Banca & Economía

2024

Edición 1426

27 de mayo de 2024

Un enfoque de auditoría para los riesgos cibernéticos

Director:

Jonathan Malagón González

ASOBANCARIA:

Jonathan Malagón González
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

- Durante el último año, las denuncias sobre ataques informáticos, específicamente al sector financiero, crecieron hasta en 400%. Además, del total de los casos de delincuencia informática detectados, en 2022 y 2023 se investigaron 18.317 y 24.288 ciberataques[1], respectivamente.

- Se han desarrollado tecnologías que pueden ser utilizadas con el fin de mejorar la eficiencia y precisión en las auditorías, tales como: (i) la analítica y la minería de datos; (ii) la Inteligencia Artificial y el aprendizaje automático; y (iii) la interconexión de dispositivos físicos a través de internet.

- Implementar un proceso de auditoría efectivo como el que sugiere el Modelo de Auditoría de Ciberseguridad (CSAM), en el cual se da un diagnóstico sobre 18 componentes que influyen en la ciberseguridad de las organizaciones, podría disminuir el impacto financiero hasta en más de USD 100,000 para empresas con más de 1000 empleados[2].

Para suscribirse a nuestra publicación semanal Banca & Economía, por favor envíe un correo electrónico a bancayeconomia@asobancaria.com

[1] Asobancaria (2024). *Informe Mensual de Ciberseguridad.*
[2] Risti (2019). *Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones*. Recuperado de: https://scielo.pt/pdf/rist/n32/n32a04.pdf

Banca & Economía

2024

Edición 1426

Un enfoque de auditoría para los riesgos cibernéticos

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Liz Marcela Bejarano Castillo
Víctor Alejandro Prieto Albarracín
Tanya Jineth Téllez Garcia
Gabriela Montilla Dueñas

La seguridad cibernética, mejor conocida como ciberseguridad, es un esquema compuesto por procedimientos e infraestructuras tecnológicas implementadas para proteger los sistemas informáticos contra ataques, acceso restringido a la información, y en general, contra cualquier tipología de amenaza digital. Esta ha sido reconocida como uno de los pilares esenciales para garantizar la estabilidad y la viabilidad financiera contemporáneas.

En la actualidad, la digitalización avanza a un ritmo exponencial, lo que no solo ha permitido agilizar procesos, sino que ha contribuido sustancialmente a aumentar la eficiencia en nuestras labores diarias. No obstante, la velocidad de su evolución ha hecho necesario que las organizaciones conformen un equipo sólido para prevenir el riesgo cibernético, pues las amenazas informáticas proliferan constantemente diversificando las formas en que se presentan, dificultando así su mitigación. Por esta razón, para mantener la confianza del público y proteger la integridad de la economía global, es imperativo que las entidades tengan la capacidad de salvaguardar los datos almacenados y de resguardar toda clase de activo digital en su poder.

En este sentido, entendiendo la notable presencia de riesgos y de desafíos para combatirlos, la auditoría de ciberseguridad emerge como una herramienta de control para el fortalecimiento de las defensas digitales en las entidades del sector financiero, pues es un mecanismo que permite evaluar la situación actual de una empresa analizando sus riesgos cibernéticos[3] e implementando correctivos sobre aspectos importantes de seguridad, tales como: (i) el grado de exposición de la compañía a ciberataques; (ii) los inconvenientes de la empresa para garantizar la confidencialidad, la integridad y la disponibilidad de la información; (iii) el nivel de eficiencia de los sistemas y programas instalados; entre otros.

Adicionalmente, las auditorías de ciberseguridad no solo buscan detectar y prevenir posibles brechas de seguridad, sino que también contribuyen a garantizar el cumplimiento de regulaciones y estándares, evitando que las instituciones financieras incurran en posibles sanciones y detrimentos reputacionales.

Esta edición de Banca y Economía presenta un análisis sobre la relevancia de las auditorías de ciberseguridad en la banca. En primer lugar, realiza un comparativo internacional con el propósito de resaltar los avances regulatorios alrededor de la ciberseguridad. Luego, describe el entorno digital que rodea al sistema financiero, así como la profundización del uso de la tecnología para su

funcionamiento. En tercer lugar, analiza las amenazas específicas que enfrenta diariamente la banca con el fin de identificar la importancia de las auditorías de ciberseguridad para prevenir estos eventos y sus principales desafíos para enfrentarlos. Adicionalmente, explora los diversos mecanismos de seguridad digital que se han desarrollado, destacando aquellas que puedan ser una buena herramienta de apoyo y fortalecimiento de las áreas de auditoría en las entidades. Finaliza con algunas conclusiones en la materia.

Comparativo internacional

Con la evolución hacia la era digital, diversos organismos internacionales han trabajado en la creación de estándares regulatorios comunes para una gestión efectiva del riesgo cibernético, siendo las de más relevancia (i) la ISO/IEC 27001[4], que establece requisitos para un sistema de gestión de seguridad de la información que incluye evaluación de riesgos, control de acceso, políticas de seguridad y gestión de incidentes, ayudando así a proteger datos de manera sistemática y eficaz; y (ii) la ISO/IEC 27002[5], que proporciona directrices complementarias abarcando aspectos como la gestión de riesgos, el control de acceso a la información, la seguridad física y ambiental, y la gestión de incidentes.

