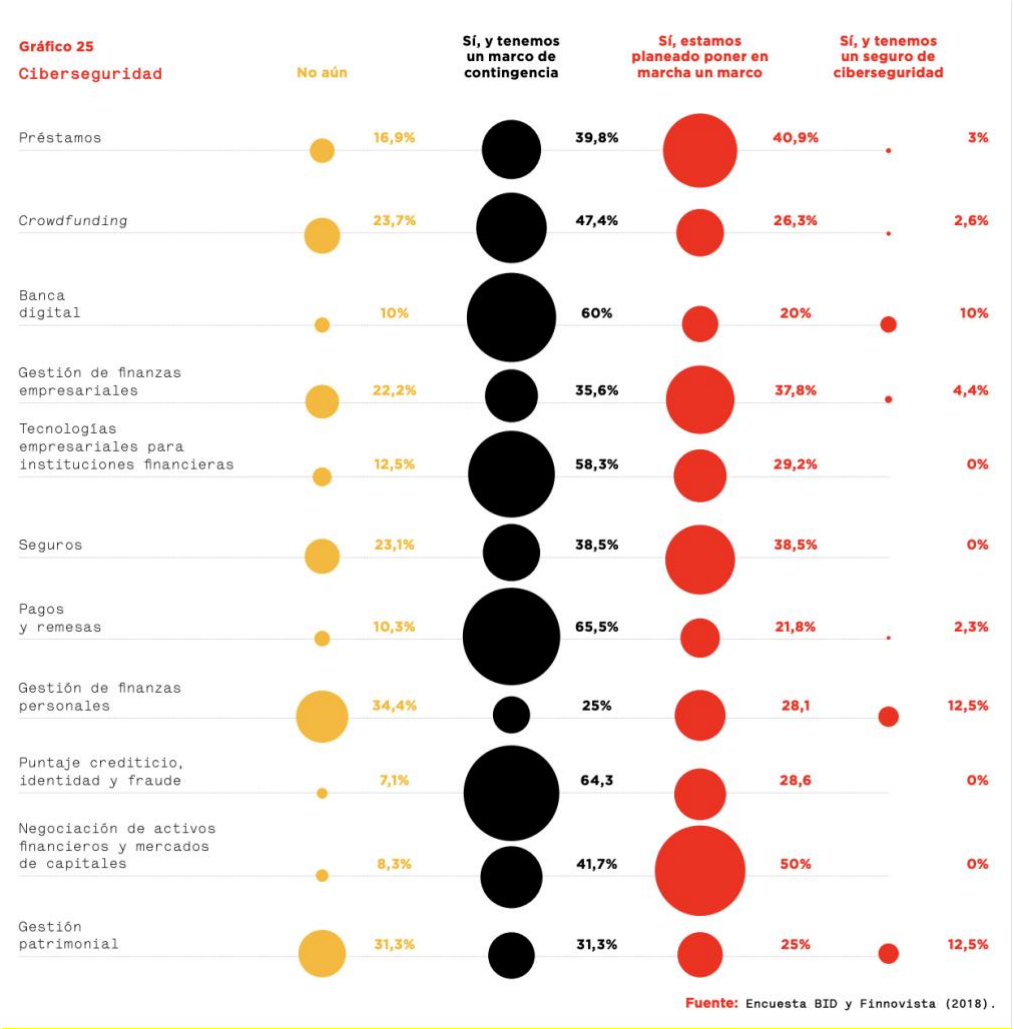

Ilustración 1 - Encuesta de BID y Finnovista

En la ilustración 1 se puede observar que la proporción de compañías Fintech con planes de contingencia en caso de incidentes es visiblemente más alta en los rubros de Pagos, Banca Digital y de Puntaje Crediticio, Identidad y Fraude, lo cual muestra un grado de preparación mayor, al menos en este aspecto, frente a otros rubros como el de seguros, gestión de patrimonio o de finanzas personales.

Estos datos no son menores, más aun teniendo en cuenta la cantidad de dinero que los usuarios confían en estos servicios, la visible tendencia a continuar haciéndolo y la inmensa cantidad de datos personales que manejan.

También se debe tener en cuenta la interdependencia que hay entre diferentes compañías Fintech con otros sectores de la economía. Durante un relevamiento publicado por Deloitte en el año 2018 se les consultó a las compañías Fintech en Argentina sobre los servicios que

prestaban o recibían con otras compañías, los resultados fueron los siguientes:

Un 50% prestaba o recibía servicios con otras Fintech

Un 48% prestaba o recibía servicios con bancos y aseguradoras

Un 19% prestaba o recibía servicios con instituciones gubernamentales

Un 13% prestaba o recibía servicios con instituciones educativas

Estos datos son cruciales, pues sabemos que uno de los mayores riesgos de estos servicios financieros es su interconexión, lo que produce que cualquier vulnerabilidad de cualquier compañía Fintech, de explotarse, pueda eventualmente impactar en las instituciones relacionadas con ésta.

A todo esto, es menester resaltar que la mayoría de las compañías Fintech son relativamente nuevas y muchas aún tienen una infraestructura de IT que probablemente no tenga la madurez necesaria en los procesos de seguridad que permitan mitigar los riesgos que afectan a su información y servicios críticos.

Por otra parte, no se debe dejar de lado la cantidad de puestos de trabajo que genera esta industria. Este mismo relevamiento detectó que el 80% de las compañías estudiadas tenían pensado aumentar su plantilla en el corto plazo. Es cierto que muchas de estas empresas aún son calificadas como Pymes, pero se debe resaltar que con el aumento rápido que tiene este rubro, viene también un aumento de la demanda de fuerza de trabajo [2]. Si un ciberincidente impactara en este tipo de institución y la empresa no esta lista para abordarlo adecuadamente, podría afectar gravemente a la reputación de la misma, provocándole graves daños.

No cabe duda de que estamos hablando de una industria con gran impacto en la sociedad, tanto por el tipo de información que maneja como por los sectores de la economía con los que está interrelacionado. por lo que sería importante contar con un marco regulatorio que contribuya a brindar una seguridad adecuada en la confidencialidad, integridad y disponibilidad de la información que estas entidades manejan, a fin de proteger los datos de todos los

usuarios financieros y sus propios datos. Según un reporte realizado en 2019 por IBM, [4], una fuga de información en el sector financiero puede generar pérdidas que promedian los 5.5 millones de dólares, aunque este valor mostraba grandes variaciones en diferentes partes del mundo. Brasil -único país latinoamericano relevado- mostraba un promedio de pérdidas por 2.2 millones de dólares en fugas de información en el sector financiero, siendo importante destacar que este valor es de todos modos importante, sobre todo teniendo en cuenta el poder adquisitivo del dólar, que es mayor en América Latina en relación con resto del mundo. Pérdidas como estas pueden significar el cese de operaciones para muchos pequeños *startups* que componen el mundo Fintech.

Otro punto interesante es que tan sólo en 2019 más de U$D110 mil millones fueron invertidos en compañías Fintech en el continente asiático. Si bien la industria en América Latina se encuentra en un estadio más temprano, esto nos sirve para ver hasta qué punto se está valorando esta industria en el mundo de los negocios y la cantidad de dinero que los inversores le confían . [3]

También, podemos ver el impacto que este sector de la economía puede tener en otros ámbitos. Por ejemplo, de la industria de los seguros, que comenzó a tener una interacción cada vez más fuerte con las Fintech en los últimos años, proporcionando plataforma de pagos más ágiles, servicios para el análisis de datos y prevención del fraude, entre otras cosas. Un problema en las Fintech relacionadas a esta industria pueden generar serios inconvenientes en materia de eficiencia, disponibilidad de servicio, costos y experiencia del usuario. [4]

En el siguiente gráfico se puede ver la inversión en millones de dólares que recibió la industria de seguros con base tecnológica (también conocida como *insurtech*) en comparación con las industrias fintech de pagos y de mercado de capitales, según el CB Insights Report [5].

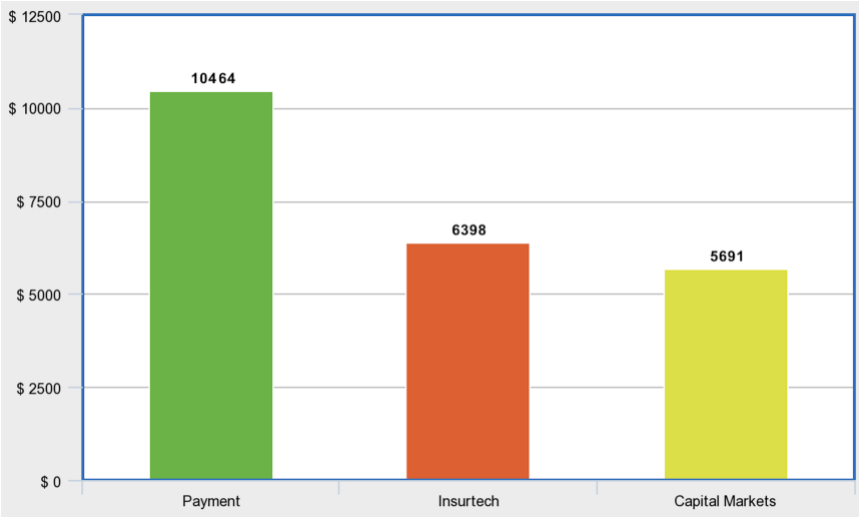

Ilustración 2 - Inversiones en Fintech según el CB Insight Report - 2019

Luego, según el mismo reporte del año 2020 vemos que para junio de ese año la inversiones (donde se agrega la categoría “banking”, no incluida en 2019) fueron las siguientes [6]:

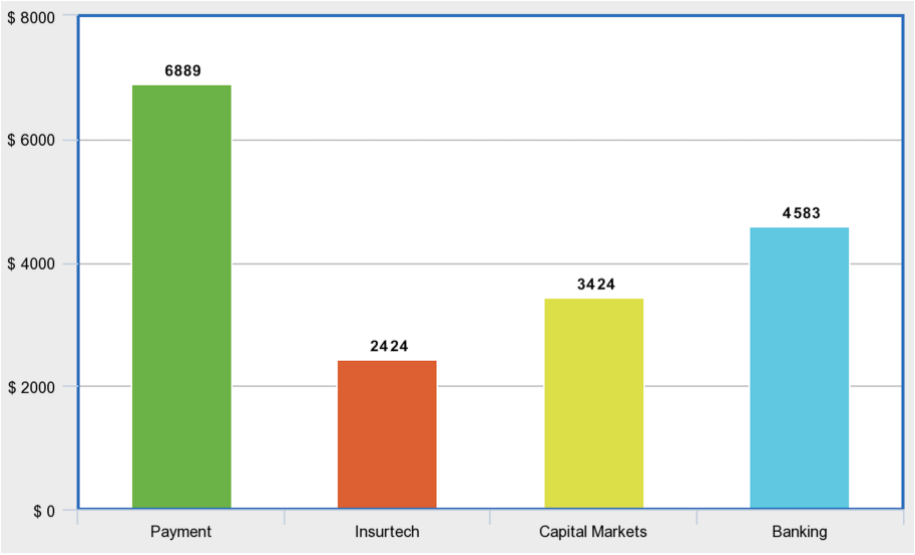

Ilustración 3 - Inversiones en Fintech según el CB Insight Report - 2020

Estos datos tienen el objeto de ilustrar el nivel de confianza que los inversores depositan en estas industrias y la manera en la que un problema en el mundo de las fintech puede comprometer enormes capitales. En este sentido es menester recordar también que las fintech representan una gran parte del crecimiento y de la innovación tecnológica, comprendiendo a 66 unicornios (empresas valuadas en más de mil millones de dólares) a nivel mundial y valuadas en su

conjunto por más de U$D248 mil millones, siendo esta tendencia creciente.

En la industria de los medios de pago, también conocida como *payments systems*, la más pujante y atractiva para los inversores, se está acelerando con rapidez la financiación de los grandes interesados, como se ve en el siguiente gráfico:

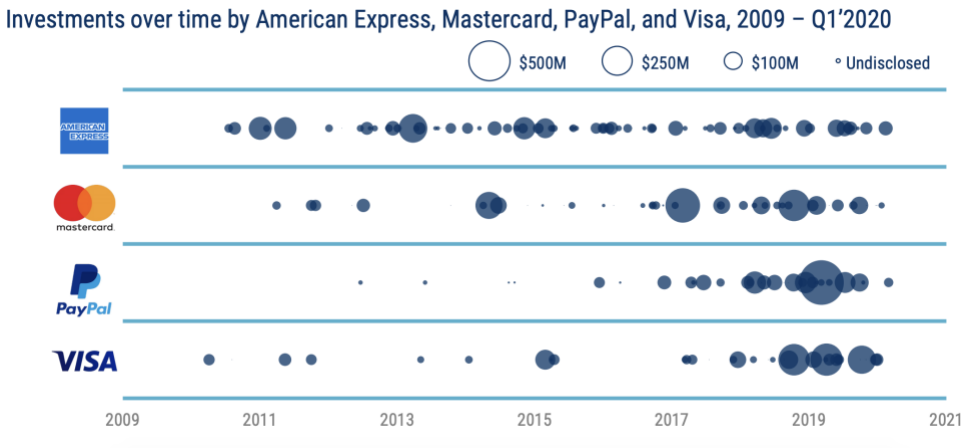

Ilustración 4 - Inversiones de las principales empresas de medios de pago en Q1'2020 [5]

Todo esto sin mencionar el creciente interés de empresas conocidas como *Bigtechs* en asumir iniciativas relativas a los medios de pagos digitales, generando productos como Whatsapp Pay, Facebook Pay, Amazon Pay, Apple Pay y Google Pay.

Por último, como consecuencia de la pandemia de Covid-19 que afectó la vida cotidiana de prácticamente todas las personas que viven en áreas urbanas alrededor del mundo, la facilidad que permiten los servicios fintech, especialmente los productos de *payment services*, implican facilidad y fluidez para que el usuario pueda realizar sus actividades cotidianas de forma segura y a distancia.

3. Algunas consideraciones previas

Es importante destacar que, en Brasil, si bien no existen normas diseñadas específicamente para regular la industria *Fintech*, sí las hay para instituciones financieras y para regular un sistema de banca abierta, lo que permitirá a las instituciones financieras compartir información sobre las transacciones de los usuarios, con previo

consentimiento de estos. Las empresas *Fintech* deben atenerse a estos lineamientos en tanto les sean aplicables.

Respecto de Chile, las normas que regulan las instituciones financieras no se aplican de manera automática a las empresas *Fintech*. Si bien todas las instituciones financieras necesitan una licencia de la CMF (Comisión para el Mercado Financiero) cuando representen una facturación anual superior al 1% de la industria nacional, para lo cual deben estar alineados a las regulaciones pertinentes, en el caso de las empresas *Fintech* la CMF les presenta un "Plan de Pruebas" que consta de una adaptación de las regulaciones para aquellas instituciones financieras que no estén contempladas en la norma. Esta adaptación mantiene el espíritu del texto original mientras sea posible, aunque puede variar en cada compañía.

En el caso de México, se promulgó en 2018 la Ley Para Regular Las Instituciones De Tecnología Financiera [7] (popularmente conocida como la "Ley Fintech"), en la cual en el artículo 48, segundo párrafo, expresa:

"Tratándose de instituciones de fondos de pago electrónico, la CNBV (Comisión Nacional Bancaria y de Valores) y el Banco de México emitirán conjuntamente disposiciones de carácter general en materia de seguridad de la información, incluyendo las políticas de confidencialidad y registro de cuentas sobre movimientos transaccionales, el uso de medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos y continuidad operativa. "

En este sentido, la CNBV ha emitido un conjunto de normativas bajo el título de "Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Financiera" [8] en la cual se establecen requerimientos que comprenden un gran espectro de asuntos relativos al rubro y entre los cuales se encuentra la seguridad de la información.

4. La gestión del riesgo

La gestión del riesgo existe desde que las compañías tienen activos para proteger. Tal vez el mejor ejemplo sean los seguros, ya sean de vida, de salud o de automóviles, estamos frente a un servicio que protege al cliente frente a potenciales daños. En este sentido la familia de normas ISO 31000 existe con el propósito de proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo.

En este sentido, en relación con los ciber riesgos, el departamento de TI o Seguridad de la Información deberá definir una estrategia para gestionarlos, utilizar una combinación de procesos y tecnologías y capacitar a las personas para proteger a la compañía de incidentes de ciberseguridad que puedan comprometer su información, su calidad de servicio o su reputación.

La gestión del riesgo en ciberseguridad toma los principios de la gestión del riesgo en general y los aplica al mundo cibernético. Se basa en la identificación de riesgos, medir su posible impacto, y si las autoridades deciden que se mitigue implementar soluciones, procesos o tecnologías para hacerlo adecuadamente y proteger a la organización. Entre los estándares de gestión de riesgos de seguridad más utilizados en la industria, podemos mencionar a la norma ISO 27005, que suministra las directrices para gestionar los riesgos que puede sufrir la información de una empresa, centrándose principalmente en los requisitos de seguridad de la información. Otra norma NIST SP 800-39:2011, cuyo propósito es proporcionar una guía para un programa integrado para la gestión de riesgos de seguridad de la información, resultante de la operación y el uso de sistemas de información federales de la organización (es decir, la misión, las funciones, la imagen y la reputación), sus activos e individuos, otras organizaciones y de la Nación.

Sin importar el tamaño de la compañía, es fundamental comprender que cualquier organización puede ser el objetivo de un

criminal cibernético. Un ciberataque puede generar daños irreparables en términos financieros y reputacionales.

Diseñar e implementar una adecuada gestión de riesgos de TI y de ciberseguridad permite a la organización reducir las amenazas que producen las vulnerabilidades existentes y mitigar el riesgo de que alguna de ellas se concrete. La creciente cantidad de ciberataques hace que los reguladores exijan una política de gestión de riesgos integral que incluya los ciber-riesgos, y esas regulaciones exigen también que sus regulados requieran a sus proveedores de servicios y terceros conectados la evidencia del tratamiento de los riesgos de TI y seguridad de los servicios en relación con la información que manejan de la compañía.

Todo esto forma parte de la toma de decisiones y debe incluirse en la planificación de las operaciones de manera más habitual, de forma de cumplir con nuestra debida diligencia en el objetivo que nuestras instituciones logren sus objetivos.

Otro beneficio de implementar un sistema de gestión de riesgos integral, que integre al de ciberseguridad y TI, es que si el equipo de trabajo logra trabajar con orientación a riesgos empezando con la información y servicios críticos, la implementación de buenas prácticas y protocolos en este grupo preseleccionado de información, el equipo estará dedicado a proteger en primer lugar lo que es más valioso para la compañía, acompañando naturalmente los objetivos de negocio , estarán mejor preparados en caso de un incidente, logrando así responder con mayor celeridad para recuperar los servicios críticos, disminuyendo los niveles de improvisación al mínimo posible, y contando con planes de acción preparados para las situaciones ya planificadas.

