

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

[DOI 10.35381/cm.v6i2.366](https://doi.org/10.35381/cm.v6i2.366)

## **Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador**

### **Risk management and cybersecurity in the popular and solidarity financial sector of Ecuador**

Fredy Israel Ojeda-Contreras  
[fredy.ojeda96@est.ucacue.edu.ec](mailto:fredy.ojeda96@est.ucacue.edu.ec)  
Universidad Católica de Cuenca, Cuenca  
Ecuador  
<https://orcid.org/0000-0002-8038-5689>

Verónica Paulina Moreno-Narváez  
[veronica.moreno@ucacue.edu.ec](mailto:veronica.moreno@ucacue.edu.ec)  
Universidad Católica de Cuenca, Cuenca  
Ecuador  
<https://orcid.org/0000-0003-1517-6124>

Mireya Magdalena Torres-Palacios  
[mireya.torres@ucacue.edu.ec](mailto:mireya.torres@ucacue.edu.ec)  
Universidad Católica de Cuenca, Cuenca  
<https://orcid.org/0000-0002-4929-6960>  
Ecuador

Recibido: 05 de agosto de 2020  
Aprobado: 01 de octubre de 2020

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

## **RESUMEN**

La gestión de riesgos es un proceso que permite identificar, analizar, evaluar y comunicar los riesgos eminentes a los que están expuestas las entidades financieras con la implementación de la banca digital. Cada vez los hackers y los estafadores infringen las medidas de seguridad de los bancos para cometer actos delictivos, es así que el objetivo de la presente investigación es diseñar estrategias de gestión de riesgos en la Cooperativa de Ahorro y Crédito La Merced como mecanismo de seguridad de la información financiera y de protección de datos de sus clientes. La investigación fue de tipo descriptiva no experimental. Los principales hallazgos demostraron que la entidad no tiene definidas estrategias para gestionar los riesgos cibernéticos, por consiguiente, se propuso estrategias de gestión de riesgo basados en el COSO III, para integrarlos en los procesos de la entidad, mejorando la seguridad y protección de la información.

**Descriptores:** Instituciones financieras; medios electrónicos; riesgos; tecnología de la información. (Palabras tomadas del Tesoro UNESCO)

## **ABSTRACT**

Risk management is a process that allows identifying, analyzing, evaluating and communicating the eminent risks to which financial institutions are exposed with the implementation of digital banking. Every time hackers and scammers violate the security measures of banks to commit criminal acts, so the objective of this research is to design risk management strategies in the Cooperativa de Ahorro y Crédito La Merced as a security mechanism for financial information and data protection of its clients. The research was descriptive, not experimental. The main findings showed that the entity does not have defined strategies to manage cyber risks, therefore, risk management strategies based on COSO III were proposed, to integrate them into the entity's processes, improving the security and protection of information.

**Descriptors:** Financial Institutions; electronic media; risks; information technology. (Words taken from the UNESCO Thesaurus)

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

## INTRODUCCIÓN

La banca digital es una herramienta que durante los últimos años las entidades financieras han venido implementando, es un innovador concepto de servicios bancarios que se realiza desde el teléfono celular, *tablet* o aparato tecnológico; también, es un modelo de gestión ante las necesidades de los usuarios de movilidad, por lo tanto, con la banca digital se realiza cualquier tipo de operación vía *online* en tiempo real y sin tener que esperar más tiempo con largas filas en una sucursal financiera. Es por esta razón que las instituciones financieras a través de la banca digital ofertan una amplia gama de servicios que les permiten a los clientes consultar saldos y un resumen detallado de su cuenta, ejecutar transferencias hacia terceras personas, así como, efectuar pagos de los servicios básicos, de facturas de las diferentes casas comerciales vía *online*, realizar avances con los datos personales, programar pagos automáticos desde la cuenta con la debida autorización de los diferentes prestadores.

En definitiva, los cambios que adopta la banca en la era digital representan hoy en día nuevos riesgos que amenazan su permanencia en el mercado, por lo que, el departamento de gestión de riesgo de las entidades financieras, entre estas cooperativas de ahorro y crédito, deben transfigurarse y familiarizarse a la digitalización para prevenir y mitigar de manera oportuna los riesgos, mediante reglamentos internos de protección de los usuarios y de toda la entidad. Estas medidas deben responder a una oferta de servicios financieros de una manera responsable con los grupos de interés, por consiguiente, los riesgos a los que se enfrentan las entidades están relacionados con el resguardo de datos, identificaciones de los clientes, manejo correcto de la *Big Data* y lo que concierne con la ciberseguridad.

A medida en que las instituciones financieras adopten sus operaciones digitales asumen mayores riesgos de ataques cibernéticos que tienen alta probabilidad de suceder, es así que, en los últimos diez años se ha incrementado la delincuencia cibernética, atacando a los negocios de los diferentes sectores de la economía, en este sentido, los directivos de

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

los entes económicos debe optar por nuevas directrices que garanticen la seguridad de la información, mitigando los riesgos cibernéticos.

La cooperativa de ahorro y crédito La Merced, en los últimos meses ha recibido quejas y reclamos por parte de sus socios que han sido víctimas de la ciberdelincuencia, con la clonación de tarjetas de debito, transferencias interbancarias, entre otros problemas que ha venido enfrentando, por consiguiente, el problema de la investigación radica en: ¿cómo asegurar la información financiera de la cooperativa de ahorro y crédito la Merced ante posibles delitos de ciberdelincuencia?, ante lo expuesto, el objetivo de la investigación consiste en diseñar estrategias de gestión y control de riesgos cibernéticos basado en COSO III en la Cooperativa de Ahorro y Crédito La Merced para la seguridad de la información financiera.

## **Referencial teórico**

### **La seguridad de la información en el sector financiero del Ecuador**

Las instituciones financieras afrontan su digitalización para responder a las exigencias de los cambios del nuevo entorno competitivo y de los hábitos de los consumidores, por tanto, el proceso de digitalización de la banca ha llevado tres fases: partiendo en la innovación de nuevos productos y canales de información, la segunda fase la adaptación a la transformación de la infraestructura tecnológica; y por último, la transición de toda la estructura organizacional para posicionarse en la era digital en un mercado exigente (Cuesta, Ruesta, Tuesta, & Urbiola, 2015).

De otro modo, las tecnologías de la información y comunicación se han convertido en factores relevantes en la transformación de los sectores económicos, es así que, las TIC se definen como activos intangibles procedentes de la innovación tecnológica (*hardware*, *software* y canales de comunicación) que se relacionan con el almacenamiento, procesamiento y transformación de la información en formato digital que permiten la adquisición, producción, tratamiento, comunicación, registro y la presentación de la información en forma de voz, imágenes y datos (Granda, 2017).