Asimismo, cada país ha adoptado sus propios mecanismos de acuerdo con sus necesidades y condiciones particulares, los cuales son detallados a continuación:

A. Estados Unidos. El Instituto Nacional de Estándares y Tecnología (NIST) desarrolló en febrero de 2024 el marco para la mejora de la ciberseguridad de infraestructuras críticas, proporcionando lineamientos, tales como la detección de amenazas y el desarrollo e implementación del plan de acción ante los incidentes cibernéticos para que toda institución pueda crear, evaluar o mejorar sus programas de ciberseguridad[6].Al respecto, es fundamental destacar que esta normativa abarca perfiles y niveles de madurez que permiten a las organizaciones adaptar su enfoque de ciberseguridad según sus necesidades específicas. Además, proporciona una taxonomía de resultados que facilita la comprensión, evaluación, priorización y comunicación de los esfuerzos relacionados con las buenas prácticas en este ámbito.

B. España. A través del Boletín Oficial del Estado se publicó la Ley 7 de 2022[7] que busca garantizar la seguridad y privacidad en el entorno digital, protegiendo datos personales, transacciones en línea y previniendo delitos cibernéticos. Además, proporciona directrices para la protección de usuarios, dentro de las cuales encontramos: (i) el análisis de las redes 5G, donde se deben identificar las amenazas y vulnerabilidades en los sistemas de control; (ii) la gestión de los riesgos, que establece medidas técnicas y organizativas para garantizar la seguridad en la instalación y la prestación de servicios de quinta generación; y (iii) las sanciones en caso de incumplimiento.

C. Brasil. La Presidencia de la República Civil mediante la Ley 12737[8], conocida como Ley de Delitos Cibernéticos, busca prevenir la comisión de infracciones digitales como el acceso no autorizado a sistemas informáticos, la interrupción de servicios de computadora, la distribución de código malicioso y el fraude en línea, mediante un marco legal que establece las sanciones respectivas.

Adicionalmente, las penas pueden aumentar si la falta cometida resulta en: (i) un perjuicio económico; (ii) la obtención de contenido de comunicaciones electrónicas privadas; (iii) secretos comerciales o industriales; y (iv) el control remoto no autorizado de un equipo.

D. Perú. Se expidió la Ley 30096[9] que previene y sanciona las conductas ilícitas cometidas mediante la utilización de tecnologías que afectan los sistemas de datos informáticos; los principales aspectos claves que se destacan son: (i) el atentado contra la integridad de datos; (ii) el fraude informático; (iii) la suplantación de identidad; y (iv) el abuso de mecanismos y dispositivos.

Además, para lograr mitigar la ocurrencia de estos eventos, en la Ley se establecieron disposiciones complementarias que robustecen los mecanismos de prevención como la creación de protocolos de cooperación operativa entre autoridades y la autorización para que el fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, pueda autorizar la actuación de agentes encubiertos para investigar los delitos contemplados en esta Ley y cualquier delito cometido mediante tecnologías de la información.

E. Chile. La Ley 21663[10], promulgada por el Congreso, creó la Agencia Nacional de Ciberseguridad (ANCI) para regular y sancionar a los organismos públicos y privados que brindan servicios esenciales en caso de incumplir con los lineamientos de ciberseguridad, tales como, (i)

[4] International Organization for Standardization (2022). ISO/IEC 27001:2022. Recuperado de: ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[5] International Organization for Standardization (2022). ISO/IEC 27002:2022. Recuperado de: ISO/IEC 27002:2022(en), Information security, cybersecurity and privacy protection — Information security controls
[6] NIST. Marco de Ciberseguridad. Recuperado de: https://www.nist.gov/cyberframework
[7] Gobierno De España (2022). *Real Decreto-ley 7/2022*.Recuperado de: BOE-A-2022-4973 Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.
[8] Presidência da República (2012). *Lei nº 12.737*. Casa Civil. Recuperado de:https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm
[9] Lpderecho (2013). *ley de delitos informáticos*. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/268450/Ley%20N%C2%BA%2030096.pdf?v=1659988813
[10] Bcn. *Ley 21663 del marco de ciberseguridad*. Recuperado de: https://www.bcn.cl/leychile/navegar?idNorma=1202434&idParte=10496230&idVersion=2222-02-02

requisitos mínimos para enfrentar incidentes tecnológicos, los cuales incluyen el plan de respuesta, equipo de incidentes, notificaciones, reportes y cooperación con otras entidades; (ii) principios rectores, como el control de daños, la cooperación con la autoridad y la seguridad en el ciberespacio.

Por otro lado, se expidió la Ley 21459[11] que define tipos de delitos informáticos como el acceso a información privada, la falsificación tecnológica y el fraude informático, y establece las penas y sanciones económicas correspondientes.

F. Argentina. Este país ha desarrollado normas claves para prevenir y mitigar ataques cibernéticos. Entre las más importantes se encuentran: (i) la Ley 25.326 del año 2000[12], que establece los principios generales de protección de datos personales, regulando la recolección, almacenamiento, uso y transferencia de estos, garantizando la protección de accesos no autorizados y abusos; y (ii) la Ley 26.388 del año 2008[13], que modifica el Código Penal para tipificar y sancionar las infracciones informáticas, estableciendo penas para delitos como el acceso indebido a sistemas y la interceptación de comunicaciones.

G. Uruguay. La Ley 18.719 de 2011[14] en Uruguay asigna a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) la responsabilidad de realizar las políticas de ciberseguridad a nivel nacional.

Bajo esta Ley, la AGESIC desarrolló el Marco de Ciberseguridad[15], que guía la gestión de riesgos en internet, en el correo electrónico y en los centros de datos. En esta se mencionan directrices que sugieren la implementación de sistemas de detección de intrusiones y de phishing, medidas de autenticación y filtrado de spam. Además, se promueve el uso de técnicas de encriptación para proteger la confidencialidad e integridad de los datos durante su almacenamiento y transmisión.