4.1. Gestión de riesgos en el sector financiero

Particularmente el sector financiero es el principal objetivo de los criminales cibernéticos, habiendo experimentado el 19% de todos los incidentes de seguridad en el año 2018. Estas empresas en la

Argentina están sujetas a la Comunicación A 5203 del BCRA, que dicta lineamientos para las entidades financieras, proporcionando buenas prácticas en materia de gestión de riesgos. Se les exige que cuenten con un proceso integral para la gestión de riesgos, que incluya la vigilancia por parte del Directorio y de la Alta Gerencia para identificar, evaluar, seguir, controlar y mitigar todos los riesgos significativos.

Además las entidades financieras deben cumplir con la Comunicación A 4609, la cual establece los requisitos mínimos para la gestión y el control de los riesgos relacionados con la tecnología informática y los sistemas de información.

Es importante destacar que ambas Comunicaciones del BCRA no tienen dentro de su alcance a las compañías *Fintech*.

Para el uso de tarjetas, las emisoras tienen que atenerse a estándares industriales de seguridad como PCI-DSS (Payment Card Industry Data Security Standard) para quienes procesan, transfieren o almacenan información de tarjetas de crédito. [9]

Una de las principales causas de riesgos de ciberseguridad es la falta de educación, entrenamiento o concientización en ciberseguridad, que afecta a las personas, usuarios, clientes internos y externos de las organizaciones que no tienen entrenamiento en estos temas, como no debería sorprender, según un relevamiento del *UK's Information Commissioner's Office* [10]. Especialmente sucede esto cuando un empleado/cliente es víctima de una técnica de ingeniería social, tal como *Phishing* o *E-mail Baiting, clickjacking*, o cualquier otro ataque que dependa del error o distracción humana. Otra fuente de riesgos muy importante pueden ser las aplicaciones desarrolladas sin control de seguridad o una gestión inadecuada de la infraestructura informática, tal como las configuraciones débiles en los sistemas o de los servidores y bases de datos de la organización.

Otro riesgo a considerar, que tiene particular peso en el sistema financiero, es el relacionado con los servicios provistos por terceros, esto toma especial fuerza con la interconexión de los sistemas, ya que si una institución cuyos sistemas tienen interacción con los de otra compañía, es atacada, entonces esta última compañía también estará

en riesgo de ser atacada. Esto podría comprometer tanto la disponibilidad del servicio, como la integridad o confidencialidad de los datos. Por eso a la hora de analizar los riesgos, es importante tener en cuenta aquellos que podrían provenir de terceras partes relacionadas, ya sea desde lo técnico como desde el lado del cumplimiento, ya que si un tercero no cumple con normas como GDPR o PCI-DSS, las consecuencias impactan de forma directa sobre la propia compañía. Tomando por ejemplo a las normas PCI-DSS, estas exigen que todos los terceros con quienes la compañía se relaciones deben también prestar cumplimiento a la norma en tanto su actividad sea aplicable al caso.

Esto nos muestra la importancia de una adecuada gestión del riesgo que ayude a la organización a abordar las vulnerabilidades que pueda padecer y considerarlas en la planificación de las operaciones y en el diseño de la estrategia corporativa. Eso sin mencionar la importancia de llevar tranquilidad a las partes interesadas respecto de los cuidados que la organización toma con su información.

4.2. Brasil

La Circular Nº 3681, publicada por el BACEN (Banco Central del Brasil) en noviembre del 2013, dispone sobre el gerenciamiento de los riesgos y la gobernanza de las instituciones de pago, entre otros, tratando riesgos operacionales, financieros y de información.

Esta norma exige que todas las instituciones de pago tengan una política de gobernanza, actualizada y formalmente aprobada por el directorio ejecutivo y el consejo de administración, la cual debe abordar el gerenciamiento de riesgos. Este documento debe tener una revisión al menos anual, definir atribuciones y responsabilidades, y garantizar una correcta segregación de tareas en las áreas operacionales y en el mismo gerenciamiento de riesgos.

Esta norma también establece lineamientos a nivel operacional, donde fija que la gestión de riesgos debe incluir los siguientes requerimientos:

- Plan de contingencia que garantice la continuidad del negocio.
- Mecanismo de protección de los datos almacenados o transmitidos.
- Mecanismos de protección de redes, sitios electrónicos, servidores y canales de comunicación, con el objetivo de reducir vulnerabilidades.
- Procedimientos para monitorear, rastrear y restringir acceso a datos sensibles, redes, sistemas, bases de datos y módulos de seguridad.
- Monitoreo de fallas de seguridad de datos y de los reclamos de los usuarios finales al respecto.
- Revisión de las medidas para la protección de los datos, especialmente luego de la ocurrencia de fallas y previamente a alteraciones en la infraestructura o en los procedimientos.
- Elaboración de reportes que indiquen procedimientos de corrección de las fallas indicadas.
- Realización de testeos que aseguren la robustez y la efectividad de las medidas de seguridad adoptadas.
- Segregación de funciones en los ambientes de tecnología de la información destinados al desarrollo, testeo y producción.
- Identificación adecuada del usuario final.
- Mecanismo de autenticación de los usuarios finales y de autorización de las transacciones de pago.
- Procesos para asegurar que todas las transacciones puedan ser adecuadamente rastreadas.
- Mecanismos de monitoreo y de autorización de transacciones de pago, con el objeto de prevenir fraudes, detectar y bloquear transacciones sospechosas de forma oportuna.
- Mecanismos para detectar operaciones de alto riesgo.

- Notificación al usuario final en caso de no concretarse una transacción.
- Mecanismos que permitan al usuario final identificar si la transacción fue realizada.

4.3. Chile

El 6 de julio del 2020, la Comisión para el Mercado Financiero publicó la RAN 20-10 (Recopilación Actualizada de Normas) como una suerte de complemento a la Circular Nº1, que regula el sector financiero del país. En ésta se encuentran disposiciones, basadas en buenas prácticas, que deben ser consideradas como lineamientos mínimos a cumplir por las entidades para la gestión de la seguridad de la información y ciberseguridad.

Tengamos en mente, como se adelantó en la Sección 3, Chile no tiene disposiciones específicas para fintech, por lo que la CMF presenta un "Plan de Pruebas" que es una adaptación de las normas vigentes al caso particular de cada Fintech que decide comenzar a operar.

El texto brinda lineamientos sobre la gestión de riesgos de seguridad de la información, aunque también abarca otros asuntos relacionados, como la gestión de incidentes y la gestión de terceras partes, por lo que aporta gran valor a los efectos de este trabajo.

Se plantea el apropiado proceso de gestión de los riesgos como fundamental para apoyar el sistema de seguridad de la información y ciberseguridad instaurado por la entidad, para esto es fundamental que se consideren procesos para:

- La identificación de los riesgos.
- El análisis de los riesgos.
- La valoración de los riesgos, a partir su probabilidad e impacto.
- Determinar el tratamiento adecuado de los riesgos, su posible aceptación y la tolerancia de la compañía las

amenazas a las que están expuestos sus activos de información, así como su monitoreo y revisión permanente.

El sistema de gestión de riesgos de seguridad de la información debe cumplir con una serie de requisitos, entre los cuales se encuentra la identificación de los activos de acuerdo con el alcance contenido en la política de seguridad de la información, que debe existir previamente. Esta identificación debe tener un nivel de detalle suficiente para que la gestión de riesgos sea la adecuada. Luego, se deben identificar las amenazas que puedan afectar a estos activos de información, así como de sus vulnerabilidades, con relación a las amenazas conocidas y los controles existentes. Esto se refuerza con información obtenida de diferentes fuentes, tanto internas como externas. Teniendo toda esta información, se debe evaluar si los controles existentes son eficientes y suficientes y, para el escenario en el que se concreten estas amenazas, cuáles serían las consecuencias en términos operativos y de negocio.

Este análisis de riesgo debe tratar elementos como la probabilidad de ocurrencia de incidentes y su consecuencia o impacto en los activos de información, en base al grado de daño o costos causados por un evento de seguridad de la información y de ciberseguridad, determinando así su nivel de riesgo. En función de todo esto la organización debe asignar una valoración al riesgo, entiendo a la valoración como una actividad donde se compara el nivel de riesgo determinado previamente contra los criterios de valoración y de tolerancia, previamente definidos.

Entendiendo los puntos anteriores, la norma exige que se elabora un plan para el tratamiento de estos riesgos, entendido como una actividad donde los riesgos priorizados en la etapa de valoración, permiten establecer los controles para reducir, aceptar, evitar o transferir los riesgos. Además, se debe cuidar en todo momento que se respete la tolerancia al riesgo que fue definida.

Todos estos procesos y políticas deben ser revisados, al menos, anualmente y deben realizarse los ajustes necesarios. [11]

4.4. México

Si bien no hay una sección específica dedicada a la gestión de riesgos informáticos, podemos ver que en las Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Financiera este asunto se trata de manera indirecta, precisando lineamientos que las entidades deben seguir en este aspecto. [8]

De acuerdo a las disposiciones mencionadas las empresas deben mantener documentación completa y ordenada sobre la gestión de riesgos, no sólo de seguridad de la información sino de todos los riesgos operativos de la compañía. Estas políticas deben estar correctamente comunicadas al personal, el que debe estar capacitado, y deben ser aprobadas por la alta gerencia.

