

**UNIVERSIDAD MAYOR, REAL Y PONTIFICIA DE SAN
FRANCISCO XAVIER DE CHUQUISACA**

VICERRECTORADO

CENTRO DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN



“ANÁLISIS DEL RIESGO OPERATIVO EN LA BANCA DIGITAL DE BOLIVIA”

**TRABAJO EN OPCIÓN A DIPLOMADO EN BANCA Y TRANSFORMACIÓN
DIGITAL VERSIÓN I**

FLORES TORREZ NANDY PAMELA

SUCRE - BOLIVIA

2024

CESIÓN DE DERECHOS

Al presentar este trabajo como requisito previo a la obtención del Diploma en Banca y Transformación Digital de la Universidad Mayor, Real y Pontificia de San Francisco Xavier de Chuquisaca, autorizo al Centro de Estudios de Posgrado e Investigación o a la Biblioteca de la Universidad para que se haga de este trabajo un documento disponible para su lectura, según normas de la Universidad.

También cedo a la Universidad Mayor, Real y Pontificia de San Francisco Xavier de Chuquisaca, los derechos de publicación de este trabajo o parte de él, manteniendo mis derechos de autor hasta un periodo de 30 meses posterior a su aprobación.

Flores Torrez Nandy Pamela

Sucre, agosto de 2024

DEDICATORIA

El presente trabajo de investigación dedico a mis padres Carlos Martin Flores y Elba Antonia Torrez, porque supieron educarme con buenos principios y valores, por darme apoyo moral y económico, y me ayudaron a afrontar y superar momentos difíciles.

Flores Torrez Nandy Pamela

AGRADECIMIENTO

Para la realización del presente trabajo de investigación agradezco a Dios por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía en este periodo de estudios para no rendirme.

Agradecer a mi familia por todo el apoyo brindado y por aquellos consejos brindados en esta etapa de mis estudios.

También va dedicado a mis docentes de la Universidad Mayor Real y Pontificia de San Francisco Xavier de Chuquisaca de la carrera de Administración Financiera, que me acompañaron y enseñaron desde el primer momento que ingrese a esta hermosa carrera y estuvieron ahí motivándome a seguir adelante.

Flores Torrez Nandy Pamela

ÍNDICE

CESIÓN DE DERECHOS	i
DEDICATORIA	ii
AGRADECIMIENTO	iii
ÍNDICE	iv
ÍNDICE DE TABLAS.....	viii
ÍNDICE DE GRÁFICOS.....	ix
ÍNDICE DE CUADROS.....	x
RESUMEN	xi
CAPÍTULO I	1
INTRODUCCIÓN.....	1
1.1 Antecedentes.....	1
1.2 Justificación	3
1.3 Metodología	3
1.3.1 Enfoque de investigación	3
1.3.1.1 Enfoque cualitativo	3
1.3.2 Tipo de investigación.....	4
1.3.2.1 Investigación documental.....	4
1.3.2.2 Investigación descriptiva	4
1.3.3 Métodos de investigación.....	4
1.3.3.1 Método histórico	4
1.3.3.2 Método analítico	5
1.3.3.3 Método inductivo.....	5
1.3.3.4 Método sintético.....	5
1.3.4 Técnicas.....	6
1.3.4.1 Revisión documental	6
1.4 Objetivos	6
1.4.1 Objetivo general.....	6
1.4.2 Objetivos específicos.....	6

CAPÍTULO II	7
DESARROLLO	7
2.1 Marco teórico	7
2.1.1 Marco conceptual	7
2.1.1.1 Sistema financiero	7
2.1.1.2 Banco	7
2.1.1.3 Banca electrónica	8
2.1.1.4 Banca digital	8
2.1.1.5 Banca móvil	8
2.1.1.6 Banca por internet	8
2.1.1.7 Gestión de riesgo	9
2.1.1.8 Riesgo operativo.....	9
2.1.1.9 Otros riesgos	10
2.1.1.9.1 Riesgo de crédito.....	10
2.1.1.9.2 Riesgo de mercado	10
2.1.1.9.3 Riesgo tecnológico	10
2.1.1.9.4 Riesgo reputacional.....	11
2.1.1.9.5 Riesgo legal	11
2.1.1.10 Canales electrónicos de pago.....	11
2.1.1.11 Transacciones bancarias	12
2.1.1.12 Código QR	12
2.1.1.13 Fraude.....	12
2.1.1.14 Fraude con transferencias de dinero	12
2.1.1.15 Protección de datos.....	13
2.1.2 Marco contextual	13
2.1.2.1 Sistema Financiero en Bolivia	13
2.1.2.2 Características del Sistema Financiero de Bolivia.....	13

2.1.2.3 Ley 393, Ley de Servicios Financieros	14
2.1.2.4 Autoridad de Supervisión del Sistema Financiero – ASFI.....	16
2.1.2.5 Banca digital de Bolivia	16
2.1.2.6 Entidades financieras que operan en Bolivia con una banca digital	17
2.1.2.7 Adopción del sistema QR	19
2.2 Información y datos obtenidos	20
2.2.1 Transacciones realizadas en la banca digital de Bolivia	20
2.2.1.1 Transacciones de Órdenes Electrónicas de Transferencia de Fondos	20
2.2.1.2 Transacciones a partir de la tarjeta de débito.....	21
2.2.1.3 Transacciones a partir de la tarjeta de crédito.....	22
2.2.1.4 Transacciones a partir de la billetera móvil.....	23
2.2.1.5 Transferencias a partir de cobros y pagos por código QR.....	24
2.2.2 Riesgo operacional que emergen en las transacciones digitales	26
2.2.2.1 Fraude y ciberataques.....	26
2.2.2.2 Errores humanos	30
2.2.2.3 Fallas técnicas	30
2.2.2.4 Riesgo en la seguridad de la información.....	30
2.2.2.5 Problemas de infraestructura	31
2.2.2.6 Riesgo regulatorio y de cumplimiento.....	31
2.2.2.7 Riesgo de confianza y reputacional	32
2.3 Análisis y discusión.....	32
2.3.1 Gestión de riesgos operativos de acuerdo a la Ley N.º 393 Artículo 449 mediante ASFI	32
2.3.2 Directrices básicas para la gestión del riesgo operativo	32
2.3.3 Actividades de control del riesgo operativo	34
2.3.4 Marco Legal de protección de datos en el sector financiero	36
2.3.4.1 Normativa general	36

2.3.4.2 Gestión de datos personales y financieros	37
2.3.5 Impacto de la tecnología y su inclusión en la banca	38
CAPÍTULO III	41
CONCLUSIONES	41
BIBLIOGRAFÍA	43
ANEXOS	48

ÍNDICE DE TABLAS

Tabla 1: Entidades de Intermediación Financiera	14
Tabla 2: Entidades bancarias que operan en Bolivia	18

ÍNDICE DE GRÁFICOS

Gráfica 1: Entidades de Intermediación Financiera.....	14
--	----

ÍNDICE DE CUADROS

Cuadro 1: Transacciones digitales en las entidades financieras	26
--	----

RESUMEN

El enfoque del presente trabajo de investigación está relacionado con el crecimiento de las transacciones digitales bancarias en Bolivia, estos servicios digitales fueron impulsados por el avance de la tecnología. Este crecimiento, aunque positivo, también trajo consigo los riesgos operacionales los cuales dependen de un análisis y gestión adecuado por parte de las instituciones financieras cuyo propósito es evitar, prevenir futuras pérdidas, es por ello que el objetivo general del presente trabajo es analizar los riesgos operativos que emergen de las transacciones en la banca digital de Bolivia. Para ello se utilizó los métodos histórico, analítico, inductivo y sintético. De este modo se pudo reflejar como resultado la adaptación de la población boliviana hacia las transacciones digitales, especialmente con el código QR, que es el más utilizado por diferentes sectores sociales, donde se refleja como los bolivianos están interactuando con el sistema financiero digital. Sin embargo, el aumento de las transacciones trajo de la mano preocupaciones significativas, como los fraudes, que es la posibilidad que los usuarios sean víctimas de estafas, vulnerabilidad de las plataformas digitales, ataques cibernéticos y una variedad de ciberdelitos, que están relacionados en las transacciones de la banca digital. Finalmente se concluye que es muy importante que se implemente medidas de seguridad y se promueva la educación financiera entre los usuarios obteniendo seguridad y confianza en los servicios digitales, asimismo, es de vital importancia el cumplimiento de la práctica de gestión de riesgo operacional con el fin de minimizar los posibles inconvenientes sin que necesariamente se haya sufrido algún evento que dañe a las instituciones y usuarios.

CAPÍTULO I

INTRODUCCIÓN

1.1 Antecedentes

Bolivia país que desde su independencia ha enfrentado diversas crisis, que han afectado su desarrollo económico y social de los cuales han sido provocados por fenómenos naturales como sequías o epidemias. Sin embargo, el año 2020 se destacó como un periodo crítico en la historia, por lo que la crisis del coronavirus y el distanciamiento social han impulsado un aumento inmediato del uso de canales digitales en la banca. La innovación y digitalización de los servicios y productos bancarios en la actualidad, ya no es solo un tema estratégico de corto o mediano plazo, ahora es una urgencia, para que los bancos que quieran ser competitivos ingresen a la nueva realidad de avances tecnológicos.

La consolidación de Instituciones Financieras es cada vez más grande y sofisticadas por lo que ha sido impulsada principalmente por el desarrollo de servicios financieros, en tanto, la sofisticación de la tecnología, la desregulación financiera y la globalización se dan en múltiples mercados, por lo cual sus operaciones se han tornado más complejas, generando el incremento de sus perfiles de riesgo. Debido a esto, la gestión del riesgo operacional representa hoy uno de los grandes desafíos que enfrentan las Instituciones Financieras, como consecuencia, si no controlan el riesgo operacional al que se encuentran expuestas pueden sufrir daños (Shaw, 2017).

Según Palacios (2024) es necesario la anticipación y adaptación a entornos cambiantes por parte de las entidades financieras, pues es importante que las instituciones financieras adopten un enfoque integral y adaptativo para una gestión eficaz de riesgos operativos en un entorno dinámico y desafiante. A su vez, Cocarico (2023) indica que la evolución de la banca electrónica desde sus inicios, llegando a comprender o identificar el trasfondo de como los componentes electrónicos y digitales se fueron alineando con el modelo de la banca tradicional con la invención de dispositivos como los cajeros automáticos, las primeras tarjetas para realizar las transacciones, la aparición de internet y demás en los países más avanzados en innovación y materia financiera. En el desarrollo de las tecnologías de la información y las comunicaciones (TIC) hasta los contextos actuales, se describe como la tecnología se fue desarrollando e impactando en la vida cotidiana, en todo lo que nos rodea especialmente con

la llegada del internet, las computadoras, los teléfonos móviles y demás dispositivos. Llegando a modificar incluso el comportamiento de los consumidores y que la banca misma llega a utilizarla dentro de su modelo de negocio para realizar transacciones, ofrecer sus servicios o productos financieros, teniendo cajeros automáticos, tarjetas electrónicas, sitios web y otras herramientas por los cuales se realizan estas operaciones digitales.

Asimismo, Mastercard Foundation y el Programa de IFC (2016) indica que en las últimas décadas ha visto una ola de servicios financieros innovadores que tiene por objetivo atender a las poblaciones desbancarizadas en mercados emergentes. Individuos de bajo ingresos, microempresarios y poblaciones rurales están teniendo acceso a servicios financieros, que con las amplias oportunidades ofrecidas por nuevas tecnologías y las operaciones de negocios innovadoras, también vienen nuevos riesgos. Los riesgos relacionados con la implementación de los servicios financieros digitales se extienden mucho más allá de los riesgos operacionales y técnicos. Para que la industria de la inclusión financiera pueda capitalizar plenamente los beneficios de los servicios financieros digitales, es importante que los riesgos asociados sean entendidos y abordados en forma educada.

De acuerdo a lo mencionado, se puede decir que los riesgos operativos fueron la causa fundamental de muchas fallas financieras que se suscitaron en las últimas décadas, donde prevalece los errores humanos, el fraude, robo, fallas de procesos, errores del sistema y peligros externos, son los factores que generan el riesgo, sumado a las tendencias recientes como la globalización, la conectividad global a Internet y las dependencias de la cadena de valor han hecho que los riesgos operativos sean más importantes que nunca.

Como se puede apreciar en anteriores párrafos, se destaca la importancia de analizar el riesgo operativo en la banca digital de Bolivia, en el país, se han desarrollado normas con el fin de regular y prevenir los riesgos operativos, al parecer encontramos un cuadro bien desarrollado y establecido que actualmente es aplicado en las entidades financieras, sobre el servicio de transacciones digitales. Pero hay algo que está provocando pérdidas económicas que se tienen que identificar y subsanar para el beneficio de la sociedad Bolivia.

Es por ello que surge la siguiente pregunta de investigación ¿De qué manera se puede realizar un análisis de los riesgos operativos a los cuales se encuentra expuesta la banca digital en Bolivia?

1.2 Justificación

Cada vez los hackers y los estafadores son más afluentes, los cuales infringen las medidas de seguridad de los bancos para cometer actos delictivos, es así que el objetivo de la presente investigación, es analizar los riesgos operacionales que emergen en las transacciones de la banca digital. Por ello, es de vital importancia prestar especial atención a los factores de riesgo operativo asociados a la sofisticación de los servicios financieros, la modernización continua de la tecnología y las telecomunicaciones incursionan en nuevos mercados y las innovaciones financieras.