Así mismo, la agencia lleva a cabo programas de capacitación en ciberseguridad para entidades públicas y privadas, fomentando una cultura de seguridad y resaltando la importancia de realizar auditorías periódicas para asegurar el cumplimiento de las políticas de seguridad y la eficacia de las medidas implementadas.

H. Colombia. La Ley 1273 de 2009[16] de Colombia modifica el Código Penal y establece disposiciones para proteger la información y los datos en el ámbito digital. Adicionalmente, se realizan recomendaciones preventivas que sugieren el uso de *firewalls*, antivirus, contraseñas seguras y actualizaciones regulares, así como la promoción de capacitaciones para concientizar sobre la importancia de la ciberseguridad entre los usuarios y empleados.

Asimismo, la Superintendencia Financiera de Colombia (SFC), mediante la Circular Externa 018 de 2021[17], establece las directrices para el Sistema Integral de Administración de Riesgos (SIAR) y el Sistema de Administración de Riesgos de las Entidades Exceptuadas del SIAR (SARE). Esta normativa permite obtener una visión global de las amenazas, incluidos los ciberataques, a las que están expuestas y define las etapas del proceso, las cuales son (i) identificación, considerando factores internos y externos, (ii) medición, que debe ser tanto cuantitativa como cualitativa, (iii) control, implementando medidas para reducir la probabilidad de ocurrencia, y (iv) monitoreo, con seguimiento acorde al perfil y gestión de los riesgos.

Tabla 1. Resumen de la Normativa internacional sobre ciberseguridad

País	Ley	Descripción
Estados Unidos	Marco de Ciberseguridad	El Marco de Ciberseguridad del NIST ayuda a las organizaciones a gestionar sus riesgos.
España	Ley 7 del 2022	La ley garantiza la seguridad de las redes y servicios de comunicaciones electrónicas 5G, enfocándose en generar confianza en su funcionamiento.
Brasil	Ley 12737 del 2018	Esta ley modifica el Código Penal para tipificar infracciones tecnológicas, para quienes violen contraseñas u obtengan datos privados y comerciales sin consentimiento.
Perú	Ley 30096 del 2019	Tiene como objetivo prevenir y sancionar acciones ilícitas que afecten sistemas de datos informáticos mediante tecnologías de la información o comunicación.
Chile	Ley 21459 del 2022 y Ley 21663 del 2024	A través de las cuales crea la Agencia Nacional de Ciberseguridad (ANCI) para regular y penalizar a organismos que ofrecen servicios esenciales como seguridad, transporte, financiación, entre otros, estableciendo normas especiales sobre procedimientos y multas según el grado de incumplimiento.

[11] Bcn. *Ley 21459 de delitos informáticos*. Recuperado de: https://www.bcn.cl/leychile/navegar?idNorma=1177743
[12] Argentina.gob.ar. *Ley 25326 de protección de datos personales*. Recuperado de: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790
[13] Argentina.gob.ar. *Ley 26388 de Delito informático*. Recuperado de: https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto
[14] Normativa y avisos legales (2010). Ley N° 18719. Recuperada de: Ley N° 18719 (impo.com.uy)
[15] Agencia de Gobierno Electrónico y sociedad de la Información del Conocimiento. Nuevo marco normativo de ciberseguridad. Recuperado de: Nuevo marco normativo de ciberseguridad | Agesic (www.gub.uy)
[16] Congreso de la República de Colombia (2009). *Ley 1273 de 2009*. Recuperado de: Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009] (secretariasenado.gov.co)
[17] Superintendencia Financiera de Colombia (2021). Circular Externa 018. Recuperada de: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1055683

Argentina	Ley 25326 de 2000 y Ley 26388 de 2008	Por medio de las cuales se imparten disposiciones de habeas data y tipifican las infracciones informáticas en el código penal respectivamente.
Uruguay	Ley 18719 de 2011	A través del cual se asigna a la AGESIC la responsabilidad dirigir las políticas, metodologías y mejores prácticas, de seguridad de la información.
Colombia	Ley 1273 de 2009 y CE 018 DE 2021	Se dictan disposiciones sobre delitos informáticos, así como medidas para su prevención, investigación y sanción. Así como, se imparte instrucciones relacionadas la administración integral de riesgos

Fuente: Elaboración Asobancaria

Si bien las jurisdicciones han realizado esfuerzos por desarrollar un marco normativo que permita gestionar riesgos y establecer sanciones en lo concerniente a la seguridad informática, es crucial continuar con el diseño dinámico de nuevas regulaciones respaldadas por estudios exhaustivos, pues esto permitirá crear un marco legal sólido capaz de hacer frente a los desafíos del panorama actual de la ciberseguridad.

El contexto de la ciberseguridad en el sector financiero

El sistema financiero colombiano ha experimentado múltiples fases de evolución en su interior; no obstante, una de las más grandes ha sido la transformación digital de sus operaciones, por lo que la banca tiene un fuerte apoyo tecnológico para su funcionamiento. Desde 2020, con la pandemia del COVID-19, se incrementó considerablemente el uso de la tecnología, pues las instituciones financieras cerraron sus oficinas y para continuar atendiendo al público fue necesario hacerlo a través de canales digitales. Sin embargo, no todas estaban preparadas para ello, pues las que no contaban con un desarrollo adecuado de estos sistemas tuvieron que mejorarlos, y aquellas que ya los tenían, debieron fortalecerlos.

