

El Riesgo Tecnológico de la Información para Empresas Fintech

María Elvira Neira González¹

Resumen

Las empresas Fintech hacen parte de la disrupción digital de los servicios financieros, estas enfrentan grandes desafíos por el desarrollo de su actividad; de esta manera se busca identificar el aporte que desde la auditoría de sistemas puede hacerse para brindar la asesoría que logre minimizar el impacto de riesgo tecnológico; particularmente en lo que se refiere a la confidencialidad, disponibilidad e integridad de la información.

Se presenta un ejemplo en el que se observan los resultados de la materialización de un riesgo tecnológico, la descripción del impacto a la empresa, así como a los usuarios finales y de la misma manera las acciones que posteriormente fue necesario tomar para reparar los daños ocasionados.

La exploración documental realizada ha demostrado que existe riesgo tecnológico para las empresas Fintech por muchas razones asociadas a su actividad, pero también a identificar las mejores prácticas para gestionar y mejorar la protección de la seguridad de la información, entre

¹ María Elvira Neira González, Administradora de Sistemas Informáticos de la Universidad Santo Tomás. Estudiante Especialización en Auditoría de Sistemas en la Universidad Antonio. Análisis de riesgo tecnológico de la información para empresas Fintech. e-mail: mneira82@edu.co



ellas se mencionan marcos y estándares internacionales como la norma ISO 27001 y el marco de trabajo OWASP.

Palabras Claves: Fintech, riesgos, ISO 27001, seguridad, auditoría.

Abstract

This article talks about Fintech companies, the services they offer and the great challenges they face in the development of their activity; In this way, it seeks to identify the contribution that from the systems audit can be made to provide advice that can minimize the impact of technological risk; particularly with regard to the confidentiality, availability and integrity of the information.

An example is also described in which the technological risk materialized, how it impacted the company, the end users and the actions that were subsequently taken to repair the damage caused.

The documentary exploration carried out in the university's databases leads to the identification of international frameworks and standards such as ISO 27001 and the OWASP framework that seek for organizations to manage information security and in which Fintech can be supported.

Key words: Fintech, risk, ISO 27001, security, audit.



Introducción

El análisis de riesgo TI en las empresas Fintech debe ser considerado una actividad fundamental adicional a su objeto, porque la gran aceptación de estas empresas en el mercado financiero aumenta la demanda de los servicios a un ritmo no previsto y la empresa necesita adoptar un marco de trabajo para el gobierno de los recursos de TI.

El desarrollo de la actividad de una empresa Fintech trae consigo riesgos en todos sus procesos, pero para el caso particular de este artículo, se delimitará el análisis a los riesgos en la seguridad de los activos de información. Pretendiendo así dar respuesta a la medida en que aumentará el riesgo tecnológico de información en las empresas Fintech.

La importancia de un análisis de riesgos radica en que no existe aún reglamentación en Colombia para la operación de empresas Fintech. La Superintendencia Financiera de Colombia otorga licencias para su funcionamiento y participación en el sector financiero mientras se dicta una ley que las incluya.

Se considera que la auditoría de sistemas es vital, puesto que aporta la capacidad de evaluar el sistema de gestión de riesgos, los controles definidos y hacer las recomendaciones para mitigar el riesgo tecnológico en materia de seguridad de la información.

Metodología

La investigación seguirá el método deductivo observando las situaciones y fenómenos desde lo general a lo específico para explicar la relación que se da entre los riesgos tecnológicos de la información y la democratización de los servicios financieros. Se consultará en fuentes secundarias como revistas, artículos científicos e internet con enfoque en la auditoría, seguridad de la información y empresas Fintech.

Resultados y discusiones.

Fintech es la utilización de tecnología para ofrecer financieros innovadores (Arciniegas, 2019). Se identifican cinco tipos de innovación: plataformas de pago, crédito digital, criptoactivos², blockchain³ y financiación colaborativa (crowdfunding)⁴.

² Los Criptoactivos son activos digitales y bienes y servicios basados en criptografía y blockchain (EGA Futura Nube , s.f.).

³ Blockchain es un registro digital de transacciones que se duplica y distribuye a través de la red de sistemas informáticos (Euromoney Learning, s.f.).

⁴ El crowdfunding es el uso de pequeñas cantidades de capital de un gran número de personas para financiar una nueva empresa (Smith, 2020).