En ese sentido, se busca concientizar a los clientes financieros sobre el adecuado manejo y uso de los canales digitales y a la vez prevenir posibles pérdidas o fraudes en las transacciones bancarias, en vista que la ciberdelincuencia se está viendo de forma más frecuente y se debe de trabajar en estrategias, mecanismos y control del riesgo operativo en la banca digital del país. El tema es pertinente, por las problemáticas en el sistema financiero, que se vive en la actualidad, a su vez realizar este estudio es fundamental para mantener la estabilidad y confianza del sistema financiero en la era digital, protegiendo tanto a los bancos como a sus clientes de pérdidas y amenazas.

1.3 Metodología

1.3.1 Enfoque de investigación

1.3.1.1 Enfoque cualitativo

Por enfoque cualitativo se entiende, al procedimiento metodológico que utiliza palabras, textos, discursos, dibujos, gráficos e imágenes. La investigación cualitativa estudia diferentes objetos para comprender la vida social del sujeto a través de los significados desarrollados por éste. también se sustenta en evidencias que se orientan más hacia la descripción profunda del fenómeno con la finalidad de comprenderlo y explicarlo a través de la aplicación de métodos y técnicas derivadas de sus concepciones y fundamentos (Flores, 2019).

1.3.2 Tipo de investigación

1.3.2.1 Investigación documental

La investigación documental es un proceso basado en la búsqueda, recuperación, recolección, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales, impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos (Arias, 2006).

La investigación es de tipo documental, debido a que se recolectó información de los antecedentes históricos de los riesgos operativo que se han suscitado en el mundo y en especial en el lugar de objeto de estudio que es Bolivia.

1.3.2.2 Investigación descriptiva

La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refieren, en la investigación descriptiva se trata sobre la realidad de los hechos y su correcta interpretación (Arias, 2006).

Es investigación descriptiva, en vista que se caracterizó el Sistema Financiero de Bolivia y se describió las normativas de regulación al riesgo operativo.

1.3.3 Métodos de investigación

1.3.3.1 Método histórico

El método histórico es utilizado para conocer un hecho a través de indicios pasados. Ellos se encuentran recogidos en fuentes, ya sean escritas u orales. Estas son las encargadas de dar la información y el historiador, a través del método, es el encargado de interpretarlas y clasificarlas para intentar construir la realidad del hecho pasado. Sin un método histórico las acciones investigadas quedan sujetas a la interpretación del investigador por su criterio y no por el debido contraste de las fuentes y validación de las mismas (Hérmendez & Holguín, 2020).

Este método permitió recopilar información de hechos trascendentales en el sistema financiero, banca digital tanto nacionales e internacionales.

1.3.3.2 Método analítico

El método analítico es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías (Ruiz, 2007).

Se utilizó la información recabada, descomponiendo en un análisis profundo mediante el cual se observó las causas, la naturaleza y los efectos del problema pertinente, mediante este método analítico se logró entender la normativa y tipos operacionales en la banca digital.

1.3.3.3 Método inductivo

El método inductivo es un enfoque que se utiliza en la investigación y el razonamiento científico, que busca inferir conclusiones generales a partir de observaciones específicas. Es decir, este método parte de hechos concretos y particulares para llegar a una conclusión general, se basa en la observación y la recolección de datos empíricos para generar patrones y generalización. En este proceso, el investigador recopila información a través de sus sentidos y la organiza de manera sistemática para encontrar regulaciones y patrones (Suárez, 2024).

El método inductivo permitió formular, determinar las conclusiones del presente trabajo de investigación a partir del análisis de los distintos tipos de riesgos que se suscitan en las transferencias de la banca digital.

1.3.3.4 Método sintético

El método sintético es un proceso analítico de razonamiento que busca reconstruir un suceso de forma resumida, valiéndose de los elementos más importantes que tuvieron lugar durante dicho suceso. En otras palabras, el método sintético es aquel que permite a los seres humanos realizar un resumen de algo que conocemos. La síntesis es un proceso mental que busca comprimir la información presente en nuestra memoria. Este proceso opera de tal forma que

somos capaces de identificar todo aquello que conocemos y abstraer las partes más importantes y particularidades de ello. De esta forma, somos capaces de reintegrar estas partes, creando una versión corta que pueda expresar la información más importante sobre lo conocido (Teyes, 2019).

Este método se utilizó en el presente trabajo como una herramienta de análisis, rescatando las definiciones y los aspectos más relevantes de cada hecho suscitado en lo que concierne al sistema financiero, riesgo operativo y banca digital.

1.3.4 Técnicas

1.3.4.1 Revisión documental

La revisión documental se toma como punto de partida en el análisis de fuentes documentales, mediante una lectura general de los textos, se iniciará la búsqueda de los hechos presentes en los materiales escritos consultados; esta lectura inicial, será seguida de varias lecturas más detenidas y rigurosas de los textos, a fin de captar sus planteamientos esenciales y aspectos lógicos de sus contenidos y propuestas así es importante, extraer los datos bibliográficos útiles para el estudio que se está realizando (Hurtado, 2006).

Se realizó una revisión documental de los avances tecnológicos que se está dando en las bancas bolivianas, a la vez permitió localizar, obtener y consultar material escrito y bibliográfico, que ayudó a una adecuada comprensión y estudio profundo del tema a investigar.

1.4 Objetivos

1.4.1 Objetivo general

Analizar los riesgos operativos que emergen de las transacciones realizadas en la banca digital de Bolivia.

1.4.2 Objetivos específicos

- ✓ Establecer la base teórica – normativa, relacionada a la banca digital.
- ✓ Caracterizar las transacciones realizadas en la banca digital de Bolivia.
- ✓ Identificar el riesgo operacional que emergen en las transacciones digitales.

CAPÍTULO II

DESARROLLO

2.1 Marco teórico

2.1.1 Marco conceptual

2.1.1.1 Sistema financiero

El sistema financiero es el medio, en el cual se realizan los movimientos de recursos financieros entre aquellos agentes económicos deficitario y superavitarios en sus ahorros. Estos movimientos de recursos se efectúan a través de un conjunto orgánico de instituciones que generan, administran y canalizan los recursos del ahorro y la inversión (Ticona Canahui, 2015).

Para el Banco Central de Bolivia el sistema financiero es: Es el conjunto de entidades financieras autorizadas por la Autoridad de Control y Supervisión del Sistema Financiero – ASFI, que cumple el rol de intermediarios financieros entre la oferta y la demanda de recursos monetarios. ASFI es una institución de derecho público y de duración indefinida, con personalidad jurídica, patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, con jurisdicción, competencia y estructura de alcance nacional, bajo tuición del Ministerio de Economía y Finanzas Públicas y sujeta a control social (Cooperativa San Antonio SL, 2018).

2.1.1.2 Banco

Los bancos hacen muchas cosas, pero su función principal es captar fondos, depósitos, de gente con dinero, aglomerarlos y prestarlos a quienes lo necesitan. Un banco es un intermediario entre los depositantes (quienes le prestan dinero) y los prestatarios (a quienes les presta dinero). Lo que paga por los depósitos y lo que cobra por los préstamos que otorga, son en ambos casos intereses. Tanto los depositantes como los prestatarios pueden ser personas y hogares, empresas financieras y no financieras, o gobiernos nacionales y locales (Gobat, 2012).

2.1.1.3 Banca electrónica

Es la prestación de servicios financieros a través de internet u otros medios electrónicos y digitales sin necesidad de presencia física del cliente en las oficinas de la entidad financiera (Banco Central de Bolivia BCB, 2023). A su vez, Francisco Coll (2023) indica los términos banca electrónica, banca virtual y banca online se utilizan a menudo de manera intercambiable para referirse al mismo concepto todos estos terminados describe el servicio ofrecido por las entidades financieras y realizar transacciones utilizando dispositivos electrónicos por internet.

2.1.1.4 Banca digital

La banca digital es una versión virtual de los bancos a través de la cual una persona puede gestionar sus finanzas y realizar acciones como abrir una cuenta bancaria, domiciliar recibos o realizar transferencias y envíos instantáneos de dinero, entre otras. Esta se lleva a cabo a través de bancos 100% online que no tienen sucursales bancarias u oficinas a las que acudir de manera presencial; o bien, por medio de bancos tradicionales que ofrecen versiones móviles y en línea. Por tanto, si hay dos cosas que no pueden faltar a la hora de operar con banca digital, estas son contar con un dispositivo electrónico (móvil, tableta u ordenador) y acceso a Internet (Universidad Europea, 2023).

2.1.1.5 Banca móvil

La banca móvil es la banca y sus servicios presente en el teléfono celular. Para los bancos es indispensable tener una banca móvil ya que pueden ir ofreciendo servicios totalmente digitales, que crean valor y ventajas competitivas por sobre sus competidores, toda vez, se pueda captar el mayor número de clientes y que estos sientan una experiencia positiva por los servicios recibidos (Ticona, 2023).

2.1.1.6 Banca por internet

La banca por internet o en línea es un canal digital que engloba las herramientas que le permiten al cliente realizar distintas transacciones como transferencias a terceros, interbancarias, pagos de servicios y de tarjetas, giros nacionales, entre otras operaciones a través de la computadora sin acudir a una agencia bancaria, generalmente se da a través del sitio Web de un banco con una computadora de escritorio o portátil (Ticona, 2023).

2.1.1.7 Gestión de riesgo

Es el proceso de identificar medir, monitorear, controlar, mitigar y divulgar todos los riesgos a los cuales la Entidad de Intermediación Financiera se encuentra expuesta, en el marco del conjunto de objetivos, políticas, procedimientos y acciones, establecidas por la entidad para este propósito.

La gestión integral de riesgo debe ser entendida como un proceso que conlleva una amplia gama de elementos, definiciones y la realización de una serie de actividades por parte de las EIF, con el propósito de hacer frente a los diversos riesgos a los que se exponen las operaciones que realiza. Este proceso debe ser estructurado, consistente y continuo, implementado a través de toda la organización. De manera puntual, la gestión integral de riesgo implica que las EIF implementen sistemas de identificación, medición, monitoreo, control, mitigación y divulgación de todos los riesgos inherentes a sus actividades, bajo un enfoque global. Este requiere que las entidades tengan una visión clara de sus fortalezas tácticas y de sus debilidades potenciales, a fin de diseñar las metodologías más apropiadas a sus características particulares de tamaño y grado de desarrollo, así como a su grado de preparación (Guías para la Gestión de Riesgos , 2008).

2.1.1.8 Riesgo operativo

La definición de riesgo operativo de Basilea II; es el riesgo de pérdida directa o indirecta como resultado de procesos inadecuados, donde se da una falla interna humana, también puede ser por los sistemas inadecuados o de eventos de carácter externo. Muchos bancos son suministrados por servidores externos y expertos (outsourcing), quienes se encargan de la parte operativa y el mantenimiento de sus actividades de banca digital, sin embargo, el outsourcing también de cierta forma expone al banco al riesgo operacional, si no se aplica la fidelidad al banco (Salas, 2021).

Los malos usos del cliente tanto intencionados como inadvertidos, constituyen otra de las fuentes de riesgo operacional, el riesgo puede ser mayor si el banco no previene adecuadamente a sus clientes sobre las precauciones de seguridad puede dar lugar a importantes pérdidas financieras para el banco.

2.1.1.9 Otros riesgos

2.1.1.9.1 Riesgo de crédito

Es donde la contraparte no cumple su obligación, por su entero valor, los bancos que operan en el segmento de la banca digital pueden extraer créditos a través de canales no tradicionales y expandir su mercado más allá de las fronteras geográficas tradicionales. La utilización de los procedimientos inadecuados para determinar la capacidad crediticia de los prestatarios que piden créditos en remoto, pueden elevar el riesgo de crédito, los bancos que operan en programas de pago con dinero digital-electrónico afrontan el riesgo de créditos si una tercera parte inmediata intermediaria incumple sus obligaciones con respecto al pago, de igual forma los bancos que compran dinero digital de un emisor para revenderlo a sus clientes están también expuestos al riesgo de crédito en el caso de que el emisor falle en sus obligaciones para redimir el dinero digital (Dominguez, 2023).

2.1.1.9.2 Riesgo de mercado

El riesgo de mercado es el riesgo de pérdidas, en caso de movimientos en los precios del mercado incluyendo los tipos de cambio, los bancos que aceptan moneda extranjera en pago de dinero digital están sujetos a perder ya que se manejan en este ámbito que todo es cambiante y nada es fijo.

2.1.1.9.3 Riesgo tecnológico

El riesgo tecnológico tiene varias implicaciones para los proveedores, con la incapacidad de realizar transacciones, tanto los corresponsales como los clientes pueden perder la confianza en el producto si no pueden acceder a sus fondos, esto puede crear riesgos reputacionales y pérdidas financieras a medida que los clientes y corresponsales se vuelven inactivos y la presión competitiva les proporciona opciones alternativas.

Los fallos tecnológicos también dejan oportunidades para que los estafadores aprovechen las insuficiencias del sistema para realizar transacciones no autorizadas que resulten en robo de fondos. Riesgo tecnológico se refiere al fracaso tecnológico que conduce a la incapacidad de realizar transacciones, está estrechamente vinculado al riesgo operacional. las transacciones dentro de un Servicio Financiero Digital viajan a través de varios sistemas y dispositivos de

comunicaciones para iniciar la transacción, transferir fondos y enviar confirmaciones a los clientes. (Mastercard Foundation y el Programa de IFC, 2016).

2.1.1.9.4 Riesgo reputacional

Es el riesgo que se forma de una opinión pública negativa sobre el servicio bancario prestado, el riesgo reputacional puede derivar en acciones que fomenten la creación de una mala imagen o un posicionamiento negativo en la mente de los clientes de tal forma que se produzca una migración de fondos hacia otras entidades, debido a una pérdida de credibilidad, en este sentido una ruptura significativa en la seguridad ofrecida puede dinamitar la confianza pública en un banco.