Al menos cada dos años se debe hacer una evaluación de riesgos elaborando un reporte que debe ser presentado a la gerencia, la CNBV y al Banco de México. Además, se debe presentar un plan de acción para tratar las observaciones de criticidad “alta” y “muy alta”. La metodología utilizada para clasificar criticidad y los riesgos de las observaciones presentadas debe estar correctamente explicitada.

Como se verá más adelante en la sección de Gestión de Incidentes, es necesario que haya una persona designada para gestionar las contingencias en materia de seguridad de la información, esta persona es también responsable de gestionar los riesgos en relación al cumplimiento de las regulaciones vigentes y aplicables.

Por último, de existir una vulnerabilidad que afecte a la confidencialidad, integridad o disponibilidad de las información sensible de los usuarios, éstos deben ser informados de los riesgos en los que incurren por la contratación del servicio.

5. La gestión de Incidentes

5.1. ¿Qué es la gestión de incidentes?

La Gestión de Incidentes de Seguridad Informática es el conjunto de procesos para, identificar, analizar y registrar amenazas e incidentes de seguridad en tiempo real y de ejecutar las respuestas apropiadas a dichos eventos. Un incidente de seguridad puede ser tanto un evento o serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio, provocando una pérdida o uso indebido de información, interrupción parcial o total de los Sistemas, siendo los más comunes, la infección por malware, *phishing*, entre otros. Podemos entender por incidente de seguridad a hechos como el intento -fructífero o no- de acceder de forma no autorizada a información de una determinada entidad, a una fuga de información, a la pérdida de datos o la imposibilidad de acceder a éstos, entre otros ejemplos de eventos que afecten la disponibilidad, integridad o confidencialidad de la información. [12]

El *Financial Stability Board* (FSB), organismo que busca la eficacia y estabilidad del sistema financiero internacional, ha desarrollado un *toolkit* de buenas prácticas de respuesta y recuperación de incidentes cuyo objetivo es asistir a las organizaciones en implementar procesos de respuesta y recuperación ante incidentes de ciberseguridad, que se inserten dentro del plan de crisis de una organización. La función de una respuesta ante incidentes es la ejecución de una actividad apropiada frente a un evento de ciberseguridad detectado, mientras que la función de la recuperación ante incidentes tiene como fin la restauración de los servicios afectados. [13] Esta herramienta tiene como objetivo facilitar que las instituciones estén preparadas para responder rápidamente y recuperarse lo mejor y mas efectivamente posible de un ciber-

incidente, ante la virulencia de los ciber-ataques y sabiendo que es difícil prevenirlos.

Este *marco de trabajo* propone practicas efectivas, acciones y procesos que se deben plantear a la hora de diseñar e implementar el circuito de respuesta y recuperación ante incidentes, fue elaborado dentro del plan de trabajo encarado por el FSB ante el pedido del G20 y está basado en siete componentes que recorreremos a continuación.

Gobierno

El gobierno define el marco de trabajo que da lugar a las actividades de recuperación y respuesta (ARR),debe ser impulsado por las altas autoridades, quienes deben funcionar como sponsors para alinear las actividades de respuesta y recuperación con los con los objetivos para la continuidad del negocio, deben definir la estructura y los roles de la organización de tal forma que se logre una eficaz coordinación entre las metas corporativas y las ARR. El gobierno incluye también la construcción de un marco de trabajo para la toma de decisiones donde queden claras las responsabilidades y que permita involucrar a los *stakeholders* en caso de incidentes. La gobernanza también encapsula el compromiso para apoyar las ARR a través de medidas adecuadas para cumplir el rol de sponsor y de la promoción de comportamiento adecuados de los usuarios y todos los participantes de la organización para lidiar con eventos potencialmente nocivos de ciberseguridad.

Preparación

Durante las actividades de preparación se establecen y mantienen los procesos para sostener la capacidad de responder ante incidentes de ciberseguridad y para restaurar las procesos, funciones, actividades sistemas y datos críticos afectados y llevarlos a un estado normal respecto de las operaciones. Si bien la preparación ocurre antes del incidente, afecta de forma directa a la efectividad de las ARR.

Análisis

La actividad de análisis se realiza para asegurar la efectividad en la respuesta y recuperación de actividades, incluyendo análisis forenses, y para determinar la severidad, el impacto y la raíz del incidente de ciberseguridad. Esto posibilitará la determinación de actividades apropiadas de respuesta y recuperación en función de la criticidad del incidente.

Mitigación

Las actividades de mitigación son desarrolladas para reducir el impacto ante una determinada situación y erradicar las ciber-amenazas en un tiempo adecuado para que las operaciones del negocio y los servicios resulten afectadas de la menor manera posible.

Restauración

Esta actividad tiene por objeto reparar y restaurar sistemas o activos críticos afectados por un incidente de ciberseguridad para reanudar de manera segura los procesos y los servicios del negocio que han sido impactados.

Mejora

Se establecen procesos para mejorar la respuesta y la restauración de las capacidades de una organización a través de tomar en cuenta las lecciones aprendidas de incidentes de ciberseguridad del pasado, además de realizar diferentes ejercicios de carácter proactivo. Con los resultados de las lecciones aprendidas y de los ejercicios, se realizan y actualizan cambios a las procedimientos y procesos de respuesta de incidentes y a la planificación de operaciones para mejorar la eficiencia de los procesos, las capacitaciones y los testeos. Las lecciones aprendidas son usadas en la selección de implementación de controles adicionales y las medidas de mitigación.

Coordinación y comunicación

Las organizaciones coordinan con los *stakeholders* externos de confianza para mantener un buen nivel de concientización y apoyo a las políticas y directrices relacionadas a la seguridad de la información. Durante un incidente de ciberseguridad, con una frecuencia establecida y acordada, con cada grupo de *stakeholders*, usando un nivel de detalle y un lenguaje apropiado para cada uno, de esta forma es posible promover el involucramiento en las ARR.

El progreso y los resultados de los análisis que se elaboran son compartidos también, tanto con las partes interesadas internas como externas, para poder tomar medidas que prevengan, contengan o mitiguen incidentes de ciberseguridad o para evitar malos entendidos como consecuencia de falta de información. Un buen canal de comunicación permite eficiencia y seguridad a la hora de compartir información.

5.1.1. ¿Por qué la gestión de incidentes es importante para las Fintech?

Tal como se mencionó en el punto anterior, gestionar apropiadamente los incidentes de ciberseguridad es una actividad fundamental en cualquier empresa, mas aun cuando son tan dependientes de la tecnología. Según un reporte realizado en 2019 por IBM [14], las compañías que tienen procesos definidos para la gestión de incidentes pueden reducir pérdidas, en promedio, por 360 mil dólares por cada incidente que implique fuga de información.

La gestión de incidentes de ciberseguridad que afecten el sistema financiero es esencial para limitar cualquier riesgo a la estabilidad financiera de ese ecosistema. Estos riesgos aumentan al contar con sistemas tecnológicos interconectados ya sea entre diferentes entidades financieras o entre una entidad y una tercera

parte asociada, el impacto ante un ciber-incidente podría provocar en general falta de confianza en el sector de la industria en la que se opera y en particular la pérdida de capital consecuente en una institución ante un incidente. Las organizaciones que se muestren resilientes a esta clase de incidentes podrían lograr un funcionamiento fluido y estable y mayor confianza en sus usuarios y *stakeholders*.

Es evidente que este asunto es de gran interés para los entes reguladores, que investigan las diferentes maneras en las que la falta de diligencia en este aspecto puede afectar no solamente a la seguridad de los usuarios que confían en los servicios de las instituciones financieras, sino en el ecosistema financiero del país. Es en función de esto que se analizan normativas que las empresas fintech deben seguir.

5.2. Brasil

En Brasil existen dos circulares principales emitidas por el Banco Central de Brasil que hacen referencia a la gestión de incidentes: la Circular Nº 3.909 y la Nº 4.658. Refiriéndose la primera a las instituciones de pago y la segunda a las instituciones financieras.

Ambas normas son prácticamente idénticas, difiriendo principalmente en los plazos de adecuación que las empresas tienen para ajustarse a lo establecido en las normas. Las empresas Fintech, de acuerdo a la normativa brasileña, entra en la categoría correspondiente a la Circular Nº 3.909.

Tanto la circular Nº 3.909 como la 4.658 tienen varias secciones que hacen referencia específicamente a la gestión de incidentes.

De acuerdo con las directrices de estas normas, todas las instituciones de pago deben crear una Política de Seguridad Digital donde conste un plan de acción ante incidentes de seguridad. Todo esto dentro de un marco donde debe estar elaboradas políticas y normas para la protección de la información y proteger los datos personales, haciendo foco en la detección, clasificación y solución de potenciales vulnerabilidades. Para todo esto se deben estudiar todos

los escenarios posibles y tener previstas las respuestas pertinentes, con el objetivo de resolver los problemas en el menor tiempo posible.

Se prevé también la obligatoriedad de las instituciones de pago de compartir información sobre incidentes que sean relevantes para el resto de la industria, explicitando en un reporte anual las acciones que se tomaron en el marco de sus políticas de seguridad y su plan de respuesta a incidentes. Este reporte debe estar elaborado por el área responsable de la protección y la Gobernanza de los datos.

Estos reportes deben ser remitidos al Gestor de Seguridad, cargo que debe estar contemplado en el área de IT, quien estará a cargo de la planificación de la seguridad de la información de la institución. Siendo esto así, nombrar a este funcionario dentro de la compañía es uno de los primeros pasos para cumplir con los requisitos de estas circulares.