El término Fintech es un acrónimo de las palabras en inglés “Finance and Technology” (Holgado, 2017), que involucra las comunicaciones y tecnologías de información en la provisión de servicios financieros (Lucai, 2017)

En vista que la investigación y análisis de los riesgos y desafíos que enfrentan las empresas Fintech ha estado aumentando desde 2017, se han encontrado diferentes referencias con enfoques tales como startup, análisis de riesgo, norma, impacto económico, que permiten conocer más sobre el funcionamiento y el futuro en expansión, tal como se evidencia en la tabla 1:

Tabla 1

Énfasis de la importancia del riesgo Fintech

Identificación	Objetivo general	Categorías	Resultados
BBVA¿Qué es el fintech? Innovación en servicios financieros. 05 sep 2019 (BBVA, 2019)	Definir fintech	financiamiento, tecnología, banca online	proyectar startups basadas en nuevas formas de servicios financieros.
Deloitte. Instituciones de tecnología financiera. 2019 (Deloitte, 2019)	Asesoría en riesgos.	Servicios Deloitte. Identificación de riesgos.	Presentar los escenarios de riesgo en una empresa Fintech.
Javier Raventós. EMPRESAS FINTECH EN COLOMBIA Sus retos y logros. Junio 2020 (Raventós, 2020)	Hacer una radiografía de la industria Fintech en Colombia a través de la presentación de las empresas que colaboran entre sí.	Fintech, Colombia, Servicios financieros, Banca	compilación de la industria Fintech en Colombia.



Identificación	Objetivo general	Categorías	Resultados
Carolina Arciniegas ¿Qué es y cómo funciona el Fintech en Colombia?.lunes, 9 de septiembre de 2019 (Arciniegas, 2019)	Describir los principales tipos de innovación que trae Fintech a Colombia y como está regulado.	Fintech, regulación, Super Intendencia Financiera	Describe los desafíos que trae Fintech para el sector financiero en Colombia.
Antonio Martín Holgado. LOS RIESGOS FINANCIEROS DE LAS FINTECH.Agosto 2017 (Holgado, 2017)	Dar a conocer los riesgos financieros en que incurren las Fintech centrándose en su carácter innovador con respecto a las entidades financieras tradicionales.	Fintech, Riesgos, Tecnología, Innovación, Ciberseguridad.	Presenta la evolución de los riesgos financieros, destacando que los nuevos riesgos no están incluidos en la normativa vigente.
Finnovating News. EL RIESGO ECONÓMICO DE LOS CIBERATAQUES PARA LAS FINTECH.31 enero 2017 (https://www.finnovating.com, 2017)	Distinguir las principales amenazas para las empresas Fintech.	Fintech, amenaza digital, ciberataque,	El impacto económico de un ciberataque para las empresas Fintech.

Sin duda alguna se hace necesario el control de riesgo dado que falta una ley que reglamente la actividad de las Fintech en Colombia. En países como México, La Unión Europea y Reino Unido ya tienen legislación al respecto; para México se emitió la ley Fintech que entró en vigor en septiembre de 2018 y regula los pagos electrónicos, el financiamiento colectivo, la administración de activos virtuales y la asesoría financiera a través de canales digitales, sumando así mejoras importantes en materia de seguridad financiera (Rodríguez, 2018)

Los riesgos a los que se pueden enfrentar las empresas Fintech (Deloitte, 2019) se dan en diferentes ámbitos tales como aspectos legales, plan de negocio, políticas y proyectos de



manuales, información de accionistas, gobierno corporativo e información en materia de riesgo tecnológico tal como se observa la figura 1:



Figura 1. Escenarios de riesgo Empresa Fintech. Fuente <https://www2.deloitte.com>

Ahora bien, el análisis de riesgo del presente artículo, hace enfoque en el riesgo tecnológico y particularmente en confidencialidad, disponibilidad e integridad de la información.

La seguridad de la información es un gran desafío para una empresa Fintech (Arciniegas, 2019). Al aumentar los datos almacenados, aumenta la exposición para que los datos sean objeto de un ataque. (Holgado, 2017).

El impacto de los riesgos que enfrentan las Fintech es del tipo económico, reputacional, legal, interrupción de los servicios entre otros, debido al crecimiento de ataques y explotación de



vulnerabilidades del software. Estos escenarios representan una seria amenaza para el desarrollo Fintech (<https://www.finnovating.com>, 2017).