Aunque en un principio la aceleración digital se centró en la atención al cliente dada la ocurrencia de este evento, se abrió la puerta a nuevas oportunidades para la optimización de procesos, evitando que los usuarios tuvieran que trasladarse a una oficina para, por ejemplo, adquirir productos financieros o recibir cualquier tipo de asesoría. Por esta razón, actualmente más del 72%[18] de las transacciones se realizan a través de canales informáticos, las cuales en su mayoría se llevan a cabo por medio de la aplicación móvil del banco.

A pesar de que estos avances demuestran un gran desarrollo para las instituciones financieras, también conllevan grandes desafíos debido a que, si bien la banca hace uso de la tecnología para brindar un mejor servicio a sus clientes y productos personalizados acorde con sus necesidades, también hay quienes aprovechan las vulnerabilidades de estos sistemas para conseguir un beneficio, ejecutando un delito denominado ciberataque o ataque cibernético.

Este tipo de violaciones informáticas constituyen una serie de técnicas maliciosas destinadas a explorar y comprometer la seguridad de los sistemas. Entre ellas se encuentran:

- El *phishing*: es una estrategia que consiste en engañar a engañar a los usuarios mediante correos electrónicos o sitios web fraudulentos con el objetivo de obtener información personal, como contraseñas o datos financieros.

- El *pharming*: es una técnica más sofisticada que busca desviar el tráfico web legítimo hacia sitios controlados por los atacantes, vulnerando el *software* o la infraestructura de redes, redirigiendo a los usuarios hacia páginas web falsas sin su conocimiento.

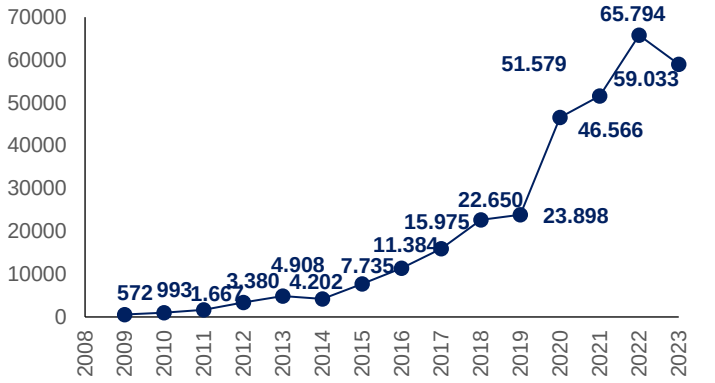
- El *spoofing*: es la suplantación de la identidad de una página web, entidad o persona de confianza para engañar a los usuarios y obtener información confidencial a través de diversas técnicas de *hacking* para falsificar direcciones de correo electrónico o sitios web, lo que les permite generar confianza en las víctimas y llevar a cabo sus ataques de manera efectiva.

- El *ransomware*: es una forma especialmente perniciosa de ciberataque, pues es un *software* malicioso que cifra los datos de la víctima o bloquea el acceso a su dispositivo, exigiendo un rescate a cambio de revertir estos efectos. Por lo general, estos ataques suelen propagarse a través de correos electrónicos fraudulentos o mediante el aprovechamiento de vulnerabilidades en sistemas informáticos, lo que genera grandes pérdidas económicas y daños a la reputación de las organizaciones afectadas.

La creciente sofisticación de estos delitos ha convertido esta problemática en la principal preocupación de las líneas de defensa[19], dada su fuerte proliferación y nivel de complejidad[20]. El volumen de denuncias sobre estas amenazas aumentó en toda la economía a medida que se produjo un mayor desarrollo tecnológico desde 2009 (Gráfico 1). Este comportamiento se evidenció hasta el 2022, pues en 2023 se registró una caída del 10%[21] frente al año anterior. Sin embargo, cabe destacar que la banca, al poseer gran cantidad de datos sensibles y de recursos financieros, es un objetivo atractivo para la ciberdelincuencia.

[18] Universidad Libre (2021). *Impacto del Desarrollo Tecnológico en la Banca de Colombia y su Interacción con los Usuarios*. Recuperado de: https://repository.unilibre.edu.co/bitstream/handle/10901/24078/MD0407.pdf?sequence=1&isAllowed=y
[19] The Institute of Internal Auditors (2013). *Las tres líneas de defensa para una efectiva gestión de riesgos y control.* Recuperado de: PP The Three Lines of Defense in Effective Risk Management and Control Spanish.pdf (funcionpublica.gov.co)
[20] Institute of International Finance (2024). *Managing through persistent volatility: the evolving role of the CRO and the need for organizational agility*. Recuperado de: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-iif-bank-risk-management-survey.pdf
[21] Dirección de Investigación Criminal e Interpol (2023). *Balance de Ciberseguridad*. Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

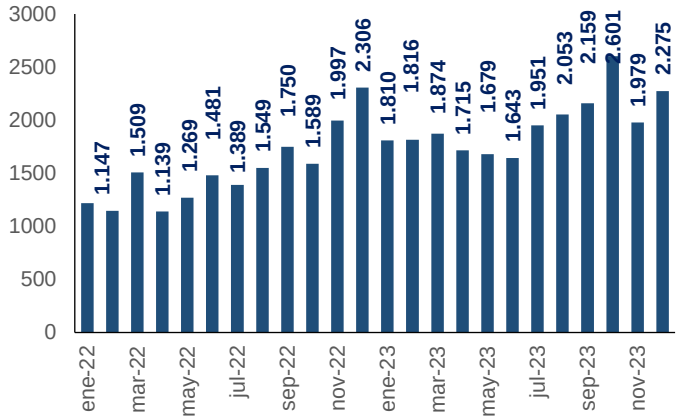
Gráfico 1. Denuncias de delitos informáticos.