Toda la documentación producto de las exigencias del Bacen deberán estar a disposición de éste por un plazo mínimo de 5 años. [15]

Además, la Circular Nº 3909 establece que todas las instituciones de pago deben tener plan de acción definido y formalizado en caso de incidentes; éste debe incluir:

- La forma en la que se va a adaptar estructuralmente la organización a las directrices de la política de ciberseguridad
- Los controles y procedimientos que se van a utilizar
- Definir al área responsable por el registro y el control de los incidentes
- Designar un director responsable por la política y su ejecución
- Deben elaborar un reporte anual sobre la implementación del plan de acción y de respuesta a incidentes. En el mismo se deben detallar
    - Su nivel de efectividad
    - Rutinas, procedimientos y controles de información útil obtenida para tratar nuevos incidentes
    - Incidentes relevantes ocurridos

- Resultados de test de continuidad del negocio, considerando escenarios de indisponibilidad ante incidentes
- Revisar (y eventualmente actualizar) la documentación anualmente [16]

Todas las políticas de seguridad informática deben estar disponibles al público, sin embargo, el BACEN permite publicar versiones resumidas de éstas donde se restrinja la información confidencial.

5.3. Chile

La Superintendencia de Bancos e Instituciones Financieras de Chile (SBIF) ha emitido la Circular Nº1 para regular a las entidades financieras no-bancarias. Específicamente, en una extensión de ésta circular, la Recopilación Actualizada de Normas (RAN) 20-8, se establecen los lineamientos que se deben seguir en materia de Gestión de Incidentes.

Al respecto la norma comienza afirmando lo siguiente:

" (…) resulta relevante que las entidades dispongan de sistemas, procedimientos y mecanismos de gestión que permitan identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales, en especial aquellos relacionados con la Ciberseguridad. Estos sistemas deben permitir al banco tener una visión oportuna de los incidentes y, a la vez, asegurar la existencia de herramientas para hacer el seguimiento y correlacionar eventos, a objeto de detectar otros incidentes, identificar vulnerabilidades de la infraestructura física y virtual comprometida, modus operandi de los eventuales ataques, entre otros." [17]

En virtud de esta norma es que se establece cómo se deben gestionar los incidentes de seguridad informática, cómo se debe notificar a la Superintendencia en caso de que eso ocurra y cómo informar a los clientes de eventos relevantes y cómo compartir la información de ataques de ciberseguridad con otros agentes de la industria.

Dentro del alcance de esta norma entran todos los incidentes operacionales que cumplan con alguno de los siguientes requisitos:

- Que afecten o pongan en riesgo la continuidad del negocio
- Que afecten los recursos de la entidad o de sus clientes
- Que afecten la calidad de los servicios
- Que afecten la imagen de la institución.

Cuando algo de esto ocurra, se debe informar a la Superintendencia sobre el hecho y sobre las medidas que se tomen en consecuencia. Se tiene un tiempo máximo de 30 minutos desde la ocurrencia del incidente para concretar la comunicación.

La norma es extremadamente detallada sobre el formato en el que debe realizarse el reporte, la que debe contener:

- Número único identificador del incidente (asignado por la SBIF)
- Nombre de la entidad informante
- Descripción del incidente
- Fecha y hora de inicio del incidente
- Causas posibles o identificadas
- Productos o servicios afectados
- Tipo y nombre de proveedor o tercero involucrado (si corresponde)
- Tipo y número estimado de clientes afectados
- Dependencias y/o activos afectados (si corresponde)
- Medidas adoptadas y en curso
- Otros antecedentes

Luego, al cierre del incidente, una nueva comunicación debe ser emitida con un estado actualizado de la información anterior, agregando además la fecha y horario del cierre del caso. Adicionalmente, las autoridades se reservan el derecho de solicitar reportes complementarios.

Si los hechos afectan a los usuarios de la entidad, se los debe mantener informados y actualizados periódicamente sobre el caso hasta que el problema haya sido resuelto.

Como se adelantó al comienzo de esta sección, las compañías deben informar al resto de la industria sobre todos los incidentes de ciberseguridad que sean relevantes a modo de proteger a los usuarios y al sistema en su conjunto. Para esto es importante que todas las instituciones mantengan un sistema de alertas de incidentes en el cual deberán reportar, como mínimo, una descripción del hecho, qué canales o servicios fueron afectados, la identificación del *software* malicioso y los mecanismos de protección detectados (si se encuentran disponibles). Esta comunicación debe hacerse en el más breve plazo posible. Además, el sistema de alertas debe permitir a la SBIF el acceso a la información compartida de los incidentes.

La norma define la obligatoriedad de designar un funcionario de la institución que sea el responsable último de que estos procesos se lleven a cabo como corresponde, ese funcionario será el encargado de la seguridad de la información.

Se destaca que desde el 1º de julio de 2019 la SBIF se ha fusionado con la Comisión Para el Mercado Financiero de Chile (CMF) y por lo tanto todas las resoluciones emitidas por la SBIF figuran desde ese entonces en el sitio web oficial de la CMF. Esto ocurre como consecuencia del gran impacto que tuvo el ciberataque realizado al Banco de Chile, que obligo al Gobierno Chileno a realizar reformas que le permitieran tener mejor controlado el sistema financiero en su conjunto, en relación con los ciber ataques. [18]

5.4. México

Al igual que con la gestión de riesgos, no hay una disposición explícita sobre cómo debe ser la gestión de incidentes, sin embargo podemos ver -a lo largo de diferentes regulaciones- que hay muchas exigencias que las instituciones de pago electrónicos deben seguir a lo largo de las diferentes disposiciones [8] publicadas por la CNBV.

Por ejemplo, es indispensable que todas las empresas de pagos electrónicos dispongan de políticas de seguridad informática, donde

se contemplen procedimientos para la gestión de incidentes, que estén correctamente comunicadas y aprobadas de acuerdo a los mecanismos formales de la organización que incluyan la identificación, evaluación, monitoreo y mitigación del problema. Debe poder garantizarse la continuidad operativa.

Debe haber un responsable asignado por la alta gerencia con el propósito de administrar las contingencias. Entre sus objetivos deben estar:

- Elaborar, revisar y, en su caso, actualizar el Plan de Continuidad de Negocio.
- Evaluar, por lo menos una vez al año, el alcance y efectividad, así como el cumplimiento del plan de gestión de contingencias establecido e informar los resultados.
- Definir y comunicar las metodologías utilizadas para la administración de contingencias y para determinar los impactos cualitativos o cuantitativos de los escenarios planteados.
- Poner a prueba la eficacia de las metodologías utilizadas al menos una vez al año, informando los resultados.

Es obligatorio que ante una contingencia que imposibilite las operaciones por más de 30 minutos o se comprometa la información de los usuarios, se comunique el incidente al Banco de México y a la CNBV con una demora de no más de 60 minutos desde tomado conocimiento del hecho. Estos hechos deberán implicar luego una investigación interna de la compañía cuyos resultados deben ser informados.

Debe también haber canales de comunicación definidos con los clientes para mantenerlos informados cuando el nivel de disponibilidad del servicio o la integridad o confidencialidad de sus datos se vean afectados.

Respecto de los requerimientos a nivel infraestructura, es mandatorio que se cuente con antivirus y herramientas que ayuden a detectar eventos de seguridad, así como también alertas que notifiquen

casos relevantes. Esto debe quedar registrado y se debe llevar cuenta de la detección de fallas, errores operativos, intentos de ataques informáticos y de aquellos efectivamente llevados a cabo, así como de pérdida, extracción, alteración, extravío o uso indebido de información de los Usuarios de la Infraestructura Tecnológica o de los Clientes, en donde se contemple la fecha del suceso y una breve descripción de este, su duración, servicio o el elemento de la Infraestructura Tecnológica afectado, Clientes afectados y montos, así como las medidas correctivas implementadas.

6. La Gestión de las Terceras Partes

La gestión de las terceras partes es un proceso fundamental en el cuidado de la seguridad de la información de cualquier organización, pues finalmente sigue siendo responsabilidad de la institución el manejo adecuado de los datos, mas allá de quien lo gestiona, la responsabilidad no se delega. Esto implica el análisis y la implementación de controles para cualquier riesgo resultante de la interacción entre la organización y un tercero. Estos riesgos pueden ser financieros, cumplimiento, operacionales, entre otros. Una buena gestión de los riesgos de los terceros proveedores de servicios, puede mitigar de manera considerable el impacto de estos riesgos.

Para lograr todo esto es necesario que una compañía tenga políticas y procedimientos debidamente implementados, que incluyan, entre otras, evaluaciones de seguridad previas a la contratación del proveedor, sumadas a una gestión continua y completa de los controles de acceso a sus propias redes.

Un estudio realizado por el Instituto Ponemon en los Estados Unidos en 2018 encontró que el 61% de las compañías de ese país que tuvieron una filtración de datos le acreditan la causa a una vulnerabilidad de un tercero con el que tenían interacción, lo que muestra un incremento respecto del 56% en 2017 y del 49% en 2016. Esto es especialmente importante en las compañías grandes con

infraestructura tecnológica bien desarrollada pero que al mismo tiempo tienen gran cantidad de clientes y proveedores, tendrán probablemente una buena parte de sus potenciales vectores de ataque relacionados con los terceros que interaccionan, dando buenas razonas para hacer especial foco en el manejo de las terceras partes.

Este incremento cobra aún más sentido si observamos que, de acuerdo al mismo estudio, el porcentaje de compañías con las que una determinada organización comparte información sensible aumentó desde un 27% en 2016 a un 43% en 2018.