El riesgo reputacional puede también surgir en aquellos casos donde los clientes experimentan problemas con un producto o servicio y no han sido adecuadamente informados sobre el mismo y los procedimientos de resolución del problema, los errores, la malversación y el fraude de terceras partes exponen igualmente a los bancos al riesgo reputacional (Dominguez, 2023).

2.1.1.9.5 Riesgo legal

El riesgo legal es donde surge de violaciones e incumplimientos con las leyes y reglas o cuando los derechos y obligaciones legales de las partes respecto a una transacción no están bien establecidos, se debe tomar bien en cuenta este tipo de riesgo dada la relativa a la nueva naturaleza de muchas de las actividades constantes que se realizan en la banca digital (Dominguez, 2023).

Todos estos riesgos, acontecen por la falta de controles dentro de las entidades bancarias, puede ser: fallas tecnológicas, administración deficiente, fallas humanas o faltas de conocimiento de los empleados respecto a la banca y sus medios digitales.

2.1.1.10 Canales electrónicos de pago

Son de manera enunciativa y no limitada, los dispositivos (cajeros automáticos – ATM, terminales de puntos de ventas. POS), redes de comunicación (internet, telefonía fija o móvil), pasarelas de pago o aplicativos que permitan procesar las órdenes de pago o aplicativos que

permitan procesar las órdenes de pago originadas con instrumentos de pago (Banco Central de Bolivia BCB, 2023).

2.1.1.11 Transacciones bancarias

Es un método de transferencia electrónica de fondos de una persona o entidad a otra. Una transferencia bancaria puede hacerse a partir de una cuenta bancaria a otra cuenta bancaria, o a través de una transferencia de dinero en efectivo en una oficina de caja. Diferentes sistemas y operadores de transferencias electrónicas proporcionan una variedad de opciones relativas a la inmediatez y la firmeza de la liquidación y el costo, el valor y volumen de las transacciones. Los tipos de transacciones bancarias incluyen retiros o depósitos de efectivo, cheques, pagos en línea, cargos de tarjetas de débito, transferencias bancarias y pagos de préstamos (Crime Academy, 2024).

2.1.1.12 Código QR

Matriz de puntos o códigos de barras bidimensional con estructura cuadrada que permite almacenar datos codificados para el procesamiento de transferencias electrónicas de pago (Banco Central de Bolivia BCB, 2023). A su vez, Juan Ranchal (2021) indica que un QR tiene el objetivo de almacenar información en una etiqueta óptica legible por algún tipo de máquina o dispositivo.

2.1.1.13 Fraude

El término fraude se refiere al acto intencional de la Administración por parte de uno o más individuos que pertenece a la empresa o por terceros y/o una combinación de intereses entre ambos, que da como resultado una prestación equivocada o una distorsión de los Estados Financieros esto implica la manipulación, falsificación o alteración de registros o documentos. La malversación (uso indebido) de activos, la supervisión u omisión de los efectos de ciertas transacciones en los registros o documentos. El registro de transacciones sin la debida sustentación, la aplicación indebida de las políticas de contabilidad (René, 2012).

2.1.1.14 Fraude con transferencias de dinero

El fraude con transferencias de dinero involucra el mal uso de los sistemas por parte de los defraudadores externos, para hacer transferencias fraudulentas de fondos, los fraudes

generalmente incluyen el mal uso de las claves y contraseñas y de los códigos de autorización o la falsificación de los documentos que autorizan la transferencia (René, 2012).

2.1.1.15 Protección de datos

Los datos personales son aquellos que permiten identificar a una persona o brindar información de carácter privado de la misma como su nombre, dirección, cédula de identidad, sus ingresos, su estado de salud, su orientación sexual, entre otros (Sagardía, 2021).

2.1.2 Marco contextual

2.1.2.1 Sistema Financiero en Bolivia

El sistema financiero nacional es el conjunto de entidades de intermediación financiera (EIF) cuyo objetivo social es la intermediación financiera y la presentación de servicios financieros complementarios, entre la oferta y demanda de recursos monetarios que están autorizadas, reguladas y supervisadas por la autoridad de Supervisión del Sistema Financiero ASFI.

Los objetivos del sistema financiero nacional son:

- ✓ Estimular la captación del ahorro privado
- ✓ Asegurar la utilización sistemática irracional de los recursos
- ✓ Orientar la colocación de los recursos en sectores productivas
- ✓ Promover el crecimiento de las entidades financieras

Las funciones del sistema financiero nacional

- ✓ Garantizar una eficaz asignación de recursos financieros
- ✓ Garantizar la estabilidad monetaria y financiera (BanComunidadBC Banco Pyme, 2023).

2.1.2.2 Características del Sistema Financiero de Bolivia

Comprende a todas las entidades que realizan actividades de intermediación financiera, a las entidades que ofrecen otros servicios financieros complementarios, a los consumidores financieros y como ente rector al Estado (Autoridad de Supervision del Sistema Financiero-ASFI, 2024)

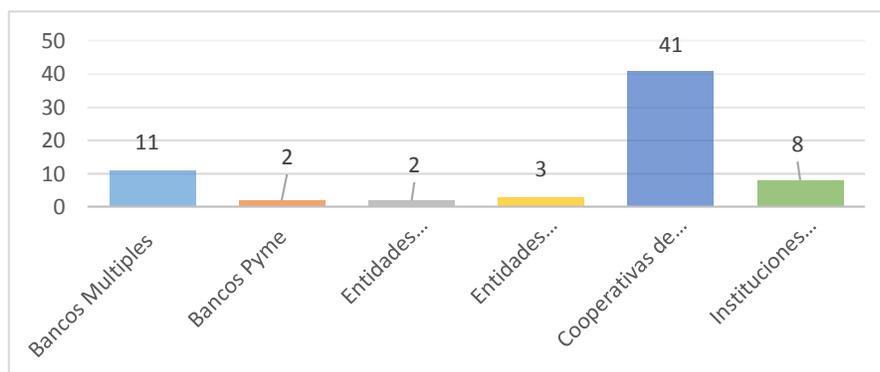
Tabla 1: Entidades de Intermediación Financiera

Entidades de Intermediación Financiera	Cantidad
Bancos múltiples	11
Bancos Pyme	2
Entidades financieras del estado	2
Entidades financieras de vivienda	3
Cooperativas de ahorro y crédito abiertas	41
Instituciones Financieras de Desarrollo	8

Fuente: Elaboración propia con datos de la ASFI, 2024

El sistema Financiero Boliviano está compuesto por: 11 Bancos múltiples, 2 Bancos Pyme, 2 Entidades financieras del estado, 3 Entidades financieras de vivienda y 41 Cooperativas de ahorro y crédito abiertas y 8 Instituciones Financieras de Desarrollo.

Gráfica 1:Entidades de Intermediación Financiera



Fuente: Elaboración propia con datos de la ASFI, 2024

Se puede observar que en Bolivia existen más cooperativas de ahorro y créditos abiertas, en comparación con las otras entidades de intermediación financiera.

2.1.2.3 Ley 393, Ley de Servicios Financieros

La Ley 393 de Servicios Financieros de Bolivia es una normativa de gran relevancia que busca regular y supervisar las actividades relacionadas con los servicios financieros en el país. Esta ley, promulgada el 21 de agosto de 2013, es el marco legal que rige el funcionamiento de las

entidades financieras y establece los derechos y obligaciones tanto de los proveedores como de los usuarios de servicios financieros en Bolivia.

La presente Ley tiene por objeto regular las actividades de intermediación financiera y la prestación de los servicios financieros, así como la organización y funcionamiento de las entidades financieras y prestadoras de servicios financieros; la protección del consumidor financiero; y la participación del Estado como rector del sistema financiero, velando por la universalidad de los servicios financieros y orientando su funcionamiento en apoyo de las políticas de desarrollo económico y social del país.

Se encuentran bajo el ámbito de aplicación de la presente Ley, las actividades financieras, la prestación de servicios financieros y las entidades financieras que realizan estas actividades.

Rector del sistema financiero, El Estado en ejercicio de sus competencias privativas sobre el sistema financiero, atribuidas por la Constitución Política del Estado, es el rector del sistema financiero que, a través de instancias del Órgano Ejecutivo del nivel central del Estado, definirá y ejecutará políticas financieras destinadas a orientar y promover el funcionamiento del sistema financiero en apoyo principalmente, a las actividades productivas del país y al crecimiento de la economía nacional con equidad social; fomentará el ahorro y su adecuada canalización hacia la inversión productiva; promoverá la inclusión financiera y preservará la estabilidad del sistema financiero.

Regulación y supervisión por parte del estado I. Es competencia privativa indelegable de la Autoridad de Supervisión del Sistema Financiero - ASFI ejecutar la regulación y supervisión financiera, con la finalidad de velar por el sano funcionamiento y desarrollo de las entidades financieras y preservar la estabilidad del sistema financiero, bajo los postulados de la política financiera, establecidos en la Constitución Política del Estado.

Según la autoridad de supervisión del sistema financiero – ASFI aplicara la supervisión basada en riesgos, para verificar la existencia y funcionamiento de sistemas formalizados de gestión integral de riesgos en las entidades financieras. Para dicho efecto de manera enunciativa no limitativa, deberá:

- a) Evaluar la efectividad de los sistemas de las entidades financieras para gestionar oportunamente los riesgos.

- b) Controlar la eficiencia y efectividad del control oportuno de riesgos inherentes a las actividades financieras que desarrollan las entidades. Artículo 35 (LEY N° 393, 2013).

2.1.2.4 Autoridad de Supervisión del Sistema Financiero – ASFI

La Autoridad de Supervisión del Sistema Financiero - ASFI es una institución de derecho público y de duración indefinida, con personalidad jurídica, patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica con jurisdicción, competencia y estructura de enlace nacional, responde al Ministerio de Economía y Finanzas Públicas y sujeta a control social.

El objetivo de la ASFI es regular, controlar y supervisar los servicios financieros en el marco de la Constitución Política del Estado, la Ley N.º 393 de Servicios Financieros y los Decretos Supremos reglamentarios, así como la actividad del mercado de valores, los intermediarios y entidades auxiliares.

Las actividades financieras y la presentación de servicios financieros deben ser realizadas únicamente por entidades que tengan autorización de ASFI, según los tipos de entidades definidos en la Ley N.º 393 (Estado Plurinacional de Bolivia , 2024).

2.1.2.5 Banca digital de Bolivia

Para Bolivia el crecimiento de la banca digital y sus operaciones electrónicas han ido en aumento conforme al paso de tiempo. Operaciones como pagos QR, transacciones mediante banca móvil, y uso de tarjetas electrónicas han beneficiado a la inclusión financiera, los bancos tienen un largo recorrido a cumplir frente a otros países que ya tiene la banca digital totalmente implementada.

En definitiva, el modelo financiero bancario se encuentra constantemente en proceso de evolución. La transformación de la banca tradicional a la banca digital beneficia a la inclusión financiera y conduce a un modelo fuerte, innovador y confiable, siendo cada vez más eficiente de cara a los consumidores financieros, la banca digital es una realidad que crece conforme al apoyo de los bancos y los clientes (Ticona, 2023).

A su vez, ASFI (2013) indicó, la banca móvil es una nueva innovación financiera conocida también como servicio financiero móvil, que ha sido definida de diferentes formas:

- ✓ La prestación de servicios financieros que no se realiza a través de sucursales bancarias convencionales, sino utilizando teléfonos móviles y agentes minoristas no bancarios.
- ✓ Todo tipo de servicio financiero que se realiza utilizando un dispositivo móvil
- ✓ La utilización de un dispositivo móvil como un canal para la realización de transacciones desde una o varias cuentas bancarias.

La banca móvil también se considera como parte de la banca sin sucursales y como un subgrupo perteneciente a la banca electrónica, la cual también incluye a la banca por internet y el uso de canales móviles como cajeros automáticos y dispositivos de punto de venta. Nuevos actores intervienen en la prestación de servicios financieros mediante la banca móvil, la Operadora de Servicios de Telefonía Móvil y la Empresa de Servicios de Pago Móvil (ESPM). Así mismo, en este servicio se ha identificado la existencia de riesgos que afectan su desarrollo e implementación, entre los cuales resalta el riesgo de liquidez, por lo que se deben establecer medidas para asegurar la liquidez de cada transacción financiera, y el riesgo operativo, relacionado con el uso de los dispositivos móviles.

La Autoridad de Supervisión del Sistema Financiero mediante resolución ASFI N.º 835/2011 de fecha 23 de diciembre del 2011 aprobó y puso en vigencia el reglamento para la Constitución, Funcionamiento, Disolución y Clausura de las Proveedoras de Servicio de Pago Móvil, con la expectativa de que este nuevo mecanismo de utilización del dinero electrónico impulse en gran medida la inclusión de la población especialmente de áreas rurales, a medios de pagos seguros, sin necesidad de movilizar dinero en efectivo de una población a otra.