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

En este contexto, las instituciones financieras se encuentran hoy en día en constantes transformaciones, debido a las exigencias internas y externas que han venido enfrentando; entre las condiciones internas está la baja rentabilidad de los productos financieros que han tenido en los últimos años, llevándoles a optar por nuevas soluciones flexibles, seguras, dinámicas y competitivas; las condicionantes externas son diversas y se destacan, por una parte, la demanda de servicios financieros más adaptados a las experiencias y necesidades de los clientes a través de los diversos soportes, que se han ido integrando, adaptándose a las tendencias sociales, y por otra parte, la tecnología de la innovación y comunicación, que hace posible la interacción de las actividades como es el caso del sistema financiero; por lo tanto, la entrada de nuevos competidores a un mercado maduro como es el sector bancario y la más importante la creciente seguridad (Sánz, Aristi, & García, 2019).

Por otra parte, en el Ecuador a pesar de los mínimos estándares de calidad en el avance tecnológico, el sector de la banca continúa avanzando, brindando servicios eficientes y atención de calidad al cliente que contribuyen al desarrollo de las familias con la colocación de préstamos pagaderos en un mediano plazo y la generación de rendimientos financieros mediante la captación de ahorros de los clientes (Ordoñez, Narváez, & Erazo, 2020).

Es así que, la banca digital llamada también banca electrónica o virtual, es un servicio que prestan las entidades financieras con la finalidad de que los clientes alcancen a realizar cualquier tipo de operación y transacción con los productos y servicios que se ofertan en las diferentes plataformas de una manera independiente, segura y rápida a través de la página de internet (Carme, 2014), mientras que, para (Trullols, 2018) la banca digital es la transformación del modelo tradicional a un innovador como es el uso del internet como estrategia principal para ofrecer servicios financieros con múltiples ventajas tanto para el cliente como para toda la entidad financiera, al realizar rápido las transacciones y mejorar los procesos internos de la organización, sin embargo, otros autores como (Cuesta, Ruesta, Tuesta, & Urbiola, 2015), afirman que la banca digital

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

consiste en ofertar, distribuir, y vender productos y servicios financieros por medio de canales analógicos, por tanto, permite el aprovechamiento de las nuevas tecnologías para relacionarse mejor con el cliente objetivo y responder rápido a sus necesidades de forma oportuna; en si es la automatización de los servicios.

### **Tendencias de la banca digital en el sector financiero**

El sector bancario siempre ha sido líder en adoptar cambios tecnológicos, en el Ecuador su evolución ha sido lenta, sin embargo, las constantes innovaciones y la integración de aplicaciones digitales han permitido mejorar los servicios financieros con los clientes de *apps* y plataformas *user-friendly* que utilizan los medios digitales para realizar operaciones vía *online*. Desde que aparecieron los cajeros automáticos, las tarjetas de debito/crédito, el internet y el autoservicio *online* facilitaron el retiro de efectivo sin que el cliente tenga que hacer largas filas en las instituciones financieras, en tal razón, la banca ha sabido aprovechar el potencial de la tecnología a su favor, aportando mejores servicios, comodidad, ahorro del tiempo, costos y nuevas experiencias digitales para los clientes.

En este contexto, los cambios tecnológicos trascienden en las actividades tradicionales de las entidades financieras cambiando la forma de hacer negocios; el sector financiero en la red encuentra un nuevo modelo para el desarrollo de las actividades que sobrepasa fronteras donde se comercializan productos virtuales que demandan un constante tráfico de información, es así que, en el Ecuador en los últimos cinco años el crecimiento del uso de los medios electrónicos ha sido del 21%. Según el Banco Central del Ecuador en el año 2017, se realizaron 193,3 millones de transacciones digitales, mientras que, en el 2018 fue de 218,1 millones, por lo tanto, el crecimiento del uso de los medios digitales fue del 13% con relación al año anterior.

De las transacciones que se realizaron en el año 2018, 68 millones corresponden a transferencias de dinero mediante la banca en línea. Al respecto, en el Banco de Guayaquil el 57% de los clientes realizó transacciones desde la banca virtual y la

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

aplicación móvil. En el banco Pichincha el 33% de los clientes realizan transacciones por medio de la banca móvil (Tapia, 2019), hoy en día las cooperativas de ahorro y crédito invierten en departamentos de desarrollo e innovación tecnológica en el marco de la ley ecuatoriana, a pesar de ello, todavía no se aprueban normas que permitan potenciar el uso de la firma electrónica.

Por otro lado, el 50% de los ecuatorianos todavía no está bancarizado, las entidades financieras tienen un largo camino por recorrer, deben seguir potenciando sus procesos de innovación, ya que la digitalización del sector bancario es una oportunidad de crecimiento para atraer más clientes, generar confianza, seguridad y fidelización (ASOBANCA, 2018).

En ese contexto, el 90% de las transacciones son digitales en las diferentes instituciones financieras que hay en el país, no obstante, aún es tarea pendiente para este sector la adopción de nuevas plataformas que permitan llegar a un mayor número de consumidores; con relación a lo mencionado, se debe resaltar el caso de una empresa chilena que creó un innovador servicio personalizado a través de un video dinámico de un minuto y medio para que el cliente alcance a revisar los estados de cuenta reemplazando los tradicionales. Esta innovación no solo se dio en Chile, en Ecuador en el año 2018, la entidad financiera Produbanco también adoptó este servicio, la clave de la firma fue adaptarse a los diferentes canales de comunicación que están utilizando con mayor frecuencia los clientes y a la forma como manipulan los distintos contenidos.

En este orden de ideas, es pertinente caracterizar a las cooperativas de ahorro y crédito, ya que al igual que los bancos forman parte del sistema financiero ecuatoriano. En este sentido, las cooperativas son entidades financieras que tienen como actividad principal captar depósitos y colocarlos en créditos solo a sus socios cooperados. Existen alrededor de 560 cooperativas de ahorro y crédito en el Ecuador, con 7.4 millones socios y con activos totales 14.02 millones de dólares. La mayor parte de los microcréditos otorgados en el país que representan el 69% corresponden al sistema financiero cooperativo (SEPS, 2019).

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

Las entidades del sector financiero popular y solidario de acuerdo al tipo y al total de sus activos se clasificarán por los siguientes segmentos véase (fig. 1):

Segmento	Activos (USD)
1	Mayor a 80'000.000,00
2	Mayor a 20'000.000,00 hasta 80'000.000,00
3	Mayor a 5'000.000,00 hasta 20'000.000,00
4	Mayor a 1'000.000,00 hasta 5'000 000,00
5	Hasta 1'000.000,00
	Cajas de Ahorro, bancos comunales y cajas comunales

**Figura 1.** Segmentación de las entidades del sector financiero popular y solidario.

Las cooperativas de ahorro y crédito están divididas en cinco segmentos, de acuerdo a la suma total de sus activos. En el segmento 1 están 32 cooperativas, las más grandes con activos superiores a \$80 millones, son las más eficientes, presentan buenos balances y poseen una regulación adecuada. El segmento 2 está integrado por 41 entidades, mantienen el 12% de activos totales; el segmento 3 conformado por 80 entidades con el 6% de activos. En los segmentos 4 y 5 se concentran 407 instituciones que apenas representan el 4% del total de los activos del sistema financiero popular y solidario.