Como ejemplos se pueden citar los casos de la red de hospitales estadounidense Atrium Health, donde los datos privados de más de 2,65 millones de pacientes fueron filtrados a partir de una vulnerabilidad de AccuDoc Solutions, una compañía que les gestionaba las cobranzas. Otro caso conocido es el de la agrupación criminal Magecart que, a través de vulnerabilidades en varios servicios web para el procesamiento de pagos con tarjeta de crédito de una empresa proveedora pudieron acceder a información sensible de clientes de numerosas compañías, entre ellas British Airways, TicketMaster y Newegg.

Es importante aclarar que el riesgo no pasa únicamente por la fuga de datos en sí mismo sino también por las consecuencias que eso podría acarrear desde un punto de vista legal y reputacional. Los riesgos de seguridad, de explotarse, pueden traer aparejadas indisponibilidad del servicio, pérdidas o modificaciones no autorizadas de datos, mas allá del hecho que los datos pudieran ser publicados o accedidos por un atacante.

Una práctica que está tomando impulso en el sistema financiero, es gestionar el riesgo de las cuartas partes, es decir, las entidades proveedores de servicio de las terceras partes, pudiendo aplicar el mismo criterio para las N-partes. Cuanta más indirecta sea la relación, por lo general, menor será el riesgo y mayor será el costo operativo. [19]

6.1. Brasil

Las antes mencionadas Circulares Nº 3.909 y 4.658 dedican una buena parte de sí mismas a la gestión de los prestadores de servicios y exige que se los tome en consideración en la gestión de incidentes y en la confección de las políticas de seguridad.

Se destaca lo presentado en la Sección 3, que si bien Brasil no tiene regulaciones específicas para Fintech, las regulaciones existentes para el industria financiero y bancaria deben aplicarse en la medida de lo posible.

Los prestadores de servicios deben estar ajustados a todas las exigencias de las normas a las que está sujeta la institución de pagos para la protección de los datos y tener controles para identificar y minimizar el impacto en caso de un ataque cibernético. Por supuesto, cuanto mayor la complejidad y el riesgo de los servicios prestados, mayores deben ser las exigencias por parte del cliente, quien tendrá una cuota importante de responsabilidad en caso de que sus proveedores no cumplan con las normas tanto como si estos incumplimientos hubieran ocurrido en su propio establecimiento.

El BACEN también destaca que la institución de pagos debe tener acceso a los datos propios que el proveedor almacene o procese. Además, antes de la contratación en sí misma, se debe informar al Bacen sobre cualquier proveedor relevante (es decir, que aplique al cumplimiento de las Circulares Nº 3.909 y 4658) con 60 días de anticipación y debe informar en qué países o regiones se almacenará y procesa la información. [15] Si la legislación del país donde son almacenados los datos no permite el acceso de las autoridades brasileñas en caso de requerirlo, entonces no estará permitido mantener el servicio en esas condiciones.

La institución de pagos debe poder acceder a los informes de auditorías externas de sus proveedores y habiendo analizado el estado de su seguridad es responsable de verificar que se tomen todas las medidas de protección físicas y lógicas que apliquen al caso para

proteger la confidencialidad, disponibilidad e integridad de la información.

Es también obligatorio tener un plan de contingencias en caso de que se interrumpa el servicio prestado por la empresa contratada. Tanto esto último como todo lo descrito anteriormente debe estar apropiadamente documentado y disponible ante solicitud del Bacen.

Las normas del Bacen abarcan cualquier tipo de tercerización de servicios en la nube, incluyendo servicios SaaS, Iaas y Paas.

6.2. Chile

Otra de las Recopilaciones Actualizadas de Normas (RAN) emitidas por la SBIF es la 20-7, que se encarga de especificar los lineamientos para la contratación de proveedores de servicios externos. Estas normas deberán aplicarse en la medida en la que se dispongan en el Plan de Pruebas presentado por la CMF (ver Sección 3).

La RAN contempla variados tipos de riesgos e insta a toda organización a contemplarlos en una sólida administración de riesgos entendiendo que el procesamiento externo tiene incidencia sobre ellos, éstos son el riesgo operacional, el estratégico, el reputacional, el de cumplimiento con normas industriales y con normas nacionales o riesgo de incumplir obligaciones contractuales.

Es obligatorio el establecimiento de normas, políticas y procedimientos tanto para la gestión de estos riesgos como para la gestión de las terceras partes en sí mismas.

Los procesamientos externos deben cumplir con una serie de condiciones que están divididas en seis categorías:

1. **Condiciones Generales**:
    a. Debe haber una política aprobada por el directorio donde se regule la contratación de servicios para procesamiento externo y la gestión de los riesgos que esto implica.

b. Se deben tener establecidos los criterios de selección, contratación y monitoreo de proveedores (los elementos mínimos que deben ser considerados serán explicados más adelante).
c. Se debe tener bien documentado qué servicios son tercerizados y con qué proveedor se están ejecutando. Asimismo, cada servicio debe tener asociado un nivel de riesgo y una especificación sobre su importancia estratégica para facilitar la determinación de su criticidad.
d. Bajo ningún concepto se debe considerar que el procesamiento externo de la información exime a la institución de alguna de sus obligaciones.
e. La responsabilidad del cumplimiento legal y regulatorio de estas actividades continúan siendo del banco.
f. Se deben realizar procesos independientes de selección de proveedores y se debe verificar que cumplan con todas las normativas vigentes y que tengan procesos de seguridad razonables para la actividad que desempeñan.
g. Todos los riesgos que implique el procesamiento externo deben ser tenidos en cuenta a la hora de gestionar los riesgos corporativos.

2. Continuidad del Negocio

a. El cliente debe verificar periódicamente que sus proveedores cuenten con planes apropiados que aseguren la continuidad de sus servicios. El periodo de revisión -tanto para el cliente como internamente para la compañía proveedora- es de al menos un año.

3. Seguridad de la información propia, de clientes y otros casos que correspondan

a. La institución debe asegurarse de que el proveedor de servicio pueda mantener la confidencialidad, integridad y disponibilidad de los activos de información de la institución financiera y de sus clientes. Estas condiciones deben ser consistentes con las políticas de la entidad financiera y quedar incorporadas en el contrato de prestación de servicios.

   Los roles de los involucrados deben estar bien definidos y la información procesada debe estar encriptada, dando acceso al Banco de Chile a las claves de desencriptación, para lo cual habrá que fijar previamente procesos de transmisión de claves entre la compañía y el Banco.

4. Acceso a la información por parte del supervisor

a. La institución contratante debe asegurarse que esta Superintendencia tenga acceso permanente a todos los datos e información que se mantengan y generen a través de un proveedor externo ya sea establecido en el país o en el exterior.
   Al igual que el BACEN en Brasil, en Chile es obligatorio tener analizar las restricciones en los diferentes países donde se almacene o procese la información que puedan evitar el acceso de las autoridades a la ésta.

5. Riesgo país

a. No se podrán externalizar servicios en jurisdicciones que no cuenten con calificación de riesgo país en grado de inversión. Aquellos bancos que contraten servicios con empresas ubicadas en países cuya clasificación de riesgo internacional sea inferior a la otorgada a Chile, deberán tomar

resguardos adicionales para mitigar el mayor riesgo asumido, lo que será evaluado caso a caso por esta Superintendencia.

6. **Responsabilidad por la gestión**
    a. La responsabilidad de la gestión de los riesgos y procesos de control la tiene el Directorio u órgano equivalente.

La normativa Chilena, además, discrimina los servicios que se realizan localmente de los que tienen procesamiento en el exterior, ambos con sus requerimientos particulares:

1. **Servicios realizados localmente:** En estos casos se deberá comprobar que la infraestructura tecnológica y los sistemas que se utilizarán para la comunicación, almacenamiento y procesamiento de datos, ofrecen suficiente seguridad para resguardar permanentemente la continuidad operacional, confidencialidad, integridad, exactitud y calidad de la información y los datos. Se debe verificar también que las condiciones del servicio permitan la recuperación de la información tanto por requerimientos del cliente como de las autoridades competentes.
2. **Servicios realizados en el Exterior**: En este caso se debe comunicar la intención de contratar el servicio a la Superintendencia y proveer información de la compañía proveedora respecto de sus antecedentes, su solidez financiera, el nivel de experiencia de su personal que intervenga en el servicio contratado, certificaciones de calidad y sistemas de control. Se debe especificar si hay empresas subcontratadas interviniendo en el servicio e incorporarlos a este mismo proceso descrito.

   Cuando la institución financiera en cuestión tiene una participación en el mercado superior al 5% se la considera como “Sistémicamente Relevantes”. En estos casos deben cumplir con los siguientes dos requerimientos:

    a. Debe haber un centro de procesamiento de datos de contingencia y debe estar ubicado en Chile.

b. La administración principal del centro de procesamiento de datos debe hacerse desde Chile, igual que la administración, soporte y mantención de infraestructura de *Hardware*, *Software*, telecomunicaciones y aplicaciones de negocios.

En cualquier caso, para la contratación de un servicio se debe notificar a la Superintendencia y solicitar su autorización. Se debe incluir información de la compañía externa que posibilite el análisis a las autoridades. La información mínima que debe estar incluida es especificada en el Anexo I. [20]

6.3 México

En la Ley Fintech de México, en el artículo 54, deja claro que las instituciones financieras pueden contratar a empresas externas para derivar parte de sus operaciones, tanto en el territorio nacional como en el exterior, y que tanto la CNBV como el Banco de México pueden emitir disposiciones regulando este tipo de relaciones. Además, se advierte que esto no le resta responsabilidad a la institución financiera de mantenerse en cumplimiento con las normativas vigentes, por lo que se debe velar que las terceras partes contratadas se mantengan conforme a la ley.