2.1.2.6 Entidades financieras que operan en Bolivia con una banca digital

Es necesario saber que entidades financieras operan en Bolivia y cuantas de ellas cuenta con una banca digital, A continuación, se detallan:

Tabla 2 Entidades bancarias que operan en Bolivia

Bancos	Abreviatura	Plataforma de banca digital
Banco Unión S.A.	BUN	Uninet, Unimovil.
Banco Nacional de Bolivia S.A.	BNB	BNB Móvil.
Banco Mercantil Santa Cruz S.A.	BME	BMCS Móvil.
Banco Bisa S.A.	BIS	Banco BISA.
Banco de Crédito de Bolivia S.A.	BCR	BCP Bolivia-Banca Móvil, YAPE- Bolivia
Banco Económico S.A.	BEC	Banco Económico
Banco Ganadero S.A.	BGA	Banco Ganadero S.A., YOLO pago.
Banco Solidario S.A.	BSO	Altoke, Banco Sol.
Banco de la Nación Argentina S.A.	BNA	BNA+
Banco para el Fomento a Iniciativas Económicas S.A.	BIE	Banco Fie S.A.
Banco Fortaleza S.A.	BFO	Fortaleza Móvil
Banco Prodem S.A.	BPR	PRD Móvil.

Fuente: Elaboración con información de los sitios web de cada entidad bancaria.

Cabe señalar que, con la nueva Ley de los servicios financieros, los fondos financieros privados cambiaron su razón social y estructura, a fin de ajustarse a la normativa convirtiéndose en bancas múltiples y entidades bancarias PyMEs, aspecto que no solo ha organizado las actividades dentro del sistema financiero, al mismo tiempo también ha ido adquiriendo dinamismo.

Los bancos bolivianos, en los últimos años, han encarado un agresivo proceso de digitalización para brindar mejor atención a los clientes y también para una mayor inclusión tecnológica en otros segmentos no bancarizados. Una iniciativa que resalta dentro de este proceso es simple,

un novedoso sistema de pago digital interoperable, a través de código QR, entre los bancos, los comercios y los usuarios.

En este proceso, la banca, se ha caracterizado por su rápida integración de los avances tecnológicos internacionales que estaban disponibles como el chip en tarjetas de crédito y débito, los cajeros que reciben depósitos, billetera móvil. Sin embargo, hoy la banca se ha dado cuenta que no es suficiente añadir nuevas tecnologías si no avanzar en la transformación digital de sus procesos y plantear nuevos modelos de negocios que les permita seguir atendiendo a un cliente que cada día exige nuevas formas de atención e interacción digital (Innova Bolivia S.R.L., 2020).

2.1.2.7 Adopción del sistema QR

Los pagos inmediatos QR BCB Bolivia, son el QR oficial del Estado Plurinacional de Bolivia que es un esquema desarrollado por el banco central de Bolivia para facilitar las transferencias de fondos con la premisa de integrar a todo el sistema financiero utilizando un QR estandarizado y universal que esté disponible para todos los usuarios independientemente de la entidad financiera en la que tengan su cuenta y de esta manera democratizar el acceso de la población a las transacciones electrónicas (Banco Central de Bolivia, 2024).

Según el Banco Central de Bolivia los pagos a través de QR fueron introducidos en 2020. Desde entonces, su uso ha crecido rápidamente, y se estima que en 2023 se realizaron más de 10 millones de transacciones a través de QR en el país. Bolivia ocupa el primer lugar en el uso de códigos QR para pagos en línea en América Latina, según un estudio realizado por la consultora Euromonitor Internacional. El estudio, publicado en 2023, encontró que el 37% de los bolivianos utiliza códigos QR para realizar pagos en línea, un porcentaje que es significativamente superior al promedio de América Latina, que es del 19%. El pago QR fue legalizado en Bolivia en 2020, a través del Decreto Supremo No. 4158. Este decreto estableció el marco regulatorio para los pagos QR en Bolivia, y definió los requisitos que deben cumplir los operadores de este tipo de pagos (Gumucio Escobar, 2023).

2.2 Información y datos obtenidos

2.2.1 Transacciones realizadas en la banca digital de Bolivia

2.2.1.1 Transacciones de Órdenes Electrónicas de Transferencia de Fondos

Las Órdenes Electrónicas de Transferencia de Fondos (OETF) son instrumentos Electrónicos de pago que, mediante un sistema informático y redes de comunicación, permiten al titular de una cuenta realizar órdenes de pagos asociados a las cuentas relacionadas por el instrumento.

A través de las Órdenes Electrónicas de Transferencia de Fondos se podrán realizar las siguientes operaciones:

- ✓ **Transferencia Electrónica de Fondos:** es una operación electrónica mediante la cual el cliente o titular debita fondos de su cuenta para transferir a cuenta determinada.
- ✓ **Débitos autorizados:** son operaciones electrónicas mediante el cual, a requerimiento del cliente o titular, el emisor de IEP debita fondos de la cuenta del titular para abonarlos a una cuenta determinada, los débitos automáticos deben contar con automatización expresa del titular de la cuenta a ser debitada.
- ✓ **Otros servicios:** como ser: giros o remesas, pagos en caso de ser beneficiarios por la prestación de un servicio o por el cumplimiento de obligaciones (deudas, impuestos y otros), compraventa de bienes y de una moneda extranjera, entre otros.

Las órdenes electrónicas de transferencia de fondos (OETF) deben cumplir con las siguientes características:

- ✓ **Autenticidad:** Contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago y que este se encuentre debidamente autorizado.
- ✓ **Integridad:** Estar protegida contra alteraciones originadas por contingencias tecnológicas, acciones intencionales o accidentales durante su proceso, transporte y almacenamiento.
- ✓ **Confidencialidad:** Controlar los mecanismos de cifrado estándar que eviten la difusión o divulgación no autorizada de la información contenida de operación que pueda ser utilizada para materializar eventos de fraude.
- ✓ **No repudio:** Garantizar que ninguna de las partes implicadas en las transacciones pueda negar su participación en la misma.

- ✓ **Disponibilidad:** El emisor debe garantizar en el ámbito de su control, que el sistema de procedimientos de OETF esté disponible para los clientes según las condiciones publicitarias, informadas o pactadas contractualmente.

En los últimos años, las OETF se han posicionado como el Instrumento Electrónico de Pago más utilizado para todo tipo de transacciones financieras, comerciales y personales. En este sentido, durante la gestión 2023 se procesaron 264 millones de operaciones por un monto de bs685.363 millones. El impulso regulatorio del BCB que promovió la interconexión e interoperabilidad de la infraestructura, la obligatoriedad de la provisión de servicio de transferencias electrónicas en las EIF reguladas, la habilitación de canales electrónicos en todas las EIF, la implementación de un estándar abierto y común para el procesamiento de transferencias electrónicas con QR a través de la implementación del QR BCB Bolivia, son factores que han facilitado el acceso y uso masivo de este IEP que se consolidó como el más relevante.

Es así que entre el 2019 y 2023 el número de operaciones procesadas con OETF se incrementó en 728% (Banco Central de Bolivia, 2023).

2.2.1.2 Transacciones a partir de la tarjeta de débito

Una tarjeta de débito también es un método de pago, la cantidad que se puede utilizar depender del monto que tengas disponible, los fondos son el dinero que ingreses a la cuenta relacionada con la tarjeta. Funciona mediante un débito de una cuenta de activo del tarjetahabiente.

En una tarjeta de débito deberás desembolsar de contado el total del producto o servicio que estas comprando.

En el caso de estas tarjetas algunas comisiones pueden ser por retiro en un cajero diferente al que pertenece la tarjeta, apertura, por saldo mínimo o manejo de cuentas y por reposición de tarjetas. También posee un número único de cuenta.

Se puede usar para comprar bienes o servicios y para obtener dinero en efectivo.

Se puede realizar las transacciones con la tarjeta de débito de manera efectiva en la red de cajeros automáticos sin ningún costo las siguientes transacciones:

- ✓ Acceso a más de 300 cajeros automáticos de la red telebanco en forma gratuita.

- ✓ Retirar efectivo, consultar saldos y últimos momentos.
- ✓ Realizar depósitos en efectivo en cuentas propias o de terceros en bolivianos o dolores americanos, en los cajeros habilitados.
- ✓ Realizar pago de servicios, tarjetas de crédito y prestamos mediante transferencias.
- ✓ Transferir dinero a cuentas propias o de terceros del mismo banco.
- ✓ Las tarjetas de débito es la más efectiva del mercado.
- ✓ Realizar compras directamente en los establecimientos afiliados al sistema de compra en punto de venta (POS) en comercios locales.
- ✓ Realizar transacciones con tecnología contactless en cajeros automáticos locales con uso de PIN, hasta el límite establecido de la tarjeta de débito (RedEnlace, 2022).

El 2020 el uso de las tarjetas electrónicas se ha orientado de manera creciente a los pagos debito a la ampliación de los establecimientos y comercios que acepta pagos con este instrumento, la adopción de la tecnología contactless que significa su uso, la habilitación de tarjetas de débito para procesar pagos por internet y la integración de las redes de las tarjetas electrónicas a las pasarelas de pago para facilitar el comercio el electrónico.

En el 2023 los indicadores del uso y acceso de tarjeta electrónicas de débito tuvieron un comportamiento dispar, mientras que el valor y el volumen aumentaron una tendencia creciente, las cifras relacionadas con la infraestructura de pagos y a acceso fueron negativas. La disminución de la cantidad de tarjetas electrónicas de débito en circulación fue un 5%, se explica principalmente por la salida del sistema financiero de una EIF que contaba con una amplia cobertura a nivel nacional en cuanto a infraestructura de pagos (Banco Central de Bolivia, 2023).

2.2.1.3 Transacciones a partir de la tarjeta de crédito

Una tarjeta de crédito es un medio de pago que permite disponer de cierta cantidad de dinero, gracias a una línea de crédito que una entidad financiera te otorga.

La institución financiera emisora de tarjetas, factura posteriormente bajo el concepto del crédito otorgado, para ser pagado íntegramente o dividido en pagos mensuales.

Algunas de las comisiones son: por anualidad, por disposición en efectivo, pago tardío, reposición de plástico, gastos de cobranza, entre otras.

Posee un número único de cuenta y límite de crédito establecido.

Se puede usar para comprar bienes o servicios y para obtener desembolsos de efectivo de crédito (RedEnlace, 2022).

En el 2023 los indicadores del uso y acceso de tarjeta electrónicas de crédito tuvieron un comportamiento dispar, mientras que el valor y el volumen aumentaron una tendencia creciente, las cifras relacionadas con la infraestructura de pagos y a acceso fueron negativas. La disminución de la cantidad de tarjetas electrónicas de crédito en circulación fue un 8%.

La disminución de las ATM es un 3%. se explica principalmente por la salida del sistema financiero de una EIF que contaba con una amplia cobertura a nivel nacional en cuanto a infraestructura de pagos. En cuanto a la cantidad de POS se observó una ligera disminución de 2% lo que se debe al retiro de POS obsoletos que no cumplían con la normativa PCI, el recojo de equipos sin actividad y devolución de equipos, este último debido a un efecto sustitución por OETF y Billetera Móvil que han mostrado un incremento importante a lo largo de la gestión y cuyo uso se ha masificado para el procesamiento de pagos en comercios, principalmente con el uso del QR (Banco Central de Bolivia, 2023).

2.2.1.4 Transacciones a partir de la billetera móvil

La billetera móvil opera en un dispositivo móvil con una línea móvil de un operador de servicios de telefonía móvil y permite a los usuarios realizar transferencias electrónicas de fondos, recargas y/o retirar efectivo y solicitar información sobre el servicio de pago móvil. Las billeteras móviles solo pueden almacenar dinero electrónico.

En la actualidad, las operaciones que se realizan con billetera móvil son transferencias entre billeteras, transferencias a personas particulares (giros), transferencias a cuentas del sistema financiero, pagos inmediatos con QR, retiro de efectivo (efectivización), pago de servicios, pago con billetera móvil a pasarelas de pago de comercio electrónico y recarga de crédito a celular.

Actualmente operan en el mercado boliviano el servicio de billetera móvil

- ✓ **Tigo Money:** permite enviar y recibir dinero, pagar servicios y realizar compras en tiendas.

- ✓ **Billetera móvil del BCP (Soli):** ofrece la disponibilidad de realizar transacciones sin comisiones, administrar dinero en moneda nacional, y pagar servicios básicos.
- ✓ **Billetera Electrónica del BNB:** proporciona servicios similares, permitiendo a los usuarios gestionar sus finanzas de manera digital.
- ✓ **Billetera Móvil del Banco Ganadero (Yolo Pago):** facilita el envío y recepción de dinero, así como el pago de servicios y recargas de celular (Internet Bolivia.ORG, 2023).

La billetera móvil fue el IEP que tuvo el mayor crecimiento en cuanto a valor procesado respecto a la gestión anterior (173%) habiendo pasado de bolivianos 4.519 millones en 2022 a bs12.349 millones en 2023, el volumen procesado fue de 105 millones de operaciones lo que representa un incremento interanual del 69%.

Durante la gestión, la cantidad de billeteras móviles paso de 1.8 millones en 2022 a 2.7 millones, lo que representa un incremento de 51%, el más alto observado en los últimos 5 años.

En cuanto a los cheques, en línea con los nuevos patrones de consumo y la preferencia por los pagos electrónicos, se mantuvo la tendencia decreciente del uso de cheques en las últimas gestiones. En efecto, tanto el valor como el volumen procesado experimentaron una disminución de 10% y 8%, respectivamente, habiéndose realizado 2.6 millones de operaciones por un monto de bs128.127 millones, considerando que este instrumento se usa principalmente para procesar pagos comerciales de elevada cuantía, se observa un efecto de sustitución con las OETF, debido a que los usuarios han adoptado el uso de transferencias electrónicas (Banco Central de Bolivia, 2023).