Además, estudios ubican a las 100 cooperativas más grandes del país, de acuerdo al volumen de sus activos que registraron en el 2018. Los tres primeros lugares del segmento 1 se le otorga a la cooperativa Juventud Ecuatoriana Progresista Ltda., con 2.098 millones de activos, Jardín Azuayo Ltda. 857.4 millones, y la Policía Nacional Ltda. 773.4 millones. La cooperativa la Merced ocupa el puesto dos con un total de activos de 73.9 millones del segmento 2. Las instituciones que integran este ranking suman en créditos 9.145 millones de dólares, que representan el 82% de todo el sector financiero, tienen oficinas matrices en 16 provincias y por último el 80% de los 7.4 millones de socios atiende todo el sector cooperativo del país (Zabala, Burgos, Chávez, & Calvopiña, 2019).

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

Por otra parte, las cooperativas de ahorro y crédito han ido evolucionando con el tiempo, las nuevas tecnologías no han sido ajenas para este sector, cada vez más están al alcance de sus socios.

Hoy en día las cooperativas son capaces de ofrecer servicios tecnológicos similares a los de la banca tradicional, específicamente con lo relacionado a los medios de pago, han desarrollado plataformas multiservicios y omnicanal en los que se puede tener acceso a cajeros automáticos, tarjetas de débito y crédito. Las cooperativas están a la vanguardia del crecimiento tecnológico, en los últimos años para su permanencia en el mercado invierten en herramientas tecnológicas para no quedar atrás de la competencia.

En fin, las cooperativas se enfrentan en la actualidad a un nuevo modelo de negocio, con fuertes competidores en el mercado financiero y con socios y clientes cada vez más exigentes, con posibilidades de elección casi ilimitadas, al disponer de información más accesible y menos costosa. Al respecto, existen clientes que han evolucionado con el internet, usan las redes sociales y su ritmo de vida es digital; son clientes que ya no piensan acudir a una oficina bancaria, se estima que lo harán una o dos veces al año, y utilizarán el teléfono móvil o computadora de veinte a treinta veces al mes (Rojas, 2017). En sí, las entidades financieras deben ajustarse a las necesidades del mercado para ser más rentables y competitivas (Aterhortúa, 2003).

### **Gestión de riesgos en la banca digital**

Es probable que el tema de los riesgos cibernéticos sea considerado por las instituciones financieras a la hora de la transformación digital, pues surge en materia de gestión de riesgos como un nuevo desafío para la banca. El término riesgo está asociado a la posibilidad de ocurrencia de un acontecimiento negativo que entorpece el desarrollo normal de las operaciones de la entidad, además, impide el cumplimiento a cabalidad de los objetivos, por consiguiente, las organizaciones tienen que estar preparadas para responder ante la ocurrencia del evento con una adecuada gestión para que los impactos en los objetivos sean mínimos (Aterhortúa, 2003).

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

Por otra parte, los riesgos cibernéticos consisten en el robo de información confidencial de los clientes por delincuentes informáticos, *hackers*, grupos criminales, entre otros, con el fin de apropiarse de ella, para cometer estafas electrónicas (Martínez, 2019). Así mismo, las amenazas más peligrosas y de mayor crecimiento en los últimos tiempos han sido los ciberataques, no obstante, la era digital ha afectado más a la región de América Latina, ya que ofrece nuevas experiencias tecnológicas como las redes de internet de banda ancha y móviles 3G y 4G, dando paso a que los empresarios aprovechen la tecnología para ganar más cuota de mercado en el sistema financiero a nivel internacional. Las instituciones bancarias modernas cuentan con el 90% de activos digitales, sin embargo, el nuevo modelo de negocio con tecnología avanzada conlleva mayores riesgos, debido a que también ha crecido la ciberdelincuencia, que se aprovecha de un sistema débil de defensas cibernéticas (Gutierrez, 2017).

En tal sentido, existen tres particularidades que abordan esta nueva etapa: a) la delincuencia cibernética mundial que ha alcanzado un nivel muy alto. b) las tecnologías que permiten la conectividad digital, abriendo puertas al robo de información, devastando procesos comerciales y operativos; y, c) la participación y preocupación de las diferentes instituciones gubernamentales, regulatorias, asociaciones entre otras que unen esfuerzos para contrarrestar las amenazas cibernéticas globales (Drzik, 2018).

En el Ecuador, las cooperativas no son exentas al robo cibernético, por lo que cada vez gestionan estos riesgos con la implementación de tecnologías distintas y estrategias de prevención y detección de fraude, que son reglamentadas por la Superintendencia de Economía Popular y Solidaria, es así que, en el año 2017, el país a nivel de *ranking* mundial ocupó el puesto 66 contra los delitos cibernéticos, en noveno lugar en toda América, y en sexto lugar de América Latina, en el año 2018 se ubicó en el séptimo lugar con mayores ataques de *phishing*, este término, se refiere al robo de identidad, *malware* (hurto de información a través de un *software* malicioso), DDOS (denegación de servicios) el servidor deja de funcionar por lo que se cuelga. Además, en el año 2019 las instituciones financieras recibieron un total de 341928 alertas de seguridad (López, 2019).

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

Así mismo, las alertas que más se recibieron fueron: comportamiento sospechoso como el bloqueo de cuentas, archivos sospechosos que no se deben eliminar, ataque de fuerza bruta hacia la cuenta de los usuarios de *Windows*, intentos de entrega de paquetes maliciosos, entre otros (Mendoza, 2019).

Del mismo modo, la mayor parte de ataques cibernéticos que recibe el país proceden de Brasil, Estados Unidos y China, en un promedio de 10 a 12 ataques informáticos; el delito más común que cometen los ciberdelincuentes es el robo de información a los sistemas vulnerables, empresas y organizaciones gubernamentales (Telégrafo, 2019). Las instituciones financieras se enfrentan cada vez más a los retos del desarrollo de nuevas tecnologías y a los crecientes ataques cibernéticos, por lo tanto, los bancos y las cooperativas de ahorro y crédito deben diseñar planes innovadores en los procesos de ciberseguridad como elemento primordial de la estrategia para atacar cualquier tipo de riesgo.

A demás, las empresas tienen que gestionar un nivel de riesgo mayor que hasta ahora, como riesgos financieros, tecnológicos, reputación, control interno, este nuevo conjunto de riesgos son más dinámicos, están más interconectados, por lo que, en conjunto con los clientes permiten realizar una monitorización integrada y controlar cada uno de estos riesgos de forma proactiva, utilizando las mejores tecnologías que admiten un análisis en tiempo real (Pérez, 2014).