Un ejemplo de ataque es el ocurrido a la empresa Talk Talk en 2015 donde fueron robados los datos de los clientes, cuentas bancarias y tarjetas de crédito. La pérdida económica fue de 60.000.000 de libras y medio millón correspondió a la multa inicial; una de las mayores que se haya impuesto en el Reino Unido.

El costo más grande vino después por la salida de más de cien mil clientes debido a la pérdida de confianza por parte de los usuarios. Para mitigar el impacto en la reputación la empresa tuvo que invertir una gran fuerza en servicio al cliente, marketing, seguridad para evitar futuros ataques y relaciones públicas para recuperar la confianza perdida.

Como se puede observar las empresas Fintech necesitan protegerse, ya que su modelo de negocio las coloca en un nivel de vulnerabilidad muy alto y un gran peso corresponde al cómo están construidas las aplicaciones de estas empresas.

Los incidentes de seguridad pueden presentarse por desconocimiento o negligencia de las personas o de forma deliberada, lo que representa un ataque, por lo tanto, se considera la aplicación de distintas perspectivas para aumentar y mejorar la seguridad de la información (www.welivesecurity.com, 2015).

Aquí cobra relevancia la participación de la auditoría de sistemas, para evaluar la construcción o adquisición de aplicaciones a la medida para empresas Fintech. Importante revisar el modelo de madurez de la seguridad en el desarrollo de software que tiene la empresa proveedora o constructora (alvanti, 2019).

Existe todo un Framework, OWASP⁵, abierto basado en proyectos que lucha por mitigar las vulnerabilidades en el software en el que se pueden apoyar las Fintech para implantar y/o exigir y asegurar buenas prácticas de seguridad en el ciclo de vida de los desarrollos y al que los auditores pueden referenciar o verificar si ya se tiene.

Las Fintech pueden implementar la norma ISO 27001, porque esta norma describe cómo gestionar la seguridad de la información, si se tiene en cuenta que proporciona una metodología para implementar la seguridad de la información en cualquier organización, el objetivo es proteger la confidencialidad, integridad y disponibilidad de la información y su filosofía está basada en la gestión del riesgo: investigar donde están los riesgos y luego tratarlos sistemáticamente (27001academy, s.f.), como se ilustra en la figura 2:



Figura 2. Estructura de ISO 27001. Fuente: <https://advisera.com/>

⁵ Open Web Application Security Project, (owasp.org, s.f.)



La auditoría interna a la que se refiere la cláusula 9.2 de la norma ISO 27001 (Irwin, 2020) se considera una actividad necesaria e importante para asegurar que la gestión del sistema de seguridad de la información se está ejecutando de acuerdo a los requerimientos que se mencionan en la misma y se hará teniendo en cuenta los siguientes pasos que pueden ser utilizados por cualquier Fintech. En la tabla 2 se describen los pasos para realizar la auditoría interna:

Tabla 2

Pasos para realizar auditoría interna

Actividad	Tareas
Revisión de la documentación	Se debe revisar la documentación que se creó al implementar el SGSI. Identificar las partes interesadas en el SGSI.
Revisión de la gestión	Establecer el alcance de la auditoría según los dos puntos anteriores. Acordar con la gerencia los recursos y el momento de auditoría. Establecer los puntos de control para entregar avances de la auditoría.
Revisión de campo	Ejecución de la auditoría observando y evaluando cómo funciona el SGSI. Elaboración de entrevistas al personal involucrado en el SGSI. Realizar las pruebas a los controles para la evaluar la efectividad.
Análisis	Clasificación de las evidencias. Revisión de las evidencias en relación con el plan de tratamiento de riesgos y los objetivos de control. Identificar la necesidad de pruebas adicionales.
Reporte	Presentación de los hallazgos a la gerencia en un informe. El informe incluirá el análisis de los hallazgos, las conclusiones y las acciones correctivas y las limitaciones al alcance.

Fuente: <https://www.itgovernance.co.uk>



Los pasos descritos en la tabla corresponden al ciclo de auditoría para ser aplicado por la empresa Fintech y verificar así el cumplimiento de mitigación de los riesgos de seguridad de la información.



Conclusiones

Quiero concluir que la democratización que traen las Fintech a los servicios financieros es un aspecto positivo para los usuarios, sin embargo, el aumento de la demanda y la oferta utilizando el medio digital pone de manifiesto la necesidad de proteger la información utilizada en el desarrollo de la actividad mediante la aplicación de estándares y normas internacionales, y que, para el caso de este artículo, sugiero la norma ISO 27001.