2.2.1.5 Transferencias a partir de cobros y pagos por código QR

Los pagos inmediatos con QR consisten en la generación de un código de barras bidimensionales que contiene toda la información para el pago o cobro (nombre del beneficiario, número de cuenta, entidad financiera, etc.) que se lee o escanea a través de un dispositivo móvil y permite efectuar transferencias, pagos rápidos, simples y seguros (banco, cooperativa, entidad financiera de vivienda, institución financiera de desarrollo) puede pagar o cobrar utilizando este instrumento.

También se utiliza estos códigos QR para realizar transferencias o OETF en los bancos asociados a Asoban, cada banco ha actualizado esta aplicación con este sistema de manera distinta. Este método permite realizar transacciones de dinero tan solo escaneando un código QR. Si bien es un método bastante nuevo, lo que hace compleja la evaluación de su incidencia, se puede apreciar en la actualidad que vendedoras, artesanos y emprendedores ya hacen uso del mismo.

Pagos que se puede procesar mediante transferencias de dinero con QR BCB en Bolivia

- ✓ Transferencias entre personas / empresas.
- ✓ Pensiones de colegio.
- ✓ Pagos de seguros.
- ✓ Pagos en comercio.
- ✓ Pagos en mercado.
- ✓ Transferencias de ayuda social.
- ✓ Pagos de servicios básicos.
- ✓ Pagos de comercio electrónico.
- ✓ Pagos en pasarelas de pago.
- ✓ Pagos en páginas web (comercio electrónico).
- ✓ Pago de tramites.
- ✓ Compra de bonos del BCB (directo y navideño) (Banco Central de Bolivia , 2024).

Desde su lanzamiento el 2019 se procesaron más de 179 millones de operaciones por un monto de bs86.186 millones a través de este mecanismo, mostrando un incremento exponencial. La gestión 2023 fue el año de mayor expansión para los pagos inmediatos, se procesaron 135 millones de pagos con QR por un importe de bs63. 561 millones. Destaca también el uso que se le da a los pagos inmediatos con QR, puesto que el 53% de las operaciones procesadas corresponde a montos menores a bs100, y el 84% corresponde a operaciones por montos inferiores a bs520, lo que ubica a este tipo de pagos como el preferido para las operaciones cotidianas y de bajo valor (Banco Central de Bolivia, 2023).

Cuadro 1: Transacciones digitales en las entidades financieras

Transacciones que se realizan de forma general en la Banca Digital
<ul style="list-style-type: none">✓ Transacciones interbancarias ACH✓ Transacciones entre cuentas a terceros✓ Transferencias entre cuentas propias✓ Transferencias nacionales✓ Transferencias internacionales✓ Transferencias por pagos a instituciones Gubernamentales✓ Transferencias de pagos por servicios básicos✓ Giro relámpago✓ Transferencia por pago de préstamo✓ Transferencia por pago de tarjeta de crédito✓ Transferencia de tarjetas prepago✓ Transferencias de pagos de impuestos.

Fuente: Elaboración propia con datos obtenidos de las páginas web de cada entidad financiera con banca digital

Las transferencias que se realizan de forma general en la banca Digital, se han mencionado en el cuadro N°1, mismo se da a entender que existe un sin fin de variedades en el proceso de transferencias, que corresponde tanto a la banca electrónica, a la banca por internet y banca móvil, siendo estas accesibles a todo tipo de personas y/o empresas.

2.2.2 Riesgo operacional que emergen en las transacciones digitales

2.2.2.1 Fraude y ciberataques

El fraude es obtener servicios, bienes o dinero por medios no éticos y es problema creciente en todo el mundo actual, puesto que gran cantidad de servicios que ofrecen las entidades bancarias o comercios lo hacen por vía internet (Guijarro & Silva, 2017). El fraude se puede manifestar de diversas formas como:

- ✓ **Ampliación fraudulenta en el cupo de la tarjeta:** en las tarjetas de crédito una persona que posiblemente es trabajadora de la misma entidad aumenta el cupo para después hacer retiro en cajeros o compras, luego de perpetuar este fraude vuelve a modificar los cupos como estaban anteriormente.
- ✓ **Phishing:** este fraude se realiza enviando un correo electrónico con un mensaje muy convincente que invita a la persona a ingresar, mediante un enlace (link), a la supuesta página de su banco, donde pedirá que ingrese información personal con la cual puede cometer algún tipo de fraude (Banco de Crédito de Bolivia, 2024).
El denominativo Phishing que es considerado como uno de los nuevos mecanismos de estafas digitales que hacen que, por desconocimiento, pongamos en riesgo nuestras contraseñas, código de tarjetas u otro tipo de información personal que nos ponga en situación de riesgo. Las formas más comunes y habituales de Phishing que son utilizadas a través de mensajes SMS, correos electrónicos, redes sociales y otros canales digitales, para vulnerar la seguridad de la información personal que en muchos casos pueden derivar en estafas financieras (Banco FIE, 2022).
- ✓ **Fraudes con tarjetas:** existen distintas modalidades de fraude como, cambio de tarjetas en el cajero automático, estando en el cajero automático, el estafador te ofrece ayuda, y sin que te des cuenta cambia tu tarjeta por otra, tú intentarás nuevamente la operación y alguien en complicidad observara tu clave, con tu tarjeta y tus datos podrán retirar el dinero de tu cuenta, a esta modalidad se la conoce como cambiazo.
- ✓ **Clonación de tarjetas:** un estafador copia la información de la banda magnética de tu tarjeta de débito o crédito a un dispositivo, con ello se podrán realizar una serie de fraudes: en el caso de las tarjetas de crédito además de fabricar una idéntica a la tuya, podrán realizar compras utilizando la cuenta a tu nombre y falsificando tu firma. Para la tarjeta de débito, ellos necesitarán también saber tu clave secreta, por lo que observarán en un momento de distracción (Banco de Crédito de Bolivia, 2024).
- ✓ **Spyware:** los programas spyware son programas espías que, una vez instalados en la computadora, recolectan información vinculada al uso que se da a la misma (programas utilizados, sitios web visitados, nombre de cuenta de usuarios e información de cuentas bancarias), para posteriormente remitir la información a terceras personas, todo esto sin el conocimiento del usuario de la computadora. El objetivo de estos programas es recopilar la mayor cantidad de información posible sobre el usuario, para así acceder a sus cuentas bancarias y disponer de su dinero.

A continuación, la ATT la Autoridad de Regulación y Fiscalización de telecomunicaciones y transporte (2024), describe las tácticas más comunes de fraudes:

Fraudes de compra de productos no entregados: uno de los métodos utilizados por estos estafadores involucra la venta de productos inexistentes. Los delincuentes se hacen pasar por vendedores de mercadería, como en el caso de un ciudadano estafado al intentar comprar carteras de una supuesta importadora. Después de solicitar un pago inicial, posteriormente requieren más dinero bajo falsos pretextos, como costos de envío adicionales. Por ello, la ATT recomienda a los usuarios que verifiquen la autenticidad de los vendedores y eviten realizar pagos anticipados sin garantías.

Estafas telefónicas con engaño de mejora de servicio: algunos estafadores se aprovechan de la buena fe de los usuarios, haciéndose pasar por representantes de empresas de telecomunicaciones. Bajo el pretexto de mejorar el servicio, inducen a las personas a proporcionar códigos, lo que resulta en la sustracción fraudulenta de saldo. Es imprescindible que los usuarios no proporcionen información personal o código a desconocidos.

Fraude telefónico con premio falso: también se utilizan llamadas telefónicas para ofrecer premios falsos, como teléfonos celulares, con el fin de obtener información personal de las víctimas. Es vital que la población no comparta datos personales ni proporcione códigos a personas desconocidas, incluso si se hacen pasar por representantes de empresas reconocidas.

Durante los últimos diez días, mediante su plataforma recibió 160 casos de estafas en línea, de los cuales 100 fueron identificadas como procedentes y concluyeron en el bloqueo de los teléfonos de estos estafadores.

El director ejecutivo de la Autoridad de Supervisión del sistema financiero (ASFI), Reynaldo Yujra, aclaró este lunes que las denuncias por supuestos desfalcos a cuentas bancarias de clientes del Banco Unión se deben a Hackeos de dispositivos móviles de los usuarios y no a operaciones de la entidad financiera.

Según esa denuncia habría 14 casos de robo virtual en Banco Unión. Es falso, no se trata de casos que hubieran ocurrido por aspectos atribuibles al Banco Unión, además seguro que la ASFI no tiene atribuciones para iniciar una investigación ante esas denuncias y que en las

suspensiones que realizan no se han evidenciado acciones que dejen vulnerable la seguridad de los usuarios. Lo que compete a la ASFI es asegurar que los sistemas de información que tienen las entidades financieras estén adecuadamente estructurados y no generen alguna vulnerabilidad, que este tipo de sucesos, denominado riesgo operativo, se presentaron también en al menos 4 entidades financieras. El Banco Unión más 4 entidad financieras de Bolivia atraviesan este tipo de situaciones, existen personas y organizaciones dedicadas a realizar este tipo de trabajos irregulares de tratar de clonar celulares, de hackear cuentas que proviene de países internacionales.

Según esas denuncias, aproximadamente bs638.300 habrían sido extraídos de 14 cuentas del Banco Unión.

El ciberataque es toda aquella acción ilegal que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. Muchos de estos delitos, al no estar tipificados en la ley, se definen como abusos informáticos, donde se incluyen delitos como el fraude, el chantaje, la falsificación y la malversación de caudales públicos utilizando órdenes y redes como medio para realizarlos (Centeno, 2015).

- ✓ Los virus informáticos: los virus informáticos son esencialmente programas de carácter maliciosos, que pretenden infectar a otros archivos contenidos en el sistema.
- ✓ El envío masivo de correo no deseado o SPAM.
- ✓ La suplantación de remitentes de mensajes mediante Spoofing.

El último Reporte Global de Ciberseguridad de la unión Internacional de Telecomunicaciones (UIT), posicionó a Bolivia en el puesto 140 de un total de 194 países. Este informe evalúa las amenazas digitales que enfrentan los países y el nuestro tiene el peor desempeño en Sudamérica.

Entre los mayores riesgos identificados se encuentran el robo de datos y de identidad, la intrusión a sistemas e infraestructura estratégicas, y las acciones de acoso y discurso de odio en redes sociales. El informe insta a los gobiernos en tomar acciones.

Entre las debilidades de nuestro país, resaltadas por el informe encargado con la organización de naciones unidas (UNO), se encuentra la ausencia de un andamiaje institucional. Bolivia no tiene una estrategia nacional de ciberseguridad y una normativa específica sobre cibercrimen.

Tampoco cuenta con legislación sobre protección de datos y/o entidades con un mandato específico en esa materia (Internet Bolivia.Org, 2021).

2.2.2.2 Errores humanos

Son los riesgos operacionales resultantes de la inadecuada gestión del capital humano que ejecuta el proceso, falta de entrenamiento. Entre los ejemplos: negligencia, deficiencia de conocimientos, destreza y/o experiencia, desmotivación, violación de políticas, inapropiadas relaciones interpersonales, ambiente laboral desfavorable. Si un empleado tiene acceso a transacciones que no son de su competencia, puede alterar información sensible o tener a su disposición datos confidenciales de los clientes y de la entidad, lo que puede resultar en fraudes, robos, secuestros de la información y sabotajes (Shaw, 2017).

2.2.2.3 Fallas técnicas

Un aspecto que tenemos que tomar en cuenta para proteger las transacciones en línea es utilizar sitios web confiables y seguros, antes de realizar una transacción, estos sitios web deben ser legítimos y que estén protegidos, se recomienda verificar la autenticidad del sitio web buscando señales de confianza como un candado en la barra de direcciones o un certificado de seguridad. Además, es útil leer las contraseñas de otros usuarios y verificar la reputación del sitio web antes de proporcionar información personal o financiera. No se recomienda realizar transacciones en redes Wi-Fi públicas o no seguras, ya que pueden ser vulnerables a ataques de intermediarios.

Dado que la banca digital depende por completo de que la tecnología funcione a la perfección, cualquier problema, como corte de luz, ataques maliciosos o filtraciones, podrían suponer que los clientes perdieran el acceso a sus cuentas al menos de forma temporal este periodo corto sería aprovechado por los ciberdelincuentes para desviar la transacción que el cliente estaba procesando antes del corte de luz (Nominalia, 2023).

2.2.2.4 Riesgo en la seguridad de la información

El concepto de manipulación informática corresponde en la conducta de alterar, modificar u ocultar datos informáticos de manera que se realice operaciones de incorrecta o que no lleven a cabo con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera tener. De esta forma un sujeto puede introducir instrucciones

incorrectas en un programa de manera que no anote cargos a su cuenta corriente. La transacción no consentida esta referida a cambio de una partida económica de un lugar u otro, es decir, desplazamiento de dinero de la cuenta bancaria de la víctima a la cuenta del autor del delito (Ávalos, 2014).

Si una persona accede a sistemas de información que son sensibles para la entidad, o cuenta con acceso a usuarios o contraseñas que no son de su responsabilidad, puede aumentar el riesgo de pérdida de confidencialidad o exponer los datos a modificaciones no autorizadas.

2.2.2.5 Problemas de infraestructura

Se refiere a la interrupción del negocio por fallas en la tecnología de información que generan pérdidas derivadas de incidentes por fallas tecnológicas, problemas de telecomunicaciones y sistemas públicos. Los problemas de infraestructura afectan a la integridad física del cajero, llegando incluso a provocar daños importantes en las infraestructuras donde está ubicado, así como a las personas.