(Miranda, 2012) afirma que, para gestionar los riesgos, hay que diseñar una metodología, donde se identifiquen y clasifiquen los riesgos, para luego, medir la exposición que tiene la organización, así como la incertidumbre o volatilidad de las variables que determinan algún nivel de riesgo. A partir de la identificación, se cualifica y cuantifica el riesgo, diseñándose las estrategias a seguir para responder de manera oportuna y eficiente a los riesgos identificados, que culmina con la definición y apropiación de un conjunto de políticas y procedimientos que permitan controlar todos los procesos.

Por lo mismo, en los riesgos cibernéticos deben contemplarse cuatro pilares fundamentales: seguridad, vigilancia, resiliencia, estrategia y gobierno, por tanto, en el

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

pilar de la seguridad, se organiza el control por el nivel de riesgo, que sea capaz de controlar las amenazas; estos controles están dirigidos a prevenir la fuga de información, dar seguimiento a las aplicaciones y gestionar las identificaciones y acceso de personas. La vigilancia es el segundo parámetro de gestión, se da seguimiento de una manera cuidadosa las amenazas con el fin de reconocer a tiempo comportamientos inseguros. Por otra parte, la resiliencia, es asumir de manera rápida las amenazas, continuar con las operaciones normales y minimizar el impacto del riesgo que afecte a la organización (Castro, 2018). En la actualidad existen entidades que ya realizan esfuerzos en inversiones tecnológicas en ciberseguridad y están enfocadas en mitigar los riesgos y cada vez ir mejorando la estructura para seguir generando confianza en los clientes.

Por otra parte, teniendo en cuenta los grandes cambios que han tenido la industria y los avances tecnológicos, aparece una versión actualizada de un marco integrado de control interno COSO III, que permite una mayor cobertura de los riesgos a los que se enfrentan hoy en día las organizaciones; este marco permite que las empresas desarrollen y mantengan un efectivo y eficiente sistema de control interno que ayude a la adaptación de los cambios, al cumplimiento de los objetivos de las entidades, a mitigar los riesgos a un nivel aceptable, y apoyar la toma de decisiones. El marco integrado de control interno abarca cada una de las áreas de la empresa determinando cinco componentes relacionados con los objetivos de la misma: entorno de control, evaluación de riesgos, actividades de control, sistema de información y comunicación, y por último el componente de supervisión del sistema de control-monitoreo.

Es así que, en cada componente el marco establece 17 principios de control que representan los conceptos fundamentales y que estos deben estar operando en forma conjunta; los principios permiten evaluar la efectividad del sistema control interno, así también, proporciona puntos de enfoque que reconoce que el diseño y la implementación de controles para cada principio y componente, requiere de juicio, por consiguiente, los pasos que propone este marco para iniciar con la aplicación del COSO III son: estudiar y

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

entender, evaluar el estado actual, definir un plan de implementación y comunicar en la organización (Galaz, 2015).

### **Contabilidad en la era digital**

La contabilidad es una ciencia que utiliza técnicas para registrar de una forma sistemática las transacciones diarias de un negocio, que se ven reflejadas en los libros y estados financieros para tener una clara concepción de la parte financiera de la empresa, la misma servirá como referente para la correcta toma de decisiones (Rincón, Mormolejo, & Bolaños, 2012). Para Prada (2015) es una ciencia que tiene como objetivo generar información económica de la empresa, del pasado, presente y futuro, con el fin de disponer datos relevantes para la adopción de decisiones financieras tanto internas como externas; en sí, los dos autores coinciden en que la contabilidad es una ciencia, su fin es generar información financiera de las actividades económicas de la empresa de un cierto periodo, como base para la toma de decisiones.

Por otra parte, en la nueva era digital surge el término de contabilidad digital que no es más que el registro contable por medio electrónico; en este nuevo y revolucionario concepto la contabilidad digital se origina en Ecuador a partir del año 2003 con la factura electrónica; al interior de las empresas se empieza un nuevo estándar para el manejo de las transacciones de forma más técnica. Además, en las transacciones de compra y venta se aplican las nuevas tecnologías, así como también a otros procesos internos de cada organización como las cotizaciones enviadas y recibidas de manera electrónica, comprobantes electrónicos, pedidos electrónicos, órdenes de compra electrónica, entre otros. Después aparecen los formularios electrónicos para hacer las declaraciones del impuesto donde se refleja las compras y ventas del mes, es decir, el principal *input* de todo sistema contable es la facturación digital, que ahora se extiende al output de la contabilidad (Valenzuela, 2010).

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

Para Márquez (2018) los impactos tecnológicos en los procesos contables han sido muy notorios, en la actualidad ya no se requiere contar con facturas impresas, ahora se envían documentos al correo electrónico, mientras que, los informes financieros se encuentran almacenados en un *software* contable, dejándose atrás los procesos con papeles; de la misma forma, la información fluye más rápido con las nuevas plataformas digitales permitiendo disponer de información en tiempo real a la organización y los clientes.

En ese contexto, la contabilidad en las últimas décadas se ha convertido en un factor relevante para la sostenibilidad de las organizaciones y hoy en día se ve afectada por tres variables: complejidad y globalización, tecnología, la formación y educación. La primera variable se refiere a que la contabilidad en la actualidad demanda de nuevos métodos para la presentación y procedimiento de la información financiera; la segunda es la tecnología, es un elemento que está en auge, que ha permitido que los negocios tengan a tiempo información financiera confiable y veraz en cualquier momento para uso interno y externo, mediante la velocidad con la que se generan las transacciones financieras en tiempo real, a través de los medios electrónicos como es el internet y por último la formación y educación que requieren que para los próximos años los gerentes se preparen para dominar los nuevos lenguajes de negocios (Rincón, Mormolejo, & Bolaños, 2012); (Iñiguez, Narváez, & Erazo, 2020).

En la misma línea, los procesos contables automatizados han llevado a cinco tendencias en el mercado, según Deloitte (2015) estas son las actuales:

- En una industria de servicios gestionar los negocios y el manejo de libros contables se ha desarrollado de una forma significativa y seguirá avanzando en respuesta a la cuarta revolución industrial.
- Los procesos contables y administrativos están en plena tendencia automatizada de datos, además se realizan demasiados procesos en la red de internet.
- Permiten procesos interactivos que deben ser creados por las organizaciones.

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

- Las nuevas herramientas tecnológicas y páginas de internet agilizan procesos como transacciones en línea, pagos electrónicos y servicios *online*.
- La centralización de los servicios permite compartir a otros centros.

## **MÉTODO**

El presente estudio de investigación fue de tipo descriptivo no experimental, se observó el fenómeno en un contexto natural sin tener que manipular la información para en lo posterior analizarla (Hernández, 2004). Se enmarcó en un diseño transversal al considerar los datos en un solo momento de recopilación, (Corona, 2010).