Fuente: Datos de la Dirección de Investigación Criminal e Interpol Centro Cibernético Policial. Elaboración de Asobancaria.

En particular para el sector financiero, del total de los casos de delincuencia informática detectados, en 2022 y 2023 se investigaron 18.317 y 24.288 ciberataques[22], respectivamente. (Gráfico 2)

Gráfico 2. Casos investigados por mes.



Fuente: Datos del Informe Mensual de Ciberseguridad de Asobancaria. Elaboración de Asobancaria.

Lo anterior resalta la creciente importancia de la ciberseguridad para las organizaciones, destacando la necesidad de la auditoría para establecer políticas internas que refuercen la capacidad de identificar y responder a los ciberataques.

El rol de la auditoría de ciberseguridad

En la actualidad, la prevención de delitos informáticos se vuelve crucial, puesto que exige una revisión profunda de los protocolos de seguridad de la información en las entidades. En este contexto, la auditoría se convierte en una herramienta fundamental para mitigar los riesgos asociados, tal como lo establece la Ley 1273[23].

En este sentido, la auditoría interna permite anticiparse, adaptarse y responder a los desafíos de seguridad, ya que a través de evaluaciones periódicas puede: (i) identificar posibles riesgos o fallos en las infraestructuras y mecanismos de control de tecnología de la información dentro de la empresa; (ii) verificar que los sistemas implementados satisfagan los requisitos mínimos, tales como el control de almacenamiento, mantenimiento de datos y otros, permitiendo reducir el riesgo de manera anticipada; (iii) analizar el rendimiento y la efectividad de los procedimientos operativos de ciberseguridad; y (iv) suministrar detalles para la preparación de planes de contingencia que hagan frente a ciberataques repentinos u otras debilidades de seguridad[24].

Sin embargo, los factores de riesgos cibernéticos que la auditoría interna debe tener en cuenta abarcan más que simples pruebas de intrusión pues, aunque muchas organizaciones confían en estas medidas, la realidad es que la lucha contra los ciberdelincuentes y la minimización del riesgo de violaciones de datos están evolucionando hacia un enfoque más integral incorporando evaluaciones de los sistemas de comunicación para garantizar la eficiencia en estos procedimientos[25].

Por lo tanto, la proliferación del crimen informático requiere centrar la atención en una amplia gama de procesos que, si no son monitoreados y fortalecidos constantemente, podrían ser puntos vulnerables ante ataques cibernéticos. Al respecto, existen cuatro aspectos críticos que deben evaluarse para evitar la materialización de dichos eventos[26] (Gráfico 3).

Gráfico 3. Aspectos críticos sobre la materialización de eventos.

Fuente: Información obtenida de Grant Thornton. Elaboración de Asobancaria.

[22] Asobancaria (2024). *Informe Mensual de Ciberseguridad.*
[23] Congreso de la República de Colombia (2009). *Ley 1273 de 2009*. Recuperado de: Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009] (secretariasenado.gov.co)
[24] ISACA (2022). *Essentials for an Effective Cybersecurity Audit*. Recuperado de: https://www.isaca.org/resources/news-and-trends/industry-news/2022/essentials-for-an-effective-cybersecurity-audit
[25] Pwc (2023). *Con ciberseguridad, hay resiliencia*. Recuperado de:https://www.pwc.com/co/es/pwc-insights/con-ciberseguridad-hay-resiliencia.html
[26] Grant Thornton (2022*). How internal audit can fortify cybersecurity*. Recuperado de: https://www.grantthornton.com/insights/articles/advisory/2022/how-internal-audit-can-fortify-cybersecurity

De acuerdo con lo descrito en el gráfico 3, en el esquema financiero la auditoría de ciberseguridad no solo debe identificar riesgos y fallos en los sistemas, sino que debe evaluar la eficacia de los controles existentes y elaborar planes de contingencia para contrarrestar ataques repentinos o debilidades en la protección de datos que eviten la prevalencia de la integridad, la confidencialidad y la disponibilidad de la información[27].

Por otra parte, los beneficios de realizar este ejercicio son significativos, ya que proporcionan un diagnóstico que detalla el estado de la seguridad informática de la organización. Al respecto, se destacan: (i) la detección de errores, omisiones o fallos en la administración de datos; (ii) el fortalecimiento de la web, el correo electrónico o los accesos remotos de la institución; y (iii) la actualización de los sistemas y demás herramientas tecnológicas[28].

Lo anterior permite a la alta dirección tomar decisiones informadas sobre la asignación de recursos y la implementación de medidas correctivas. Asimismo, ayudan a aumentar la confianza de los clientes y socios comerciales al ofrecer seguridad y demostrar un compromiso con la protección de los datos y la mitigación de riesgos. Además, contribuyen a evitar costosos incidentes como la pérdida de datos, las multas regulatorias y los daños reputacionales. Sin embargo, estos procesos presentan numerosas dificultades, dada la constante evolución de las amenazas cibernéticas a través de las tecnologías emergentes, por lo que el auditor debe estar a la vanguardia para gestionarlas.

Desafíos en auditoría de ciberseguridad financiera y nuevas herramientas para gestionarlos[29]

En el mundo actual, donde la tecnología evoluciona rápidamente y la dependencia de esta aumenta sin cesar, las instituciones financieras se enfrentan a desafíos cada vez mayores en cuanto a la seguridad de la información y la protección de datos personales. Esto, por su constante exposición a riesgos de ataques cibernéticos dada la creciente adopción de la banca en línea, los pagos móviles y las criptomonedas.