Utilización de la violencia o fuerza extrema para el acceso al efectivo de la caja fuerte:

- ✓ Intento violento de acceso, mediante el uso de herramientas estándar.
- ✓ Ataques orientados a reventar la caja fuerte mediante explosivo o gas.
- ✓ Levantamiento o arranque del cajero de su lugar de fijación.
- ✓ Dispositivo electrónico que serviría para neutralizar los sistemas de seguridad.

Este tipo de ataques afectan a la integridad física del cajero, llegando incluso a provocar daños importantes en la estructura donde está ubicado (Fujitsu Technology Solutions, 2017).

2.2.2.6 Riesgo regulatorio y de cumplimiento

El riesgo regulatorio se refiere a los riesgos asociados con el cumplimiento (o incumplimiento) de las directrices y normas reglamentarias, como la protección de datos, límites de cuentas y transacciones, cuentas fiduciarias y normas respecto al uso de corresponsales. El riesgo regulatorio también incluye normas más amplias relacionadas con el funcionamiento de una entidad. El incumplimiento puede ser en áreas que no están directamente relacionadas con servicios financieros digitales, pero pueden tener un impacto significativo en las operaciones

de negocio, incluyendo multa, sanciones e incluso la pérdida de la licencia (Mastercard Foundation y el Programa de IFC, 2016).

2.2.2.7 Riesgo de confianza y reputacional

El riesgo reputacional se refiere al riesgo de pérdidas por daños a la imagen de un proveedor, socio o parte interesada, llevando a una reducción en la confianza de los clientes y corresponsales. Pueden ocurrir pérdidas en la reducción de ingresos y el alto valor para los accionistas, así como en el aumento de los costos operativos o responsabilidad legal. El riesgo reputacional no es un riesgo directo, sino que es el resultado de otros problemas relacionados con el riesgo. Sin embargo, por su naturaleza, las consecuencias pueden ser graves y perdurables. Los riesgos que es más probable que puedan resultar en daños reputacionales son un fallo tecnológico que causa imposibilidad para realizar transacciones, falta de transparencia en las políticas y los precios, fraude, mala experiencia del cliente, falta de liquidez de los corresponsales y precios altos (Mastercard Foundation y el Programa de IFC, 2016).

2.3 Análisis y discusión

2.3.1 Gestión de riesgos operativos de acuerdo a la Ley N.º 393 Artículo 449 mediante ASFI

En la presente Ley de Servicios Financieros hace referencia a la Gestión Integral de Riesgos. De forma clara establece que: Las entidades financieras deberán implementar sistemas metodológicos y herramientas de gestión integral de riesgo, que contemplen objetivos, estrategias, estructura organizacional, políticas y procedimientos para la prudente administración de todos los riesgos inherentes a sus actividades y operaciones; en base a la normativa que emita para el efecto, la Autoridad de Supervisión del Sistema Financiero.

2.3.2 Directrices básicas para la gestión del riesgo operativo

La Autoridad de Supervisión del Sistema Financiero - ASFI en su circular de recopilación de normas para servicios financieros, en su artículo número 1 y 2 expone lo siguiente:

Artículo 1° - (Implementación de la gestión del riesgo operativo) La entidad supervisada es responsable de administrar su riesgo operativo, a cuyo efecto debe contar con procesos formales para su gestión que le permitan identificar, medir, monitorear, controlar, mitigar y divulgar las exposiciones de riesgo que está asumiendo.

El proceso de gestión del riesgo operativo, debe considerar la exposición de la entidad supervisada a los riesgos legal y tecnológico. En este último caso se deben considerar en lo que corresponda las disposiciones establecidas en el Reglamento para la Gestión de Seguridad de la Información contenido en la Recopilación de Normas para Servicios Financieros. La administración del riesgo operativo, implica que la entidad supervisada debe definir su apetito al riesgo, de acuerdo a su naturaleza, tamaño y complejidad de sus operaciones. El conjunto de políticas, procedimientos y acciones que constituyen un sistema para la gestión del riesgo operativo, deben ser revisados y actualizados permanentemente. Este sistema debe formar parte de la estrategia institucional de la entidad supervisada.

Artículo 2° - (Principios para la gestión del riesgo operativo) La entidad supervisada, en la implementación de la gestión del riesgo operativo, debe observar mínimamente los siguientes principios:

- a. Contar con una estrategia formal para la gestión del riesgo operativo, desarrollada a partir de la estrategia general de la entidad supervisada que responda a su modelo de negocios;
- b. Establecer una estructura organizativa con una clara segregación de funciones, acorde a la estrategia, tamaño y complejidad de las operaciones de la entidad supervisada, que facilite la gestión del riesgo operativo y evite posibles conflictos de interés;
- c. Desarrollar políticas, procedimientos y herramientas adecuadas a la estrategia, tamaño y complejidad de las operaciones de la entidad supervisada, que apoyen la gestión de riesgo operativo;
- d. Actualizar oportunamente el proceso de gestión del riesgo operativo en respuesta a los cambios en el entorno, modelo de negocios y/o al apetito al riesgo de la entidad supervisada;
- e. Promover una cultura de gestión del riesgo operativo al interior de la entidad supervisada;

- f. Implementar sistemas de información que permitan la divulgación del riesgo operativo al cual se encuentra expuesta la entidad supervisada, a las instancias que correspondan;
- g. Priorizar la implementación de acciones preventivas, antes que correctivas;
- h. Identificar y evaluar el riesgo operativo inherente a todos los productos, actividades, procesos y sistemas;
- i. Instaurar un proceso para el seguimiento regular de los perfiles de riesgo operativo y de su exposición a pérdidas;
- j. Implementar planes de contingencia y de continuidad del negocio a fin de garantizar su capacidad de operar en forma continua y minimizar las pérdidas en caso de interrupción del negocio (Gestión de Riesgo Operativo , 2013).

Las sanas prácticas financieras se constituyen en el elemento principal de las normas prudenciales emitidas hasta la fecha, las que han contribuido al crecimiento ordenado y sostenido de la actividad financiera en el Estado Plurinacional de Bolivia. Adicionalmente, las recomendaciones del Comité de Basilea para la Supervisión Bancaria, han contribuido en la modernización de la normativa vigente.

2.3.3 Actividades de control del riesgo operativo

La Autoridad de Supervisión del Sistema Financiero - ASFI, dispone: Artículo 5° - (Actividades de Control) Las Actividades de Control son las políticas y procedimientos aprobados por el directorio para asegurar que se llevan a cabo las respuestas a los riesgos a los cuales se encuentra expuesta la entidad supervisada. Las Actividades de Control, tales como aprobaciones, autorizaciones, conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones u otros, deben tener lugar a través de toda la organización, en todos los niveles y en todas las funciones. Las Actividades de Control apoyarán en las respuestas a los riesgos a los que se encuentra expuesta una entidad supervisada, con el propósito de lograr una atención oportuna. Asimismo, éstas deben ser parte integral de sus operaciones diarias y ser desarrolladas en el marco de una estructura de control que sea apropiada al tamaño, la naturaleza, complejidad de las operaciones y el nivel de riesgo definido como tolerable. Dichas actividades se establecerán en tres (3) niveles:

a. Revisiones del Directorio y Comité de Auditoría. Comprende el análisis de informes planteados por la Alta Gerencia o Auditoría Interna al Directorio y el Comité de Auditoría, según corresponda, que permita verificar los avances en el logro de los objetivos contenidos en el Plan Estratégico y las medidas propuestas para su cumplimiento.

b. Controles Gerenciales. Consiste en la revisión y seguimiento que efectúa la Alta Gerencia a los informes y actividades que realizan las instancias operativas. Estos informes deben ser precisos y medibles, permitiendo la toma de decisiones.

c. Control de Operaciones. Comprende la implementación de:

1) Controles físicos. Medidas de seguridad que restringen el acceso físico a lugares autorizados sólo para el personal de la entidad supervisada.

2) Controles de accesos lógicos. Medidas de seguridad que registren el acceso lógico a los activos y sistemas de información de la entidad supervisada. Las actividades incluyen entre otros, perfiles de seguridad, monitoreo de las actividades de los usuarios de Sistemas de Información, políticas de seguridad en el acceso, en el marco de lo dispuesto en el Reglamento para la Gestión de Seguridad de la Información, contenido en la Recopilación de Normas para el Mercado de Valores.

3) Controles cruzados. Actividades o funciones que deben ser verificadas por al menos dos (2) funcionarios responsables de la entidad supervisada, así como el doble control de activos y firmas dobles.

4) Conciliaciones. Conciliaciones periódicas de los movimientos de efectivo con los registros contables.

5) Segregación de funciones. Separación de responsabilidades de la diversidad de actividades que intervienen en la consecución de objetivos específicos, con el fin de reducir el riesgo de error o de acciones inapropiadas que conlleven la manipulación de datos y/o malversación de activos

La entidad supervisada debe segregar mínimamente las siguientes funciones:

- ✓ Atención al público y registro contable

- ✓ Registro y ejecución de operaciones, diferenciando adicionalmente las de cartera propia o de clientes y/o participantes (si corresponde).
- ✓ En el Departamento o Área de Sistemas, se debe mantener separadas las funciones de: Desarrollo, Pruebas y Producción, seguridad informática y Operaciones.
- ✓ Cual otra función donde surjan conflictos de intereses que no sean mitigados por tres mecanismos de control (Recopilación de Normas para Servicios Financieros, 2013).

2.3.4 Marco Legal de protección de datos en el sector financiero

En Bolivia, la protección de datos es una temática relegada que precisa ser atendida urgentemente frente al peligro que supone el empleo indiscriminado de datos personales en medios digitales.

La falta de una norma específica, ha incentivado la creación de regímenes especiales de diferentes sectores como ser el financiero, que se caracteriza por componerse principalmente de datos sensibles.

Las medidas para el tratamiento de los datos financieros, que se adoptan en las entidades financieras bolivianas deben cumplir con lo establecido en el reglamento de gestión de la seguridad de la información de la autoridad de supervisión del sistema financiero (ASFI), y la política de seguridad de la información de la entidad financiera. Para garantizar la efectiva protección de datos bancarios y el derecho a la intimidad las entidades financieras supervisadas en Bolivia deben cumplir con las obligaciones que establece la normativa del sector financiero, pero además otras disposiciones relacionadas directa o indirectamente con la protección de datos ante la ausencia especifican de una norma para el sector financiero.

2.3.4.1 Normativa general

- ✓ Ley general de telecomunicaciones y transporte No. 164 de 8 agosto de 2011
- ✓ Ley de servicios financieros No. 393 de 21 de agosto 2013
- ✓ Reglamento para el desarrollo de las tecnologías de la información y la comunicación de 13 de noviembre de 2013
- ✓ Reglamento para la gestión de la seguridad de la información de la autoridad de supervisión del sistema financiero (ASFI) de 18 de diciembre de 2017

- ✓ Instructivo de cumplimiento para entidades de intermediación financiera de la unidad de investigación financiera (UIF) de 22 de septiembre de 2024
- ✓ Resolución de directorios No. 079/2022 del Banco Central de Bolivia de 26 de septiembre 2022

Autoridades de supervisión en la materia

- ✓ Autoridad de supervisión del sistema financiero (ASFI)
- ✓ Autoridad de Regulación y Fiscalización de telecomunicaciones y transporte (ATT)
- ✓ Banco Central de Bolivia BCB

2.3.4.2 Gestión de datos personales y financieros

✓ Lineamientos jurídicos para el procesamiento de datos

La ley de servicios financieros establece que las instituciones financieras deben mantener la reserva y la confidencialidad de la información de sus clientes en todo el momento. La transferencia de datos podrá ser realizada únicamente cuando el usuario financiero haya dado su consentimiento y bajo las excepciones legales establecidas.

En relación a las medidas de seguridad que deben ser tomadas, el reglamento de desarrollo de las tecnologías de la información y la comunicación establece que el responsable del tratamiento de los datos personales debe adoptar las medidas de índole técnica y organización necesarias, de acuerdo con el estado de la tecnología, para garantizar la seguridad de los datos personales y evitar su alteración, pérdida o tratamiento no autorizado.

✓ Políticas y aviso de alteración

No existe legislación al respecto, sin embargo, el reglamento de tecnologías de la información y comunicación establece que el tratamiento técnico de los datos personales en el sector público y privado en todas sus modalidades, incluyéndose entre estas actividades de recolección, conservación, tratamiento, cancelación, cesiones, consultas e interconexiones, requerirá el conocimiento previo expreso del interesado.

✓ **Notificación en caso de vulneración a la privacidad de los datos**

No hay obligación de notificar las vulneraciones a la privacidad de los datos, sin embargo, las entidades que tratan datos personales deben optar las medidas correctoras adecuadas tras una violación de la seguridad y a solicitud del interesado deberán otorgar información sobre dicha vulneración (Internet Bolivia.ORG, 2022).

2.3.5 Impacto de la tecnología y su inclusión en la banca

La evolución de las transacciones electrónicas a través de cajeros automáticos y otras tecnologías de la información y comunicación TICs hasta nuestros contextos actuales, se pone en evidencia que estos instrumentos electrónicos de pago IEP, fueron afectados, significativamente con la llegada del internet, las computadoras, los teléfonos móviles y de más dispositivos. Caracterizando todas las EIF del sistema financiero boliviano que cuentan con servicios de banca digital y que a través de sus distintas sucursales cubren el territorio nacional.