La técnica de recolección de datos que se utilizó fue la encuesta, donde se elaboró un cuestionario con 18 preguntas que se enfocaron en el análisis de la seguridad que ofrecen las entidades financieras en las operaciones electrónicas, dicho instrumento se sometió a un proceso de validación por vía de expertos, con los resultados obtenidos se calculó el estadígrafo Alfa de Cronbach, que dio un coeficiente de 0.91, lo que determinó una alta fiabilidad del cuestionario.

No se aplicó un muestreo, sino que se seleccionó por conveniencia a la Cooperativa de Ahorro y Crédito la Merced, en esta institución participaron 10 funcionarios que laboran en los departamentos de contabilidad y de riesgo, para identificar aspectos de la gestión de riesgo relacionados con las operaciones electrónicas.

## **RESULTADOS**

Las tendencias de las entidades financieras en innovar en los múltiples canales de servicio y en la digitalización de los procesos, ha dado paso también a la ciberdelincuencia donde cada vez es más frecuente el robo de la información de las entidades y de las estafas a los clientes, es por eso que, se realizó un estudio de estas variables en la Cooperativa de Ahorro y Crédito La Merced, donde se obtuvieron los siguientes resultados:

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

**Implementación de las nuevas tecnologías:** la implementación de las nuevas tecnologías en la cooperativa responde a las actuales exigencias del mercado y a la permanencia en el mismo, es un avance frente a un mercado más dinámico e innovador así lo señalan el 87% de los encuestados, es así que, en correspondencia con ese resultado el 81% afirman que el año pasado identificaron en sus plataformas digitales tres ataques maliciosos como el *malware* y *phishing*, que es la suplantación de identidad para robar contraseñas o números de tarjetas de débito, y la falta de hábito de escritorio limpio, que con frecuencia expone información en las pantallas de los computadores, papeles, entre otros.

**Delitos cibernéticos:** los delitos informáticos hoy en día conllevan una serie de riesgos por el hecho de usar los medios de la web y las tecnologías de la información y comunicación que se han convertido en uso frecuente de los delincuentes para cometer actos delictivos, En este sentido, se estableció que el 25% de los socios que realizan operaciones electrónicas se vieron afectados en el último año, la mayoría por ataques *phishing*, y *malware*. Ante esta situación, la cooperativa ha venido haciendo esfuerzo para mitigar los riesgos, comprometiéndose con la implementación de un conjunto de prácticas de ciberseguridad, a fin de orientar a sus socios, clientes y empleados a la protección de datos.

**Beneficios de la implementación de las nuevas tecnologías:** la implementación de las nuevas tecnologías es de gran valor para las instituciones financieras porque permite mejorar sus procesos, mantenerse en el mercado financiero y sobre todo responder a los cambios de los clientes que en la actualidad están digitalizados, sobre todo se puede evidenciar que la cooperativa es más eficiente, obtienen datos más rápidos, claros y sobre todo en tiempo real así lo señalan el 90% de los encuestados.

Sin embargo, a pesar de contar con canales virtuales aún existe una fuerte dependencia del 65% de los socios por las oficinas físicas, mientras que, el 35% de socios utilizan las herramientas digitales para realizar operaciones financieras online, de este grupo el 25% lo hace por telefonía celular.

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

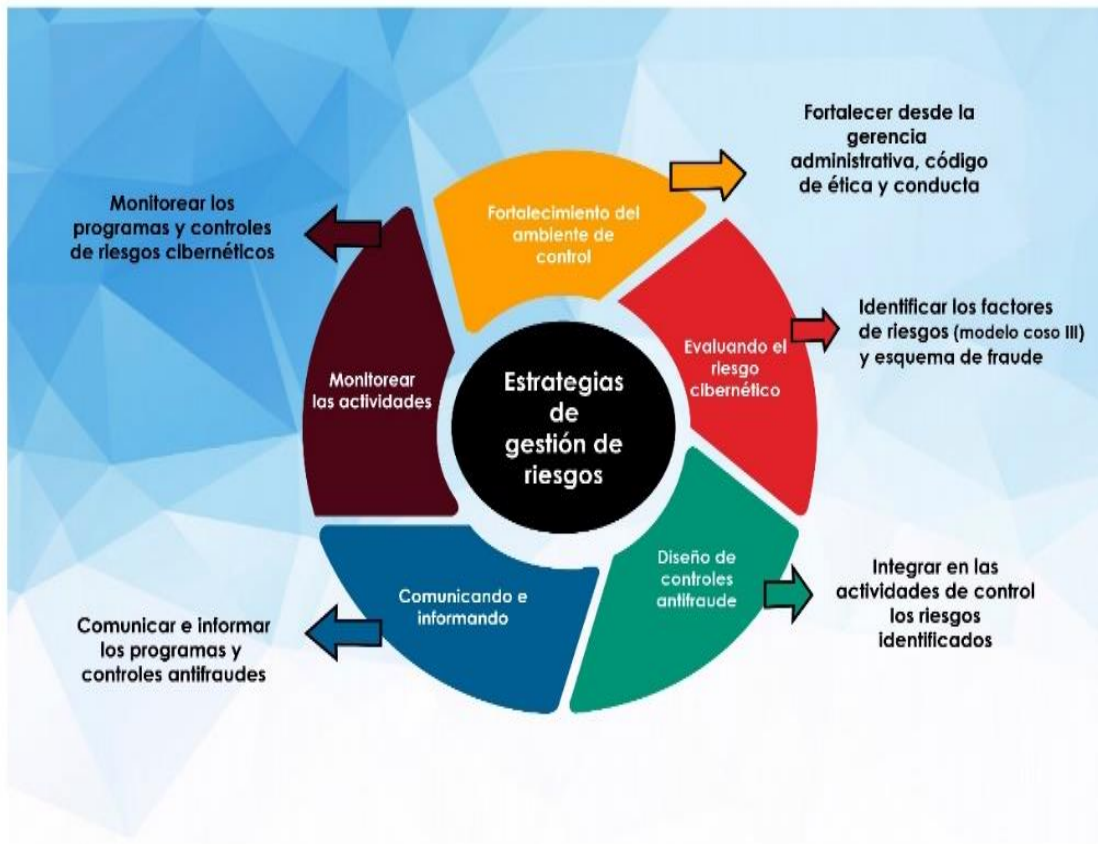
Por otra parte, el 89% de los empleados consultados señalan que la gestión de los riesgos se desarrolla de una manera empírica sin considerar los objetivos estratégicos de la institución.