Dentro de las Disposiciones [8] emitidas por la CNBV se exige la autorización tanto de la CNBV como del Banco de México para la contratación de terceros, siempre que cumplan con alguna de las siguientes tres características:

1. Los servicios que dicho tercero preste impliquen la transmisión, almacenamiento, procesamiento, resguardo o custodia de Información Personal o Información Sensible, imágenes de documentos de identificación expedidos por autoridades oficiales o información biométrica de los Clientes, siempre y cuando el tercero de que se trate tenga privilegios de acceso para conocer dicha información o a la información de configuración de seguridad, o bien, a la administración de control de accesos
2. Realice procesos en el extranjero relacionados con la contabilidad o tesorería
3. Funja como el proveedor primario de aquellos servicios cuya interrupción, parcial o permanente, imposibilite a la institución de

fondos de pago electrónico la emisión, administración, redención o transmisión de fondos de pago electrónico.

Si el tercero cumple con el punto 3 anterior o bien se trata de una empresa financiera enmarcada en las Disposiciones de Carácter General Aplicables a Las Instituciones de Tecnología Financiera, entonces se deberá notificar a la CNBV y al Banco de México sobre la contratación con un mínimo de 20 días de anticipación y se deberá aguardar su autorización durante 25 días hábiles, de no haber respuesta se podrá entender la solicitud como aprobada. Durante ese período la contratación puede ser rechazada por cualquiera de las dos entidades si se considera que el tercero no podrá ajustarse a las regulaciones vigentes o que puede afectar negativamente a la estabilidad financiera de la entidad contratante.

Asimismo, si se llegasen a modificar las condiciones del servicio, también se deberá notificar a la CNBV y al Banco de México con 20 días de anticipación.

Ahora bien, junto con el pedido de autorización es fundamental adjuntar información que permita a la CNBV y al Banco de México comprender el servicio y el contexto en el que esto se está llevando a cabo, conteniendo como mínimo:

- La descripción detallada y diagramas de flujo de los procesos de los servicios a contratar
- El proyecto de contrato de prestación de servicios
- Información respecto de la infraestructura tecnológica, como por ejemplo:
    - La descripción de los enlaces de comunicación utilizados por la institución de fondos de pago electrónico para conectarse con el proveedor de servicios, que incluya el nombre del proveedor, el ancho de banda y el tipo de servicio prestado, entre otros.
    - Un diagrama de telecomunicaciones en donde se muestre la conexión existente entre cada uno de los participantes en la prestación del servicio (proveedores, centros de datos, institución de fondos de pago electrónico, entre otros), incluyendo los esquemas de redundancia.

    - La dirección completa del lugar en donde se realizarán cada uno de los servicios, así como de los centros de datos, primario y secundario, en donde se almacenará y procesará la información.
    - En su caso, el esquema de interrelación de aplicaciones o sistemas objeto de la contratación, incluyendo los sistemas propios de la institución de fondos de pago electrónico.
    - Los mecanismos de continuidad del servicio contratado.
    - Si el tercero mantenga Información Personal e Información Sensible deberá acreditar que dicha información se encuentre cifrada y que los mecanismos y procedimientos para descifrarla estén en posesión del oficial en jefe de seguridad de la información quien será responsable, en caso de pérdida, de la ejecución de los referidos mecanismos y procedimientos.
- Los mecanismos que le permitan a la institución de pagos disponer de todas las transacciones que se realicen y de los estados contables que se generen
- Los mecanismos que permitan vigilar el desempeño del tercero contratado y el cumplimiento de sus obligaciones
- Planes de acciones para evaluar y reportar la performance del tercero al comité de auditorías de la institución de pagos.
- Evidencia que acredite que el tercero tiene adecuadas políticas de confidencialidad y de protección de datos personales.
- Si se va a procesar o almacenar información fuera de México se debe demostrar que en esos países en cuestión hay marcos regulatorios que protejan la confidencialidad de los usuarios o bien que esos países tengan acuerdos con México que permitan intercambiar información con organismos supervisores.
- Esquemas de soporte técnico para la resolución de problemas

La institución de pagos deberá hacer una auditoría anual de cada tercero que aplique al caso y llevar registro de los hallazgos que recolecte. Se deberá contar con un seguimiento de los mecanismos de control y vigilancia del acceso a los sistemas informáticos y a la Información Personal o Información Sensible transmitida, almacenada, procesada, resguardada o custodiada en

dichos sistemas, así como de las bitácoras, bases de datos y configuraciones de seguridad que se establezcan al efecto.

En caso de auditorías, tanto de un tercero independiente como de la CNBV o el Banco de México, es indispensable entregar la documentación necesaria y suficiente sobre los servicios contratados con los proveedores.
Como se dejó entrever antes, la institución de pagos electrónicos tendrá la obligación de asegurarse de que sus proveedores puedan brindar el nivel de confidencialidad correspondiente en cada caso y serán responsables si así no ocurriese.

Por último, con una frecuencia mínima de dos años se deberán realizar auditorías por parte de una entidad independiente y, en caso de encontrarse vulnerabilidades consideradas críticas por el agente auditor, se deberá entregar un reporte a las autoridades ejecutivas de la compañía y se deberá notificar a la CNBV y al Banco de México.

7. Conclusiones

Es evidente que en América Latina, en lo que respecta a seguridad informática, aún queda mucho por hacer en materia regulatoria en el rubro *fintech*. También hemos podido ver que no todos los países están en el mismo estado de madurez. Los casos de Brasil y Chile, donde se toman las regulaciones ya existentes para la industria financiera en general y se las intenta adaptar en la medida de lo posible a las fintech, son el caso más frecuente a nivel global, aún más incluso en economías en vías de desarrollo.

En particular, en el caso de Chile, se detecta una situación clara: su método no es escalable. Como se comentó anteriormente, en Chile las empresas cuya facturación supera el 1% de la industria financiera nacional debe obtener una licencia para operar, para lo cual deben estar alineados a las regulaciones pertinentes. En el caso de las fintech, la CMF presenta un “plan de pruebas”, es decir, una adaptación de las normas existentes para ser aplicadas a la compañía fintech en cuestión que se esté tratando. Esto es muy poco eficiente tanto para las autoridades nacionales como para el sector

privado y genera demoras innecesarias hasta que la compañía recibe noticias sobre los requisitos a los que se debe atener.

En este sentido, y considerando lo expuesto, México pareciera ir por un camino bastante acertado. Allí ya se ha dictado una ley específica para la industria fintech y de ella se han derivado disposiciones que abarcan un gran abanico de cuestiones relativas a la seguridad de la información, pero aún en este caso se observa que por momentos estas disposiciones parecen insuficientes. Por ejemplo, en lo que respecta a la gestión de incidentes y a la gestión de riesgos, las disposiciones son muy generales, si bien en caso de una auditoría la CNBV se reserva el derecho de solicitar medidas de protección específicas que apliquen al caso de manera particular, esto resulta muy abierto y deja un nivel de incertidumbre importante para los emprendimientos que recién comienzan a entrar en el mundo Fintech para comprender de qué manera se pueden ajustar a las regulaciones existentes. De todas formas se espera que esto mejore en la medida en que la industria vaya creciendo y madurando, ofreciendo reglas de juego claras que a su vez facilite la llegada de inversores externos.

En Argentina existen las circulares 6354, 6375 y 6885 del BCRA (Banco Central de la República Argentina) que forman parte del Texto Ordenado de Normas “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras” [21], que regula a todas las entidades financieras que operan en el país, a las cuales también se deben alinear las empresas *Fintech* que dependen de instituciones bancarias, como la billetera electrónica MODO.

Además, existe la Comunicación 6731, donde se establecen principios para las “Infraestructuras del Mercado Financiero”, cuyo alcance son las redes de cajeros automáticos, las cámaras de compensación de valores de entidades financieras y la cámara compensadora privada, encargada de procesar electrónicamente los pagos de bajo valor. En este aspecto, bajo el alcance de la norma se encuentran empresas como Link, Coelsa o Prisma, BYMA, Caja de valores, entre otros [22].

Dada la interconexión existente entre los servicios financieros ofrecidos por las *Fintech* y el sistema financiero, es deseable que existan normativas

específicas para la regulación de las empresas *Fintech*, las que al menos deberían abarcar los puntos necesarios para mantener la resiliencia operativa del sistema en su conjunto.

Algunos de esos puntos podrían ser:

- **Gestión de Riesgo**

  Se deben tener en cuenta factores clave para la gestión de riesgos, como la integración de estos procesos con la toma de decisiones.

  Es deseable considerar también mecanismos apropiados para documentar y comunicar la información que, además de mejorar los procesos en cuestión, contribuyen a generar una cultura orientada a la gestión de los riesgos, que esté abierta informarse y buscar informar a otros, que tengan documentados sus análisis de riesgos y sepan comunicarlos debidamente, sabiendo sugerir las opciones de mitigación adecuadas. De esta forma también se facilita que el programa de gestión de riesgos esté sincronizado con la estrategia corporativa.

  Se sugiere que las normas también contemplen el establecimiento de roles bien definidos con tareas correctamente segregadas y que existan políticas internas que vayan de soporte a la gestión de riesgos.