Se caracterizo diversas transacciones que actualmente se realizan por medio de los IEP se evidencia que la billetera móvil a través del código QR, es la más preferida del cliente boliviano. El informe de vigilancia del sistema de pagos 2023 del BCB da cuenta de forma general del desarrollo y evolución de OETF siendo este el instrumento más usado para todo tipo de transacciones financieras. Los principales hallazgos de este informe, las transferencias mediante tarjeta de crédito y débito en el último año, en cuanto valor y volumen de operaciones procesadas mantuvieron una tendencia creciente, la disminución de cantidad de tarjetas en circulación fueron negativas, así también los POS terminales de punto de venta que se retiro del servicio por quedar obsoletos y rezagados. En línea con los nuevos patrones de consumo y la preferencia por los pagos electrónicos se evidencio la decreciente tendencia del uso de cheques en la última gestión.

Es notorio el impacto por la tecnología que los efectos de la inclusión tecnología a los servicios de la banca tradicional ha cambiado y transformado los servicios financieros actuales dando comodidad y muchos beneficios a los clientes digitales, sin embargo, este avance también trajo consigo riesgos operativos.

Se identificó los riesgos operativos que emergen de las transacciones digitales, los fraudes y las estafas más comunes que son ejecutadas por ciberataques, gracias al robo de datos personales, clonación de tarjetas, para ellos existen varios tipos, formas, denominativos y procedimientos, para sustraer dinero de cuentas digitales, el medio por el que se ejecuta esta sustracción son las transacciones que tiene una relación directa sobre la problemática actuales que enfrenta la banca digital de Bolivia

La ATT en una de sus últimas notas de prensa informa 4 formas más comunes de robo que los delincuentes han creado como tácticas fraudulentas que tiene el único propósito de engañar a personas. La ATT prensa a través de su plataforma bloquea estafa recibe cada determinado tiempo denuncias de estafas en línea, una de ellas de 160 casos de denuncias de las cuales 100 fueran identificados como procedentes y concluyeron con el bloqueo de las líneas telefónicas de estafadores.

Estos registros que son publicados por la ATT a través de notas de prensa son los únicos registros de denuncia que existen en nuestro país, por parte de entidades regulatorias los servicios de las empresas de telecomunicaciones tienen relación directa con la actividad de la banca digital.

Dentro de los pocos pronunciamientos de parte de la Autoridad de Supervisión del Sistema Financiero- ASFI, según el director ejecutivo Reynaldo Yujra, la ASFI no tiene atribuciones para iniciar una investigación ante esas denuncias. La competencia de la ASFI es asegurar que los sistemas de información que tiene las entidades financieras estén adecuadamente estructurados y no generen alguna vulnerabilidad.

Asimismo, la fundación internet Bolivia rescata informes internacionales como el último reporte global de ciberseguridad de la unión internacional de telecomunicaciones UIT, donde se evalúa las amenazas digitales ubicando a nuestro país como uno de los que tiene el peor desempeño en Suramérica. En el informe de la ONU se indecencia que entre una de las debilidades que tiene nuestro país se encuentra la falta de un andamiaje institucional, no cuenta con una estrategia de ciberseguridad tampoco una normativa específica sobre cibercrimen, tampoco con legislación sobre protección de datos y/o entidades con mandato específico.

Se rescata estos informes por lo importante y la veracidad de los datos de instituciones reconocida en el medio internacional. Se evidencia que diferentes actores nacionales coinciden la falta de normativas como las que se mencionó, pero estas aseveraciones solo se conocen por medios de prensa a través de entrevistas tanto físicos como digital.

En general diremos que la ausencia de estas normas da paso a situaciones que provocan incidentes de pérdidas que afectan a los clientes provocando desconfianza por el servicio y a las entidades financieras afectando a su reputación y su integridad.

CAPÍTULO III

CONCLUSIONES

En cuanto al estudio realizado se logró establecer la base teórica que permitió conocer, información de investigaciones pasadas con respecto al tema de investigación, Bolivia en línea general se encuentra en una etapa acelerada de inclusión de los servicios digitales al sistema financiero boliviano. En los últimos años los bancos han invertido cifras importantes en incluir tecnología de punta, para introducir e innovar diversos servicios y productos en el mercado boliviano.

Se caracterizo las diferentes transacciones que opera la banca digital de Bolivia. Las más importantes que se identificaron en este estudio son, transacciones de tarjetas de crédito, transacciones de tarjetas de débito, transacciones de billetera móvil, y transacciones por código QR. Siendo esta última que desde el 2020 a tenido un incremento alto y significativo ubicándose como número uno en adopción por los clientes. Llegando a mercados importantes como también a mercados informales. Además, se menciona a todas las entidades financieras que operan con banca digital y la variedad de servicios que ofrecen a través de diferentes aplicaciones y plataformas todas diseñadas para facilitar las transacciones digitales.

Sin embargo, los riesgos operacionales que emergen en las transacciones digitales son, en su mayoría, el resultado de diferentes políticas en una gestión de riesgos operacional, cuando estas políticas fallan se convierte en eventos de fraudes y estafas. Estos riesgos son una de las principales amenazas que provocan pérdidas significativas ya que están directamente relacionados con diversos factores externos que, a su vez, establecen conexiones entre el fraude y las transacciones digitales. Identificando varias formas de fraude, como el fraude con tarjetas, la clonación, el robo de identidad entre las más destacadas, estos delitos permiten a los ciberdelincuentes a acceder al sistema de datos de las entidades financieras y cuentas bancarias de los usuarios, cuyo propósito es extraer dinero, utilizando como herramienta las transacciones digitales.

En ese sentido, se concluye que las entidades financieras deben profundizar el tema de socializar los servicios digitales enfocándose al conocimiento y el uso de las plataformas y aplicaciones que se utiliza para proceder al servicio de transacciones, asimismo, los bancos

deben implementar procedimientos rigurosos para la gestión de riesgos operacional, asegurando así un entorno más seguro y confiable para todas las partes involucradas.

BIBLIOGRAFÍA

- Alejandro, C. S. (2023). *La Banca Electronica y su Incidencia en el crecimiento Economico de Bolivia 2013-2021*.
<https://repositorio.umsa.bo/bitstream/handle/123456789/34183/T-2827.pdf?sequence=1&isAllowed=y>
- Arias, F. G. (2006). El Proyecto de Investigación. Episteme. <https://abacoenred.org/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf-1.pdf>
- Autoridad de Supervisión del Sistema Financiero - ASFI. (2013). *Gestión de Riesgo Operativo* . <https://servdmzw.asfi.gob.bo/circular/Textos/L03T05.pdf>
- Autoridad de Supervision del Sistema Financiero - ASFI. (2013). *La banca móvil como Intrumento de Inclusion Financiera* .
https://www.asfi.gob.bo/images/INT_FINANCIERA/DOCS/Publicaciones/Editoriales/2013/Editorial_042013.pdf
- Autoridad de Supervision del Sistema Financiero- ASFI. (2024). *Entidades de Intermediación Financiera con Licencia de Funcionamiento* .
https://www.asfi.gob.bo/images/INT_FINANCIERA/DOCS/Siglas EIF.pdf
- Ávalos, G. E. (2014). Necesidad de aplicar la penalización de los delitos informaticos en Bolivia Referente a estafas electronicas .
<https://repositorio.umsa.bo/bitstream/handle/123456789/23390/TD-4663.pdf?sequence=1&isAllowed=y>
- Banco Central de Bolivia . (2024). *¿Que son los pagos inmediatos QR BCB Bolivia?*
https://www.bcb.gob.bo/?q=pagos_qr_bcb_bolivia
- Banco Central de Bolivia. (2023). *Informe de Vigilancia del Sistema de Pagos*.
<https://www.bcb.gob.bo/webdocs/publicacionesbcb/2024/03/07/SISTEMA%20DE%20PAGOS%202023vf.pdf>
- Banco Central de Bolivia. (2024). *¿Qué son los pagos inmediatos QR BCB Bolivia?*
https://www.bcb.gob.bo/?q=pagos_qr_bcb_bolivia#:~:text=Los%20pagos%20inmediatos%20QR%20BCB%20Bolivia%2C%20son%20el%20QR%20oficial,y%20universal%20que%20est%C3%A9%20disponible

- Banco Central de Bolivia BCB. (2023). Requerimientos Operativos Minimos de seguridad para Instrumentos y canales electronicos.
https://www.bcb.gob.bo/webdocs/sistema_pagos/ROMS%202024.pdf
- Banco de Crédito de Bolivia. (2024). *Fraudes con Tarjetas*.
<https://www.bcp.com.bo/Seguridad/FraudesTarjetas>
- Banco de Crédito de Bolivia. (2024). *Fraudes por Internet*.
<https://www.bcp.com.bo/Seguridad/FraudesInternet>
- Banco FIE. (12 de julio de 2022). *Banco FIE lanza campaña de prevención del “phishing” una de las formas de estafa digital*. <https://www.bancofie.com.bo/novedades/noticias/99>
- BanComunidadBC Banco Pyme. (2023). *Educacion Financiera para la Comunidad* .
<https://bco.com.bo/wp-content/uploads/2023/02/Educacion-Financiera.pdf>
- Centeno, F. J. (2015). *Ciberataques, la mayor amenaza en la actualidad*.
<https://dialnet.unirioja.es/servlet/articulo?codigo=7684551>
- Cooperativa San Antonio SL. (2018). *El Sistema Financiero Nacional* .
<https://www.cacsa.com.bo/sites/default/files/2018-07/TEMA%203%20Sistema%20Financiero,%20rol%20de%20ASFI-%20ASFI%20y%20el%20car%C3%A1cter%20de%20la%20normativa..pdf>
- Crime Academy. (8 de mayo de 2024). Transaccion. *Copeyright Financial Crime Academy LLC*. <https://financialcrimeacademy.org/es/que-es-una-transaccion/>
- Dominguez, J. M. (2023). Ataques ciberneticos.
<https://core.ac.uk/download/pdf/196609423.pdf>
- Estado Plurinacional de Bolivia . (2024). Autoridad de Supervision del Sistema Financiero - ASFI . <https://www.asfi.gob.bo/index.php/asfi/acerca-de-nosotros/que-es-asfi.html>
- Flores, F. A. (2019). *Revista Digital de Investigación en Docencia Universitaria*.
http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2223-25162019000100008#:~:text=Por%20enfoque%20cualitativo%20se%20entiende,Mej%C3%ADa%2C%20como%20se%20cit%C3%B3%20en
- Fujitsu Technology Solutions. (2017). *Seguridad en los cajeros automáticos*.
https://www.fujitsu.com/es/Images/WP_Seguridad_en-red-ATMs_final.pdf
- Gobat, J. (2012). *¿Que es un banco?*
<https://www.imf.org/external/pubs/ft/fandd/spa/2012/03/pdf/basics.pdf>
- Guijarro, E. G., & Silva, L. C. (2017). *Los riesgos de las transacciones bancarias por Internet*.
https://revistapublicando.org/revista/index.php/crv/article/view/436/pdf_261

- Gumucio Escobar, A. A. (27 de octubre de 2023). *Estrategias, Metodologías & Didácticas*.
file:///C:/Users/CentroVirtual/Downloads/La_incorporacion_del_sistema_de_pago_QR_un_analisi%20(2).pdf
- Hérendez, A. V., & Holguín, J. A. (2020). *El Método Histórico Crítico en el estudio de movimientos sociales: La ideología cubana en el panorama social mexicano*.
file:///C:/Users/CentroVirtual/Downloads/7650701.pdf
- Hurtado. (2006). *Marco Metodológico*.
file:///C:/Users/CentroVirtual/Downloads/cap03%20(1).pdf
- Innova Bolivia S.R.L. (2020). *Banca Digital e Innovación en Bolivia*.
file:///C:/Users/CentroVirtual/Downloads/Banca%20digital.pdf
- Internet Bolivia.Org. (19 de junio de 2021). *Bolivia esta en una posición de alta vulnerabilidad digital*. <https://internetbolivia.org/actividades/publicaciones/bolivia-esta-en-una-posicion-de-alta-vulnerabilidad-digital/>
- Internet Bolivia.ORG. (18 de octubre de 2022). *¿Cual es el marco legal de la proteccion de datos m el serctor financiero?* <https://internetbolivia.org/noticias/cual-es-el-marco-legal-de-proteccion-de-datos-en-el-sector-financiero/>
- Internet Bolivia.ORG. (2023). *E-COMMERCE Y LA REGULACION DE PAGOSDIGITRALES EN BOLIVIA*. <https://library.fes.de/pdf-files/bueros/bolivien/20356.pdf>
- La Autoridad de Regulacion y Fiscalizacion de Telecomunicaciones y Transporte- ATT. (14 de mayo de 2024). *Conoce las estrategias más comunes que utilizan los estafadores en el país*. <https://www.att.gob.bo/conoce-las-estrategias-mas-comunes-que-utilizan-los-estafadores-en-el-pais>
- LEY Nº 393. (2013). LEY DE SERVICIOS FINANCIEROS.
<https://servdmzw.asfi.gob.bo/circular/Leyes/Ley393ServiciosFinancieros.pdf>
- Mastercard Foundation y el Programa de IFC. (2016). *Servicios Financieros Digitales y Gestión de Riesgo*. file:///C:/Users/CentroVirtual/Downloads/Digital-financial-services-and-risk-management-handbook%20(1).pdf
- Morales, F. C. (31 de mayo de 2023). Banca Electrónica.
<https://www.rankia.com/diccionario/banca/banca-electronica>
- Nominalia. (24 de mayo de 2023). *Seguridad en las transacciones online: Riesgos asociados con las compras, banca en línea y pagos electrónicos*.
<https://www.escueladeinternet.com/seguridad-en-las-transacciones-online-riesgos-asociados-con-las-compras-banca-en-linea-y-pagos-electronicos/>