**Gestión de los riesgos en la banca digital:** el 68% de los consultados afirman que en la cooperativa no se gestiona de manera efectiva y eficiente los riesgos, esto se debe a que los mismos no han sido identificados técnicamente. Los empleados desconocen de un modelo de gestión de riesgos, por consiguiente, el monitoreo establecido para los riesgos es débil. Además, el personal considera que en la cooperativa se debería crear una cultura de riesgo, así lo afirman el 76% de trabajadores, ya que la cooperativa cumple con los objetivos estratégicos establecidos en su planificación, sin embargo, estos no están enfocados en la ciberseguridad.

## **PROPUESTA**

A partir de los resultados de la investigación y del problema identificado se proponen estrategias de gestión de riesgos cibernéticos para la Cooperativa de Ahorro y Crédito La Merced. La metodología para el proceso de gestión de riesgos, se basa en prácticas COSO RM e ISO 31000 que es una norma que establece los lineamientos y principios para gestionar los riesgos. El modelo propuesto abarca toda la estructura empresarial, es decir, personal, gerencia, junta directiva de socios, auditor interno, auditor externo y áreas operativas (ver figura 2)

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios



**Figura 2.** Diseño de gestión de riesgo.

### **Fortalecimiento del ambiente de control**

Es fundamental cifrar cada archivo confidencial, sin importar si está en tránsito hacia un destinatario o almacenado en un servidor, para evitar una violación de datos. Esta estrategia se le recomienda, debido a que es una de las prácticas más importantes de seguridad cibernética. Si un ataque cibernético logra ingresar a la red privada de la entidad financiera, no podrá leer la información en los archivos.

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

Se propone capacitar a los trabajadores de la cooperativa temas de seguridad informática. Además, se sugiere fortalecer el ambiente de control en función de los parámetros expuestos en la figura 3.



**Figura 3.** Fortalecimiento del ambiente de control.

### **Evaluación del riesgo cibernético**

La COAC La Merced debe implementar un proceso de evaluación dinámico e interactivo que le permita identificar, evaluar y gestionar aquellos eventos, tanto internos como externos, que afectan el logro de los objetivos institucionales. A continuación, se propone según la norma ISO 31000 2018 tres pasos para la evaluación de los riesgos.

La evaluación de riesgo cibernético se concreta en tres fases o pasos:

#### **Paso 1.** Identificación de los riesgos

A través de un análisis de los servicios que ofrece la COAC La Merced, así como de cada uno de sus componentes organizativos y procesos operativos, se identificarán los potenciales riesgos que puedan dar paso a fraudes, uso indebido de información y demás potenciales amenazas contra la seguridad empresarial. En este punto se busca que la

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

cooperativa pueda gestionar los riesgos de forma eficiente, permitiendo el cumplimiento óptimo de los objetivos planteados.

Como resultados, se espera que exista la capacidad de reconocer los puntos críticos tanto internos como externos para medir su potencial impacto y probabilidad de que ocurran dichos eventos, para de esta manera prevenirlos. Sumado a esto y en concordancia con la norma ISO 31000, es fundamental que se diseñe y gestione el uso de un sistema de control de riesgo orientado a la mejora continua y vinculada con los objetivos institucionales.

### **Paso 2. Análisis del riesgo**

Tras la identificación del riesgo, es necesario que se proceda con el análisis del mismo. En esta fase, se realizará una calificación de riesgo de forma cuantitativa de manera que sea posible su valoración, comparación y jerarquización de acuerdo al grado de impacto. En el proceso de análisis se adquiere un conocimiento más profundo del riesgo, se describen sus causas y dimensionan sus consecuencias.

El resultado de este punto es un indicador cuantitativo que permite la jerarquización. El nivel de riesgo es el resultado del impacto por la probabilidad.

$$\textbf{Riesgo} = \text{Impacto} \times \text{probabilidad}$$

### **Paso 3. Valoración del riesgo**

La valoración del riesgo implica comparar los resultados en el análisis identificado con los criterios establecidos. En esta etapa se permite determinar cuál de los riesgos requiere de acciones inmediatas, valorar los recursos para dichas acciones y los tiempos de ejecución. Es evidente que se atenderán aquellos riesgos que presentan mayor potencial de perjuicio sobre la seguridad empresarial.

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

### **Diseño de controles antifraude**

La existencia de fraude a través de mecanismos sofisticados en el manejo y manipulación de datos en la red, han motivado a su vez la continua mejora y diseño de sofisticados métodos de control antifraude. En esta dinámica de mejora tanto en los mecanismos utilizados para fraude, como los de control antifraude, existe una competencia constante que han obligado que estos sistemas de control estén en constante análisis, investigación, valoración y perfeccionamiento.

En el entorno cibernético, debido a la complejidad de los sistemas que permiten el manejo financiero en este nuevo entorno, existe también la probabilidad de que dichos sistemas, por su misma complejidad presenten fallas que pueden ser potenciales puertas de entrada a la información.

En este sentido, los controles antifraude que se detallan a continuación se enfocan en determinar los principales riesgos a los que se expone la cooperativa con base al análisis estadístico y de probabilidades de acuerdo a las evidencias existentes, los mismos que permiten diseñar sistemas encargados de controlar los procesos.

- contratar empresas dedicadas a brindar servicios de seguridad de datos. No se habla de una asistencia puntual, sino que se espera que exista un sistema de control que se adapte cada vez a las exigencias de seguridad del sistema implementado.
- Disponer de un sistema riguroso para el manejo de datos que vaya desde el ingreso de los mismos con sistemas de protección de datos a través de encriptación.
- Implementar modelaciones de impacto financiero en función de los riesgos cibernéticos que asume la entidad financiera, con el fin de determinar la relación costo/beneficio, precisando así la proyección de continuidad de estos sistemas.
- Establecer controles de la trayectoria de las operaciones electrónicas en las entidades financieras de forma recurrente, considerando la magnitud de la entidad

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

en cuanto a número de socios y transacciones que se realizan con relación al tiempo.

- Analizar con frecuencia los informes emitidos por el software de ciberseguridad, de manera que, en caso de detectar fraude, se disponga de un tiempo pertinente para investigar el delito, reparar daños y encontrar responsables.
- Establecer la relación entre diferentes indicadores cuantitativos de datos, usuarios, ingresos, trámites, y otros indicadores de acuerdo a la necesidad específica de la cooperativa y el manejo del entorno cibernético, para valorar las diferentes dimensiones de riesgo.
- A fin de mejorar las medidas de seguridad se sugiere valorar: usuarios; posibilidad de ingreso de terceros; medidas de seguridad para el usuario; medidas de seguridad para los funcionarios; control y seguimiento de datos y trámites electrónicos.