Lo anterior facilita la diversificación del delito financiero, lo cual hace necesario contar con profesionales y equipos de trabajo altamente capacitados para la gestión proactiva de la ciberseguridad en las áreas de auditoría. En este sentido, estos expertos enfrentan el reto de evaluar prácticas y procedimientos de dichas figuras externas de alto riesgo, así como de supervisar la efectividad de las políticas para mitigar amenazas emergentes. Esta supervisión requiere analizar la estrategia general desde una perspectiva informática, de gobernanza y operativa en las organizaciones.

Para ello, se han desarrollado tecnologías que pueden ser utilizadas con el fin de mejorar la eficiencia y precisión de estas labores. Algunas de estas son: (i) la analítica y la minería de datos, que permite a los auditores examinar grandes volúmenes de datos de manera rápida y eficiente en busca de patrones y tendencias que puedan indicar riesgos o áreas de interés para la auditoría; (ii) la Inteligencia Artificial (IA) y el aprendizaje automático, los cuales brindan la posibilidad de automatizar tareas repetitivas y de mejorar la detección de anomalías en los datos; y (iii) la interconexión de dispositivos físicos a través de internet, que puede proporcionar una gran cantidad de datos en tiempo real, facilitando el monitoreo y la automatización[30].

Al respecto, la IA se destaca como la herramienta más revolucionaria, pues su uso, en especial para la auditoría, proporciona la capacidad de sistematizar tareas como la identificación y extracción de datos, el análisis predictivo y la generación automática de informes y documentación. Además, fortalece los controles identificando patrones e irregularidades a través de la evaluación multidimensional de datos y algoritmos de autoaprendizaje que se integren a los sistemas de alerta.

Además, las organizaciones deben tener en cuenta que las ciberamenazas representan una industria en constante crecimiento y que, al irrumpir en sus sistemas, les genera altos costos, tanto monetarios como reputacionales, por perdidas de información. Por lo tanto, resulta imperativo contar con herramientas de tecnología avanzada que permitan mitigar el nivel de exposición ante estas amenazas, así como continuar construyendo un marco normativo sólido que regule su alcance y garantice su uso seguro.

Finalmente, aunque la implementación de las herramientas mencionadas anteriormente suele ser la opción más atractiva, no garantiza alcanzar un nivel óptimo de protección *per se*, pues se ha identificado que, sin la participación de la alta gerencia y constantes capacitaciones al personal, estos instrumentos no agregarían el valor esperado. Por lo tanto, al implementar un proceso de auditoría efectivo como el que sugiere el Modelo de Auditoría de Ciberseguridad (CSAM), en el cual se da un diagnóstico sobre 18 componentes[31] que influyen en la ciberseguridad de las organizaciones, se podría disminuir el impacto financiero hasta en más de USD 100,000 para empresas con más de 1000 empleados[32].

[27] Scielo (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana*. Recuperado de: http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf
[28] Ambit (2021). *¿Qué es una auditoría de seguridad informática? Tipos y Fases*. Recuperado de: https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases
[29] KPMG (2019). The role of internal Audit in cyber security readiness. Recuperado de: The role of internal audit in cyber security readiness (kpmg.com)-
[30] KPMG (2023). El desafío de las nuevas tecnologías aplicadas en la auditoría. Recuperado de: el-desafio-de-las-nuevas-tecnologias-aplicadas-en-la-auditoria.pdf (kpmg.com)
[31] Los componentes son: (i) naciones; (ii) gobernanza y estrategia; (iii) marco legal y conformidad; (iv) activos cibernéticos; (v) riesgos cibernéticos; (vi) marcos y regulaciones; (vii) arquitectura y redes; (viii) información, sistemas y aplicaciones; (ix) identificación de vulnerabilidades; (x) inteligencia de amenazas; (xi) gestión de incidentes; (xii) análisis forense digital; (xiii) educación de concientización; (xiv) ciberseguros; (xv) defensa cibernética activa; (xvi) tecnologías evolutivas; (xvii) recuperación ante desastres; y (xviii) gestión de recursos humanos.
[32] Risti (2019). *Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones*. Recuperado de: https://scielo.pt/pdf/rist/n32/n32a04.pdf

Conclusiones y consideraciones finales

En este documento se destaca la importancia crítica de la auditoría de ciberseguridad en el sector financiero en un contexto de creciente digitalización y sofisticación de amenazas cibernéticas. La transformación digital ha llevado a un mayor uso de la tecnología en las operaciones bancarias, lo que a su vez ha expuesto a las instituciones financieras a una amplia gama de riesgos cibernéticos, desde ataques de *phishing* hasta *ransomware*.

De esta manera, la auditoría de ciberseguridad emergió como una herramienta fundamental para mitigar estos riesgos, proporcionando una evaluación profunda de los protocolos para la protección de datos, identificando posibles vulnerabilidades y proponiendo medidas correctivas. No obstante, la complejidad y la evolución constante de las amenazas cibernéticas, dada la fuerte innovación informática, presentan desafíos significativos para los auditores, quienes deben mantenerse actualizados con las últimas tecnologías y tendencias del crimen cibernético.

En este sentido, para mitigar los efectos negativos asociados, se ha comenzado a trabajar en robustecer los marcos normativos para la gestión de la seguridad de la información y para la adopción de controles que garanticen el uso seguro de herramientas complementarias como la IA en las áreas de auditoría. Además, para enfrentar de forma efectiva a los ciberdelincuentes es necesario que las autoridades y los legisladores de distintas jurisdicciones trabajen mancomunadamente en la construcción de lineamientos que respondan a las necesidades de protección de las entidades y las personas.