- Palacios, M. M. (2024). *Análisis de la gestión de riesgos operativos en los estados financieros de las instituciones financieras*.
<https://rperspectivasinvestigativas.org/index.php/multidisciplinaria/article/view/119/513>
- Rafael, S. (septiembre de 2021). *Gestión de Riesgo Operativo y digital en el mundo financiero*.
<http://www.abav.com.bo/wp-content/uploads/2022/03/Gesti%C3%B3n-de-riesgos-operativos-y-digitales-en-el-mundo-financiero-y-sus-procesos-de-identificaci%C3%B3n-valoraci%C3%B3n-registro-y-reporte.pdf>
- Ranchal, J. (7 de junio de 2021). Códigos QR: ¿Qué son, para qué se usan y cómo trabajan?
<https://www.muycomputer.com/2021/06/07/codigos-qr/>
- Recopilación de Normas para Servicios Financieros. (2013). *Gestión de Riesgo Operativo*.
<https://servdmzw.asfi.gob.bo/circular/Textos/L03T05.pdf>
- RedEnlace. (15 de diciembre de 2022). *Conoce los beneficios de contar con una tarjeta de Crédito y como funciona* . <https://www.redenlace.com.bo/secciones-de-interes/blog/conoce-los-beneficios-de-contar-con-una-tarjeta-de-credito-y-como-funciona>
- René, G. C. (2012). *Propuesta de una Guia como Herramienta de control interno para la unidad de Aditoria Interna em la Deteccion de Fraude para las Empresas Industriales*.
<https://repositorio.umsa.bo/xmlui/bitstream/handle/123456789/3208/PG-374.pdf?sequence=1&isAllowed=y>
- Ruiz, R. (2007). *El Método Científico y sus Etapas*. México . <https://www.index-f.com/lascasas/documentos/lc0256.pdf>
- Sagardía, D. N. (2021). *Guia de soluciones legislativas para la Proteccion de datos personales* . https://internetbolivia.org/file/2021/11/guia_soluciones_legislativas.pdf
- Salas, R. (2021). *Riesgo Operacional*. <http://www.abav.com.bo/wp-content/uploads/2022/03/Gesti%C3%B3n-de-riesgos-operativos-y-digitales-en-el-mundo-financiero-y-sus-procesos-de-identificaci%C3%B3n-valoraci%C3%B3n-registro-y-reporte.pdf>
- Shaw, I. A. (septiembre de 2017). *Guia Metodologica de Gestion de Riesgo Operacional Para Instituciones Financieras de Desarrollo De Bolivia*.
<http://repositorio.uasb.edu.bo:8080/bitstream/54000/517/2/TE-239.pdf>
- Suárez, E. (29 de julio de 2024). *Método inductivo y deductivo*.
https://expertouniversitario.es/blog/metodo-inductivo-y-deductivo/#toc_Metodo_inductivo

- Superintendencia de Bancos y Entidades Financieras de Bolivia, con el. (2008). *Guías para la Gestión de Riesgos*. Intendencia de Estudios y Normas.
<https://www.asfi.gob.bo/images/ASFI/DOCS/LIBROS/GuiasRiesgos.pdf>
- Teyes, D. M. (2019). *Metodo Sintetico de Investigacion*. SCRIBIT.
<https://es.scribd.com/document/410794711/metodo-sintetico>
- Ticona Canahui, Z. S. (2015). Incidencia del riesgo de mercado en los resultados y patrimonio de las entidades del sistema bancario boliviano.
<http://repositorio.uasb.edu.bo:8080/bitstream/54000/264/1/TE-112.pdf>
- Ticona, M. (2023). *La banca digital y su inclusión financiera: Una revisión bibliográfica*.
<https://investigacionfacefa.unitepc.edu.bo/wp-content/uploads/2023/12/2.-Banca-Digital-y-su-Inclusion-Financiera.pdf>
- Universidad Europea. (2023). *¿Qué es la banca digital?*
<https://universidadeuropea.com/blog/que-es-banca-digital/>

ANEXOS

Anexo 1

En relación con otros países, ¿cómo avanza en Bolivia la digitalización de los servicios financieros?

Se registró importantes avances desde hace varios años, en concordancia con lo observado en economías de la región, algunas de las cuales se encuentran en fases más adelantadas en virtud al propio desarrollo económico y también de las condiciones internas y regulatorias que han propiciado su aceleración.

No obstante, el avance en materia de digitalización de los servicios financieros en el país se evidencia a través de los distintos servicios con los que los usuarios financieros cuentan actualmente como: transferencias intra e interbancarias, esto es pagos entre personas naturales y jurídicas; pago de servicios básicos, pago de préstamos, pago de servicios educativos, de impuestos, a proveedores, pagos de planillas de sueldos, entre otros. Todos estos servicios son accesibles de realizar a través de la banca móvil, como la banca por internet (a través de computadores).

Por otra parte, desde 2019 la población cuenta con un nuevo servicio de cobro y pago, denominado simple pago móvil, que permite realizar transacciones a través del empleo de códigos QR. Actualmente, un importante número de comercios, supermercados, tiendas de barrio, corporaciones empresariales, farmacias, radiotaxis, empresas unipersonales, restaurantes, marketplace, entre otros, hacen uso de \$imple pago móvil. Cabe señalar que recientemente, en ocasión del Congreso Latinoamericano de Automatización Bancaria, organizado por la Federación Latinoamericana de Bancos, celebrado el pasado 14 de septiembre de 2021, el servicio obtuvo el primer premio latinoamericano a la innovación e inclusión financiera.

Esta iniciativa ha sido premiada a nivel internacional al ser la primera plataforma de pagos interoperables entre entidades financieras; es decir, sin importar cuál sea la entidad donde el usuario financiero mantenga su cuenta corriente, caja de ahorros o billetera móvil. Si cuenta con un teléfono inteligente y la app de su banco en su teléfono, el usuario tiene acceso a un medio de cobro y pago fácil, seguro, que le permite realizar transacciones, ya sea de forma presencial, a distancia de manera práctica y segura. En otros servicios se aplica la innovación

y digitalización; por ejemplo, en la apertura de cuentas de depósito en línea, pago de créditos y tarjetas de crédito, consulta de saldos, obtención de extractos de cuentas y otros, servicios que también cuentan con plataformas digitales que permiten a los clientes interactuar con sus bancos, en un marco de seguridad y aplicación de la firma electrónica.

Lo señalado muestra que el país registra avances en materia de digitalización de los servicios financieros, los que en gran parte fueron desarrollados en la última década, permitiendo que los usuarios financieros continúen realizando transacciones digitales en los periodos más complejos de la pandemia. De hecho, la pandemia se constituyó en un acelerador del uso de los servicios financieros digitales, impulsando a la población a atreverse a emplear las aplicaciones de las entidades financieras para realizar sus transacciones en lugar de apersonarse físicamente a los bancos.

¿Qué cantidad de dinero se movió en este último año a través de las plataformas digitales?

A agosto de 2021 el monto registrado en transferencias interbancarias, interbancarias y pago de servicios ascendió a 45.866 millones de dólares, registrando un crecimiento de 33% en relación con similar periodo de 2020. En términos de cantidad de transacciones, ascendieron a 57,8 millones, con un dinamismo de 88%.

A su vez, cabe indicar que a agosto de 2021 las transacciones mediante simple pago móvil han experimentado un crecimiento exponencial, superior a 1.300%, comparando con similar periodo de 2020. En efecto, las transacciones de simple pago móvil alcanzaron a agosto a 2,3 millones, por un valor equivalente a 174 millones de dólares. Desde su lanzamiento, en mayo de 2019, las transacciones totalizan aproximadamente 2,8 millones, por un monto de 211 millones de dólares.

¿Cómo está el comportamiento del cliente boliviano ante la digitalización de los servicios financieros?

A raíz de la pandemia los usuarios se vieron en la necesidad de comenzar a usar los servicios financieros digitales. Se debe puntualizar que antes de la pandemia las transacciones digitales registraban importantes cifras; sin embargo, algunos grupos etarios, principalmente el de las personas mayores eran los más reticentes a adoptar estos servicios, habiéndose observado

ciertos cambios. Desde Asoban se continúan realizando actividades para promover la educación financiera de la población, principalmente a través de la plataforma Descubre lo Simple de las Finanzas; no obstante, también se analizan alternativas de medios educativos que permitan alcanzar a los distintos grupos etarios e impulsar su educación financiera.

¿Quiénes desarrollan estas plataformas digitales o soluciones tecnológicas?

Los desarrollos de las aplicaciones de las entidades financieras son realizados de acuerdo con las políticas de cada una de ellas, pudiendo ser a través de desarrollos internos o externos en función a sus requerimientos. Los procesos de validación de las aplicaciones son realizados internamente, cumpliendo con estándares regulatorios que garantizan su funcionalidad.

¿Cuánto invirtieron las entidades financieras en la banca digital?

Hace algunos años, un estudio mostró que, en la región, Bolivia era uno de los países que más invertía en digitalización en el sector bancario, lo que muestra que los bancos realizaron importantes inversiones para otorgar a los usuarios financieros servicios acordes a los implementados en la región y en el mundo.

¿Qué factores interfieren en el avance de la banca digital?

El hecho de que la innovación no pueda adelantarse a la regulación se constituye en uno de los principales factores limitantes para acelerar su crecimiento. Si bien debe existir regulación, podría analizarse la posibilidad de generar espacios de prueba para los servicios nuevos, derivando posteriormente en un mayor acompañamiento entre la regulación y la innovación.

La promoción de la innovación requiere incentivos que garanticen sus avances. Si bien la búsqueda de interoperabilidad del ecosistema es un objetivo común, el hecho de no contar con medidas que premien la innovación se constituye en un desincentivo, pues la innovación requiere tiempo e inversión, que en muchos casos deben ser recuperados. Para ello es preciso que se analicen incentivos que promuevan al acceso de todos sin afectar a la innovación.

¿Cuánto aporta la digitalización de los servicios financieros en la inclusión financiera?

Su aporte se observa parcialmente a través de las cantidades y montos de transacciones que se realizan a través de los medios digitales. Este aporte requiere ser complementado a través

de mejoras en el acceso a los servicios financieros digitales; por ejemplo, con mayor acceso a internet por parte de la población, permitiendo que las transacciones financieras digitales no requieran del consumo de megas de la población, entre otras medidas (Villalobos, 2021).

Fuentes generadoras de ingreso del riesgo operacional y tipos de eventos

Las principales fuentes generadoras de riesgo operacional:

- ✓ Recursos humanos
- ✓ Procesos
- ✓ Sistemas tecnológicos
- ✓ Eventos externos

Tipos de eventos por riesgo operacional

- ✓ **Prácticas de empleo y seguridad en el lugar del trabajo:** Son pérdidas que surgen de actos incompatibles con las leyes o acuerdos de empleo, salud o seguridad; del pago de reclamaciones por lesiones personales; o de eventos de diversidad.
- ✓ **Clientes, productos y prácticas empresariales:** Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes concretos y de prácticas de mercado no permitidas.
- ✓ **Ejecución, entrega y gestión de procesos:** Se define como las pérdidas derivadas de errores en ejecución de procesos, operaciones o transacciones, en la administración y diseño de procesos y en las relaciones con transparencia comercial y proveedores.
- ✓ **Interacción en el negocio y fallos en el sistema:** Se define como las pérdidas derivadas de la interrupción de operaciones a causa de problemas en los sistemas.
- ✓ **Fraude interno:** Se define como pérdidas derivadas de alguna acción de fraudar, apropiarse de bienes indebidamente, soslayar regulaciones o leyes o eludir a políticas institucionales en las que se encuentra implicada uno o más funcionarios de la entidad.
- ✓ **Fraude externo:** Se define como pérdidas derivadas de alguna acción por parte de personas ajenas a la institución encaminadas a defraudar, apropiarse de bienes de forma indebida, soslayar la legislación o eludir regulaciones.
- ✓ **Daños a los activos materiales:** Se define como pérdida por daños o perjuicios a activos fijos debido a desastres naturales u otros acontecimientos (Shaw, 2017).

Tipo de evento por riesgo operacional (segundo nivel)

Cabe mencionar que es importante una adecuada gestión de riesgo operacional para poder gestionar de una forma más efectiva la clasificación de estos, de acuerdo a estos tipos genéricos es sumamente importante. Vale aclarar que cada tipo de riesgo operativo tiene subtipos y es necesario penetrar al segundo nivel o hasta donde sea posible, obtener más datos y utilizarlo para una mejor gestión adecuada.

Prácticas de empleo y seguridad en el lugar del trabajo:

- ✓ Fallas en los productos
- ✓ Prácticas impropias en los negocios o en marketing
- ✓ Actividades de asesoramiento

Daños de activos y materiales:

- ✓ Desastres naturales y otros eventos
- ✓ Accidentes y seguridad pública
- ✓ Daño intencional y terrorismo

Ejecución, entrega y gestión de procesos:

- ✓ Introducción, mantenimiento o ejecución de transacciones
- ✓ Monitoreo y reporte
- ✓ Ingreso de clientes y documentación
- ✓ Administración de cuentas de clientes

Fraude externo:

- ✓ Robo o fraude externo
- ✓ Seguridad externa de los sistemas – Daño intencional

Fraude interno:

- ✓ Actividades no autorizadas
- ✓ Robo o fraude interno
- ✓ Seguridad interna de los sistemas – Daños internacionales

Incidencias en el negocio o fallos en los procesos:

- ✓ Fallas en la infraestructura tecnológica (hardware)
- ✓ Fallas en las aplicaciones (software)

Relaciones laborales y seguridad en el ambiente de trabajo:

- ✓ Relaciones laborales
- ✓ Ambiente seguro de trabajo
- ✓ Discriminación y diversidad de empleados (Rafael, 2021).