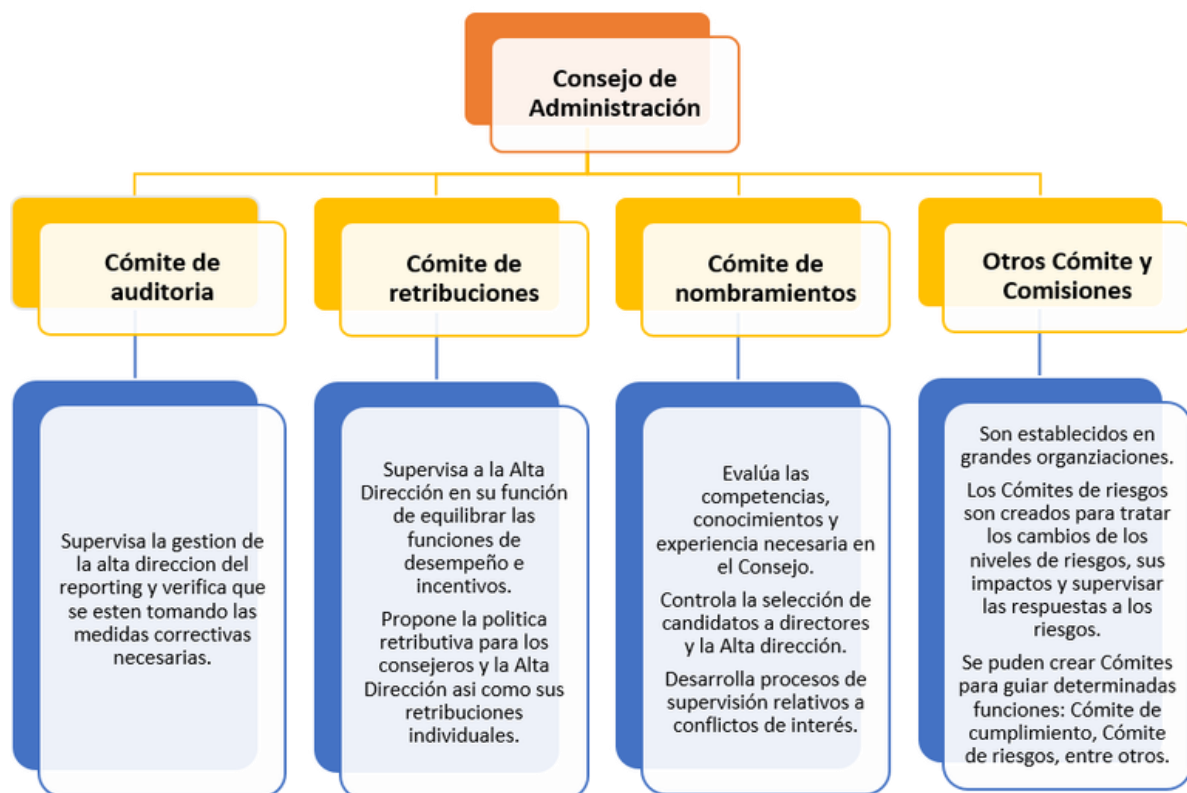
La implementación de estos controles dará como resultado un sistema activo y capaz de retroalimentarse, en función de alcanzar la excelencia en seguridad. El riesgo de fraude siempre existirá potencialmente, lo que implica que el sistema de seguridad implementado no sea estático. Así, el sistema preventivo en paralelo con la evaluación periódica garantizará un sistema confiable.

Para revelar actividades fraudulentas, la cooperativa debe organizar comités que gestionen la supervisión de los riesgos cibernéticos y los riesgos en general, por lo tanto, se motiva a evitar que la supervisión de riesgos relacionados con la ciberseguridad recaiga sobre el equipo de auditores internos quienes asumen la responsabilidad del monitoreo de la información financiera y los riesgos de cumplimiento, quienes por estar sobrecargados de trabajo, pueden descuidar el control de los delitos informáticos.

En la figura 3 se asignan las responsabilidades específicas que debe tener cada comité, siendo el cuarto comité el que debe garantizar que las decisiones relevantes relacionadas con las tecnologías de la información y comunicación, desarrollo de nuevos productos,

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

transformación digital, alianzas estratégicas entre instituciones financieras y otros corresponsales tengan implicaciones de ciberseguridad.



**Figura 4.** Organigrama del comité y funciones de participantes.

### Comunicación e información

La excelencia en cuanto a medidas de gestión de riesgo está basada en la comunicación e información. El diseño general de la estructura y funciones de la entidad financiera debe permitir el flujo de información segura entre los departamentos, así como la precisa definición de roles, de manera que esta disposición de información y adecuada delimitación permitan el manejo seguro de datos.

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

En este sentido, se propone que la comunicación permita a los colaboradores de la cooperativa comprender sus roles y responsabilidades, y esta información sea usada como medio para rendición de cuentas.

Como resultado, se espera que la cooperativa mejore la comunicación de su equipo de trabajo sobre todo del área de auditoría y los comités. La eficacia del control interno depende de la información y comunicación oportuna, es importante que los responsables de las tecnologías de información y comunicación (TIC), estén capacitados tanto en aspectos técnicos de sus funciones como en mecanismos de comunicación y manejo efectivo de trabajo en equipo, garantizando así el cumplimiento de los objetivos.

### **Monitoreo de actividades**

El monitoreo de actividades es el control recurrente de cada una de las actividades propuestas, tanto en la valoración de su eficacia técnica, como logros en relación temporal. Por tanto, se debe realizar un monitoreo constante de las actividades sugeridas en esta propuesta con la finalidad de que el comité de ciberseguridad pueda verificar los resultados de manera efectiva, caso contrario, de no haber conseguido los resultados esperados, se tendrá la posibilidad, de cambiar dichas etapas del modelo, para así mejorar la seguridad de los datos. Los beneficios que se obtendrán del monitoreo de las actividades son:

- Mejora del proceso de toma de decisiones.
- Prevención de problemas.
- Reducción de inactividad.
- Prevención de pérdidas.
- Planificación de presupuestos.

Finalmente, a través del monitoreo se permite contemplar el nivel de gasto generado por los sistemas de seguridad, valorar la relación costo/beneficio y a través de este conocimiento destinar los presupuestos para garantizar su continuidad.

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

## **CONCLUSIÓN**

Cada vez más las instituciones financieras están expuestas a los riesgos cibernéticos debido a la creciente dependencia en la tecnología que podrían tener graves consecuencias de no tomar medidas seguras ante las amenazas eminentes; por ello, la implementación de la transformación digital de cualquier entidad financiera debe estar de la mano de una fuerte inversión en ciberseguridad y de gestión de riesgos para afrontar los nuevos desafíos de hoy en día.

La entidad financiera de estudio fue la Cooperativa de Ahorro y Crédito La Merced con 55 años en el mercado financiero de la ciudad Cuenca con 23 agencias, quienes promueven la intermediación financiera entre sus socios a través de los servicios financieros de ahorros, crédito e inversiones, además seguros de salud, medicina y vivienda, no obstante, los servicios que gestionan por canales digitales representan un riesgo alto que al que los socios y cliente podría estar expuesto.