Al mismo tiempo concluyo que la auditoría de sistemas toma aquí gran relevancia dado que el aporte en la evaluación del cumplimiento del análisis de riesgo del sistema de gestión de la información, en la evaluación de los controles existentes y las acertadas recomendaciones que fuesen necesarias, contribuirán a minimizar el impacto de las vulnerabilidades presentes en la confidencialidad, disponibilidad e integridad de la información para la actividad de las Fintech.



Referencias

- 27001academy. (s.f.). <https://advisera.com>. Obtenido de <https://advisera.com/>:
<https://advisera.com/27001academy/es/que-es-iso-27001/>
- alvantia. (07 de 11 de 2019). <https://www.alvantia.com>. Obtenido de <https://www.alvantia.com>:
<https://www.alvantia.com/que-riesgos-corre-una-fintech-por-publicar-aplicaciones-web-no-seguras-y-como-puede-protegerse/>
- Arciniegas, C. (9 de 9 de 2019). *¿Qué es y cómo funciona el Fintech en Colombia?* Obtenido de *¿Qué es y cómo funciona el Fintech en Colombia?*:
<https://www.asuntoslegales.com.co/.../que-es-y-como-funciona-el-fintech-en-colombia-2905585>
- BBVA. (5 de 9 de 2019). *¿Qué es el fintech? Innovación en servicios financieros | BBVA*. Obtenido de *¿Qué es el fintech? Innovación en servicios financieros | BBVA*:
<https://www.bbva.com/es/que-es-el-fintech/>
- Deloitte. (2019). <https://www2.deloitte.com>. Obtenido de <https://www2.deloitte.com/>:
<https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/2019/Fintech-info.pdf>
- EGA Futura Nube . (s.f.). <https://www.egafutura.com/>. Obtenido de <https://www.egafutura.com/>:
<https://www.egafutura.com/glosario/criptoactivos#Glosario-Definicion-Extendida>
- Euromoney Learning. (s.f.). <https://www.euromoney.com/>. Obtenido de <https://www.euromoney.com/>: <https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain>



Holgado, A. M. (8 de 2017). <https://repositorio.comillas.edu/>. Obtenido de

<https://repositorio.comillas.edu/>:

<https://repositorio.comillas.edu/jspui/bitstream/11531/24228/1/TFM000775.pdf>

<https://www.finnovating.com>. (31 de 1 de 2017). Obtenido de <https://www.finnovating.com>:

<https://www.finnovating.com/news/riesgo-economico-los-ciberataques-las-fintech/>

<https://www.finnovating.com>. (31 de 01 de 2017). Obtenido de <https://www.finnovating.com>:

<https://www.finnovating.com/news/riesgo-economico-los-ciberataques-las-fintech/>

Irwin, L. (19 de 5 de 2020). <https://www.itgovernance.co.uk/>. Obtenido de

<https://www.itgovernance.co.uk/>: <https://www.itgovernance.co.uk/blog/how-to-conduct-an-iso-27001-internal-audit>

Lucai, A. (30 de 11 de 2017). <http://blognewdeal.com>. Obtenido de <http://blognewdeal.com>:

<http://blognewdeal.com/andrea-lucai/fintech-el-nuevo-marco-tecnologico-de-las-finanzas/>

owasp.org. (s.f.). Obtenido de owasp.org: <https://owasp.org/>

Raventós, J. (6 de 2020). *¿Qué es y cómo funciona el Fintech en Colombia?* Obtenido de *¿Qué es y*

cómo funciona el Fintech en Colombia?: <https://www.asuntoslegales.com.co/.../que-es-y-como-funciona-el-fintech-en-colombia-2905585>

Rodriguez, E. (21 de 12 de 2018). <https://blog.cobiscorp.com/>. Obtenido de

<https://blog.cobiscorp.com/>: <https://blog.cobiscorp.com/ley-fintech-mexico-latinoamericano>



Smith, T. (7 de 9 de 2020). <https://www.investopedia.com/>. Obtenido de

<https://www.investopedia.com/>:

<https://www.investopedia.com/terms/c/crowdfunding.asp>

www.welivesecurity.com. (2 de 7 de 2015). Obtenido de www.welivesecurity.com:

<https://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/>