Colombia

Principales indicadores macroeconómicos

	2021					2022					2023		2024p
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	**Total**
Producto Interno Bruto													
PIB Nominal (COP Billones)	**1192,6**	337,5	352,6	382,6	389,8	**1462,5**	384,3	378,5	398,01	411,7	**1555,4**	398,9	**1656,3**
PIB Nominal (USD Billions)	**318,5**	86,2	90,1	87,2	81,1	**344,6**	8,081	8,555	9,841	10,010	**36,487**	10,383	**41,575**
PIB Real (COP Billones)	**907,4**	212,9	213,3	230,1	251,1	**907,4**	236,10	239,09	245,7	257,2	**978,2**	237,181	**989,94**
PIB Real (% Var. interanual)	**11**	8,2	12,3	7,4	2,1	**7,3**	2,9	0,1	-0,6	0,3	**0,6**	0,7	**1,2**
Precios													
Inflación (IPC, % Var. interanual)	**5,6**	8,5	9,7	11,4	13,1	**13,1**	13,3	12,1	11	9,2	**9,28**	**7,3**	**5,29**
Inflación sin alimentos (% Var. interanual)	**3,4**	5,3	6,8	8,3	10	**10**	11,4	11,6	11,5	5,0	**10,33**	**8,7**	**5,51**
Tipo de cambio (COP/USD fin de periodo)	**3981**	3748	4127	4532	4810	**4810**	4627	4191	4054	3822	**3822**	**3842**	**3857**
Tipo de cambio (Var. % interanual)	**16**	0,3	9,9	18,2	20,8	**20,8**	23,5	1,5	-10,6	-19,32	**-19,32**	**-16,9**	**0,90**
Sector Externo													
Cuenta corriente (USD millones)	**-17.951**	-5.531	-4.889	-6.194	-4.720	**-21.333**	-3.067	-2.345	-1.680	-2.293	**-9.715**	-	**-13.715**
Déficit en cuenta corriente (% del PIB)	**-5,7**	-6,4	-5,4	-7,1	-5,8	**-6,2**	-3,8	-2,7	-1,7	-3,9	**-2,7**	-	**-3,2**
Balanza comercial (% del PIB)	**-6,4**	-5,9	-3,5	-5,2	-4,7	**-4,8**	-2,9	-2,6	-1,5	-3,9	**-2,3**	-	**-3**
Exportaciones F.O.B. (% del PIB)	**13,6**	19,2	21,7	22,2	21,7	**21,3**	21	19,3	17,5	28,9	**14,4**	-	**11,5**
Importaciones F.O.B. (% del PIB)	**18**	25,1	25,2	27,3	26,4	**26,1**	23,9	21,8	19	32,5	**16,3**	-	**14,3**
Renta de los factores (% del PIB)	**-2,8**	-4,2	-5	-5,5	-5,1	**-5**	-4,7	-3,7	-3,6	-6,0	**-4**	-	**-3,6**
Transferencias corrientes (% del PIB)	**3,4**	3,7	3,1	3,6	3,9	**3,6**	3,8	3,6	3,4	5,7	**3,6**	-	**3,3**
Inversión extranjera directa (pasivo) (% del PIB)	**3**	5,7	5,6	3,6	5	**4,9**	5,2	6,1	3,4	6,6	**3,8**	-	…
Sector Público (acumulado, % del PIB)													
Bal. primario del Gobierno Central	**-3,7**	-0,3	0,1	0,2	-1	**-1**	0,3	1,2	0,2	…	**-0,3**	-	**-0,9**
Bal. del Gobierno Nacional Central	**-7,1**	-1,2	-1,1	-1,1	-2	**-5,3**	-0,8	0	-0,6	…	**-4,2**	-	**-5,3**
Bal. primario del SPNF	**-3,5**	…	…	…	…	**-1,6**	…	…	…	…	**1,7**	-	**1,8**
Bal. del SPNF	**-7,1**	…	…	…	…	**-6,2**	…	…	…	…	**-2,6**	-	**-3,2**
Indicadores de Deuda (% del PIB)													
Deuda externa bruta	**53,9**	53,5	51,3	50,6	53,4	**53,4**	55,2	56,1	…	…	…	-	…
Pública	**32,2**	31	29,4	28,8	30,4	**30,4**	31,4	31,8	…	…	…	-	…
Privada	**21,7**	22,5	21,9	21,8	23	**23**	23,8	24,2	…	…	…	-	…
Deuda neta del Gobierno Central	**60,1**	49,3	51,9	54,9	57,9	**57,9**	52,7	50,8	50,7	…	**52,8**	-	**57,0**