En la misma línea, la necesidad de la cooperativa de satisfacer las nuevas exigencias de sus socios y clientes le obliga a impulsar una profunda transformación tecnológica, organizacional y cultural, por lo que, su tradicional sistema de control se debilita ante estas nuevas tendencias que requieren de la implementación de mecanismos de control para mitigar los riesgos cibernéticos.

Las estrategias de gestión de riesgos propuestas para la Cooperativa de Ahorro y Crédito La Merced, bajo los componentes de COSO III se enfocan en fortalecer el código de ética y de conducta de los directivos y colaboradores de la institución y a identificar los riesgos eminentes con las nuevas tecnologías para que después sean integradas en las actividades de seguridad.

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

## REFERENCIAS CONSULTADAS

- ASOBANCA. (15 de Diciembre de 2018). *Asociación de Bancos Privados del Ecuador*. Obtenido de <https://url2.cl/2aqEr>
- Aterhortúa, F. (2003). *Gestión y auditoría de la calidad para organizaciones públicas*. [Quality management and auditing for public organizations]. Medellín: Universidad de Antioquia. Obtenido de <https://url2.cl/VEI6K>
- Carme, D. (17 de Junio de 2014). *Definición de Banca Electrónica*. [Definition of Electronic Banking]. Obtenido de <https://url2.cl/h98Ee>
- Corona, J. (2010). *Apuntes sobre métodos de investigación*. [Notes on research methods]. Obtenido de <https://url2.cl/MvNRd>
- Cuesta, C., Ruesta, M., Tuesta, D., & Urbiola, P. (16 de Julio de 2015). *La transformación digital de la banca*. [The digital transformation of banking]. Obtenido de <https://url2.cl/IVC58>
- Deloitte. (2015). *Automatización de Procesos Contables - Administrativos*. [Automation of Accounting - Administrative Processes]. Obtenido de <https://url2.cl/LhN5f>
- Drzik, J. (2018). *MMC Cyber Handbook 2018: Perspectives on the next wave of cyber*. [MMC Cyber Handbook 2018: Perspectivas sobre la próxima ola de cyber]. Obtenido de <https://url2.cl/xFSeF>
- Galaz, Y. (2015). *COSO: Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno*. [COSO: Reference framework for the implementation, management and control of an adequate Internal Control System]. Obtenido de <https://url2.cl/KY55e>
- Granda, A. M. (2017). *Nuevas Tecnologías de la Información y la Conectividad/NTICx: dispositivos, saberes y prácticas*. [New Information and Connectivity Technologies / NTICx: devices, knowledge and practices]. Obtenido de <https://n9.cl/d7za>
- Gutierrez, S. (2017). *Manual de supervisión de riesgos cibernéticos para juntas corporativas*. [Cyber Risk Supervision Manual for Corporate Boards]. Obtenido de <https://url2.cl/Bhl3c>
- Hernández, R. (2004). *Metodología de la Investigación*. [Investigation methodology]. La Habana: Felix Varela. Obtenido de <https://url2.cl/EzezR>

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

- Iñiguez, A. N. (2020). *Impacto de las Normas Internacionales de Información Financiera Unidades Educativas Particulares. [Impact of International Financial Reporting Standards Private Educational Units]*. Obtenido de <https://url2.cl/ZgZPb>
- López, D. (2019). *En la región crecen los delitos cibernéticos. [Cybercrime grows in the region]*. Obtenido de <https://url2.cl/NXhbj>
- Marquéz, C. (2018). *Cambios tecnológicos en la contabilidad. [Technological changes in accounting]*. Obtenido de <https://url2.cl/QUbUF>
- Martínez. (2019). *¿Sabes qué es un ataque cibernético y cuales son los más comunes? [Do you know what a cyber attack is and which are the most common?]*. Obtenido de <https://url2.cl/Tcz6f>
- Mendoza, D. (2019). *GMS participa en la IV edición de las Jornadas de Seguridad Bancaria. [GMS participates in the IV edition of the Banking Security Conference]*. Obtenido de <https://url2.cl/dC75g>
- Miranda, J. (2012). *El Desafío de la Gerencia de Proyectos: Basado en los principios y orientaciones del PMI. [The Project Management Challenge: Based on the principles and orientations of the PMI]*. Colombia: MMeditores. Obtenido de <https://bit.ly/3fmfLMd>
- Ordoñez, E. N. (2020). *El sistema financiero en Ecuador: Herramientas innovadoras y nuevos modelos. [The financial system in Ecuador: Innovative tools and new models]*. Obtenido de <https://url2.cl/cx2Hm>
- Pérez, J. (2014). *Finanzas internacionales: cómo gestionar los riesgos financieros internacionales. [International finance: how to manage international financial risks]*. Chile: Universidad Santiago de CHILE. Obtenido de <https://url2.cl/xY5Td>
- Prada, P. (2015). *La Contabilidad en el siglo XXI. [Accounting in the XXI century]*. Obtenido de <https://url2.cl/gnAUj>
- Rincón, C. A., Mormolejo, G. L., & Bolaños, Á. E. (2012). *Contabilidad siglo XXI [21st century accounting]* (2da ed. ed.). Bogotá, Colombia: Ecoe Ediciones.
- Rojas, L. (2017). *Transformación Digital e Innovación abierta en la banca. [Digital Transformation and Open Innovation in banking]*. Obtenido de <https://url2.cl/5sGU8>

Fredy Israel Ojeda-Contreras; Verónica Paulina Moreno-Narváez; Mireya Magdalena Torres-Palacios

- Sánz, R. A., Aristi, Á. S., & García, R. (2019). *La Transformación digital en el Sector Financiero*. [Digital transformation in the Financial Sector]. Obtenido de <https://url2.cl/7hZth>
- Tapia, E. (2019). *Lideres. La Banca Digital suma usuarios en el mercado Ecuatoriano*. [Leaders. Digital Banking adds users in the Ecuadorian market]. Obtenido de <https://url2.cl/SQg63>
- Telégrafo. (2019). *12 ataques por segundo se registran en Ecuador*. [12 attacks per second are recorded in Ecuador]. Obtenido de <https://url2.cl/X84ps>
- Torres, A. N. (2020). *Auditoría de la responsabilidad social corporativa en el sector financiero popular y solidario*. [Audit of corporate social responsibility in the popular and solidarity financial sector]. doi:doi.org/10.33386/593dp.2020.4-1.282
- Trullols, J. (2018). *¿Qué es la banca digital?* [What is digital banking?]. Obtenido de <https://url2.cl/HMIhS>
- Valenzuela, J. (2010). *Contabilidad digital ¿De qué trata?* [Digital accounting What is it about?]. Obtenido de <https://url2.cl/TaqAr>

2020 por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0) (<https://creativecommons.org/licenses/by-nc-sa/4.0/>)