  Es deseable también que existan procesos de monitoreo y testeo de las actividades donde se manipule información sensible y se definan rangos aceptables para los indicadores clave de performance (KPI) y los indicadores clave de riesgo (KRI) para detectar potenciales desvíos.

- **Gestión de terceros**

  Es de vital importancia considerar todas las aristas en este punto para evitar eventualidades, teniendo en cuenta factores cómo por ejemplo el tipo de información que se comparte con los terceros y de qué manera se les brinda acceso, si la naturaleza el servicio que se provee requiere

accesos físicos a las instalaciones de la compañía, si los procesos con los terceros están apropiadamente documentados y si los contratos firmados con ellos cumplen con las prácticas requeridas por los entes reguladores de cada país.

Además, se debe tener en mente de qué manera se gestionaría la eventual terminación de relaciones con un tercero, es decir, cómo se van a gestionar la destrucción o devolución de la información compartida, la restricción del acceso físico y lógico de los empleados del tercero y la comunicación a las áreas involucradas de la compañía sobre el cese de actividades con la empresa en cuestión.

Por último, es fundamental establecer las condiciones bajo las cuales la compañía *Fintech* compartiría datos personales y financieros de los usuarios con terceras partes, buscando que estén informados sobe el manejo de sus datos y teniendo así mayor poder y control sobre el manejo de su información personal.

- **Gestión de incidentes**

  En este aspecto, estos procesos bien pueden basarse en el Marco de Trabajo desarrollado por el FSB a pedido del G20, mencionado en la sección 5.1, abarcando los siguientes tópicos:

  - **Gobierno**: Establecer principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa.
  - **Preparación**: Estar a la altura para hacer frente a las amenazas y a los posibles incidentes que puedan materializarse.
  - **Análisis**: Lograr eficiencia y eficacia en la gestión de la información para nutrir el proceso de toma de decisiones.
  - **Mitigación**: Reducir el impacto y la probabilidad de los riesgos analizados al mínimo posible.

- **Restauración**: Recuperación de sistemas y activos críticos que hayan sido afectados por un incidente.
- **Mejora**: Lograr la capacidad de pulir los procesos para conseguir mejores resultados en la gestión de la información, el tratamiento de los riesgos y los incidentes, entre otros.
- **Coordinación y Comunicación**: Lograr que la empresa tenga capacidad para coordinar sus actividades tanto internamente como con las partes interesadas, para lo cual es necesario tener canales de comunicación formalmente establecidos.

Otras áreas que se sugiere considerar, aunque escapan al alance de este trabajo son el plan de continuidad del negocio y la Definición de procesos críticos, sus interconexiones e interdependencias.

En todos los casos, deberá considerarse la coyuntura local, las amenazas, las oportunidades y las características particulares que presenta la industria en las regiones donde se opere.

De concretarse esto, se lograría un avance muy importante en la misma dirección en la que está evolucionando México y pondría a la República Argentina en una posición de vanguardia respecto de las regulaciones en ciberseguridad persiguiendo la resiliencia operativa para esta pujante industria.

8. Anexos

Anexo I

I. Información general

- Flujo actualizado de la cadena de producción del banco (detalle de inicio y término actual de la producción de todas las aplicaciones e interfaces).
- Informe de errores o fallas en TI .
- Informe de errores o fallas de Procedimientos.
- Informes de gestión detallado respecto de *uptime* de la infraestructura tecnológica y de comunicaciones.
- Informe de gestión detallado de *uptime*, errores y fallas de las aplicaciones de negocios que se van a externalizar y de aquellas que son interfaces de éstas.
- Estructura detallada de costos del procesamiento de datos actual y posterior al procesamiento externo (para los mismos ítems considerados).
- Nómina detallada por línea de negocios de proyectos que impacten el volumen de transacciones que se procesarán fuera de la institución.

II. Información del proyecto

- Alcance detallado del servicio de procesamiento externo.
- Identificación detallada de las plataformas y aplicaciones de negocios que se procesarán externamente y aquellas que se quedarán en la institución.
- Documentos de respaldo del proyecto de procesamiento externo.
- Detalle de los ítems que se considerarán en el respectivo acuerdo tarifario.
- Informe de análisis y evaluación de riesgo efectuado por una entidad independiente. Se debe incorporar la matriz de riesgos del proyecto y sus respectivos controles o mitigadores.
- Evaluación técnica y financiera del proyecto.
- Evaluaciones efectuadas para la selección de proveedores.

- Detalle de la metodología de traslado utilizada en caso que corresponda (hardware, software y telecomunicaciones).
- Metodología de certificación de pruebas y simulacros.
- Borrador del contrato de servicios (incluyendo todos los anexos) y en el caso de existir subcontratos con terceros estos también deben ser incorporados. Estos documentos deben estar en idioma español.
- Políticas de seguridad de la información del proveedor del servicio.
- Descripción, antecedentes y características técnicas detalladas del sitio de producción y contingencia del proveedor de servicios y las certificaciones con que cuenta.
- Carta GANTT detallada del proyecto de externalización.
- Proceso y herramientas que le permitan a la institución financiera controlar la aplicación de sus políticas y buenas prácticas, en la empresa prestadora del servicio.
- Proceso y herramientas que le permitirán controlar el cumplimiento de los niveles de servicios comprometidos en el contrato suscrito.
- Estructura organizacional que estará encargada de las mantenciones de hardware, software y comunicaciones, especialmente al inicio del proceso externo.
- Políticas y procedimientos que se utilizarán para la mantención de software operativo y comercial, tanto para aquellas que son de índole evolutivo y correctivo.
- Plan de continuidad del negocio que adoptará el banco ante el evento de una contingencia que impida el procesamiento por parte del proveedor o los subcontratados por éste.
- Planes de contingencia previstos para mantener la continuidad operacional de la institución contratante en caso que se produzcan fallas en la comunicación o almacenamiento de la información.

9. Bibliografía

[1] Ualá, «Ualá,» 15 Julio 2019. [En línea]. Available: https://blog.uala.com.ar/educacion-financiera/fintech-que-son-y-para-que-sirven/?utm_source=Google&utm_medium=cpc&utm_campaign=blog%20-%20fintech%20que%20son%20y%20para%20que%20sirven&gclid=EAIaIQobChMIrPHUiIPG6AIVDA-RCh0o7whQEAAYAyAAEgIWrPD_BwE.

[2] IBLISS Digital Security, «Ibliss,» [En línea]. Available: https://www.ibliss.digital/bacen-3-909-e-a-seguranca-digital-para-instituicoes-de-pagamento/.

[3] Fintechnews Singapore, «Finntech news,» 12 Agosto 2020. [En línea]. Available: https://fintechnews.sg/42673/mobilepayments/asia-paytech-emerging/.

[4] Bank For International Settlements, «Fintech developments in the insurance industry,» 2017.

[5] CB Insights, «CB Insights Fintech Report: Q1 2020,» CB Insights, 2020.

[6] CB Insights , «CB Insights Fintech Report: Q2 2020,» CB Insights , 2020.

[7] Cámara de Diputados de México, *Ley Para Regular Las Instituciones de Tecnología Financiera,* Ciudad de México, 2018.

[8] Comisión Nacional Bancaria y de Valores, *Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Financiera,* Ciudad de México, 2018.

[9] The Importance of Cyber Risk Management , «CS Risk Management,» [En línea]. Available: https://www.csriskmanagement.co.uk/the-importance-of-cyber-risk-management/.

[10] C. Wharf, «Cybsafe,» Junio 2020. [En línea]. Available: https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/.

[11] Comisión para el Mercado Financiero, *Recopilación Actualizada de Normas 20-10,* Chile, 2020.

[12] N. Lord, «Digital Guardian,» 12 Septiembre 2018. [En línea]. Available: https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process.

[13] Financial Stability Board, «Effective Practices for Cyber Incident Response and Recovery,» 2020.

[14] P. Sullivan, «Search Security,» Julio 2017. [En línea]. Available: https://searchsecurity.techtarget.com/tip/Why-security-incident-management-is-paramount-for-enterprises.

[15] Finnovista, «Fintech America Latina 2018 - Crecimiento y Consolidación,» 2018.

[16] BACEN, *Circular Nº 3.909,* 16/08/2018.

[17] Banco De Chile, «Superintendencia de Bancos e Instituciones Financieras de Chile,» 2018. [En línea]. Available: http://www.sbif.cl.

[18] C. Farro, «Cesarfarro.Medium.Com,» 10 Junio 2018. [En línea]. Available: https://cesarfarro.medium.com/banco-de-chile-robo-por-m%C3%A1s-de-10-millones-de-d%C3%B3lares-el-24-de-mayo-4a3511afc956.

[19] Editorial Team, «Panorays.com,» 08 Marzo 2020. [En línea]. Available: https://www.panorays.com/blog/third-party-risk-management-cybersecurity/.

[20] Superintendencia de Bancos e Instituciones Financieras de Chile, «www.http://www.sbif.cl/,» [En línea]. Available: http://www.sbif.cl/sbifweb/internet/archivos/publicacion_6593.pdf.

[21] Banco Central De La República Argentina, «bcra.gob.ar,» 15 Noviembre 2019. [En línea]. Available: bcra.gob.ar/Pdfs/Texord/t-rmsist.pdf.

[22] Banco Central De La República Argentina, «http://www.bcra.gob.ar/,» Junio 2020. [En línea]. Available: http://www.bcra.gob.ar/SistemasFinancierosYdePagos/infraestructuras-del-mercado-financiero.asp.

[23] IBM, «IBM Security 2019 Report,» 2019.