p: Proyecciones de Asobancaria

Colombia

Estados financieros del sistema bancario

	dic-19	dic-20	dic-21	dic-22	mar-24 (a)	feb-24	mar-23 (b)	Var. real anual (b) - (a)
Activo	**675.063**	**729.841**	**817.571**	**924.121**	**950.687**	**953.985**	**929.597**	**-4,8%**
Disponible	45.684	53.794	63.663	58.321	51.263	56.365	59.683	-20,0%
Inversiones	127.332	158.735	171.490	180.818	190.125	187.974	183.462	-3,5%
Cartera de crédito	478.705	498.838	550.204	642.473	657.313	656.429	646.002	-5,2%
Consumo	147.144	150.527	169.603	200.582	192.014	193.072	199.857	-10,5%
Comercial	251.152	263.018	283.804	330.686	342.582	341.194	333.183	-4,2%
Vivienda	67.841	72.565	82.915	95.158	104.116	104.068	96.377	0,6%
Microcrédito	12.568	12.727	13.883	16.047	18.601	18.095	16.585	4,5%
Provisiones	29.173	37.960	35.616	37.224	40.050	39.568	38.350	-2,7%
Consumo	10.779	13.729	12.251	15.970	18.492	18.445	17.224	0,0%
Comercial	15.085	17.605	17.453	16.699	16.628	16.259	16.521	-6,3%
Vivienda	2.405	2.691	3.021	3.189	3.452	3.440	3.227	-0,4%
Microcrédito	903	1.133	913	858	1.322	1.268	997	23,6%
Pasivo	**585.086**	**640.363**	**713.074**	**818.745**	**848.616**	**849.024**	**826.712**	**-4,4%**
Depósitos y otros instrumentos	500.862	556.917	627.000	686.622	733.193	742.076	695.245	-1,8%
Cuentas de ahorro	197.307	246.969	297.412	297.926	288.264	294.169	274.460	-2,2%
CDT	156.421	154.188	139.626	207.859	281.594	280.701	251.045	4,5%
Cuentas Corrientes	60.491	75.002	84.846	80.608	70.943	72.075	74.740	-11,6%
Otros pasivos	9.145	9.089	9.898	11.133	9.954	9.874	11.786	-21,3%
Patrimonio	**89.977**	**89.479**	**104.497**	**105.376**	**102.071**	**104.961**	**102.885**	**-7,6%**
Utilidades (año corrido)	**10.963**	**4.159**	**13.923**	**14.222**	**2.227**	**903**	**3.089**	**-32,8%**
Ingresos financieros de cartera	46.297	45.481	42.422	63.977	22.494	14.973	21.903	-4,3%
Gastos por intereses	16.232	14.571	9.594	28.076	14.685	9.823	14.362	-4,8%
Margen neto de intereses	31.107	31.675	33.279	38.069	9.256	6.050	8.971	-3,9%
Indicadores (%)								
Calidad	**4,28**	**4,96**	**3,89**	**3,61**	**5,06**	**5,00**	**4,23**	**0,82**
Consumo	4,69	6,29	4,37	5,44	8,27	8,19	6,68	1,59
Comercial	4,19	4,55	3,71	2,73	3,58	3,53	3,16	0,42
Vivienda	3,25	3,30	3,11	2,47	3,12	3,12	2,54	0,58
Microcrédito	6,87	7,13	6,47	5,46	9,96	9,55	6,15	3,81
Cubrimiento	**142,4**	**153,5**	**166,2**	**160,6**	**120,5**	**120,5**	**140,2**	**19,72**
Consumo	156,1	145,1	165,4	146,4	116,5	116,6	129,0	-12,49
Comercial	143,5	147,1	165,6	184,7	135,6	135,2	156,9	-21,32
Vivienda	109,1	112,3	117,1	135,5	106,4	105,8	131,9	-25,51
Microcrédito	104,6	124,8	101,7	97,9	71,4	73,4	97,7	-26,37
ROA	1,6	0,6	1,7	1,5	0,9	0,6	1,3	-0,40
ROE	12,2	4,6	13,3	13,5	9,0	5,3	12,6	-3,54
Solvencia	14,7	16,3	20,5	17,1	16,0	16,6	16,4	-0,35
IRL	211,9	213,1	204,4	183,7	200,5	188,1	209,9	-9,41
CFEN G1	0,0	109,3	113,5	109,6	113,5	115,0	108,5	5,04
CFEN G2	0,0	136,1	134,4	127,3	130,1	131,1	127,8	2,25

Nota: G1 corresponde a bancos con activos superiores al 2% del total y G2 a bancos diferentes a G1 que tengan cartera como activo significativo.

Colombia

Principales indicadores de inclusión financiera

	2017	2018	2019	2020	2021					2022				2023
	Total	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	Total
Profundización financiera - Cartera/PIB (%) EC + FNA	**50**	**49,7**	**49,9**	**55,4**	55,3	53,3	51,9	50,9	**50,9**	50	49,4	48,6	48,3	**48,3**	**46,1**
Efectivo/M2 (%)	**13,6**	**14**	**15**	**16,6**	16	16,5	16,5	17	**17**	16,2	15,9	15,6	16,3	**16,3**	**15,03**
Cobertura															
Municipios con al menos una oficina o un corresponsal bancario (%)	**100**	**99,2**	**99,9**	**100**	100	100	100	100		100	100	100	100	**100**	-
Municipios con al menos una oficina (%)	**73,9**	**74,4**	**74,6**	**78,6**	72,8	72,9	72,8	72,8	**78,8**	79,1	77,8	77,8	78,7	**78,7**	-
Municipios con al menos un corresponsal bancario (%)	**100**	**98,3**	**100**	**100**	100	100	100	92,7		98,6	98,7	99,6	100	**100**	
Acceso															
Productos personas															
Indicador de bancarización (%) SF*	**80,1**	81,4	**82,5**	**87,8**	89,4	89,4	89,9	90,5	**90,5**	91,2	91,8	92,1	92,3	**92,3**	-
Adultos con: (en millones)															
Al menos un producto SF	**27,1**	**28,0**	**29,4**	**31,2**	32,7	32,9	33,1	33	**33,5**	33,8	34,2	34,4	34,7	**34,7**	-
Cuentas de ahorro	**25,16**	**25,8**	**26,6**	**27,9**	28,4	28,3	28,6	28,9	**28,9**	29,2	29,5	29,6	29,9	**29,9**	-
Cuenta corriente SF	**1,73**	**1,89**	**1,97**	**1,9**	1,9	1,9	1,9	1,9	**1,9**	1,9	1,9	1,8	1,8	**1,8**	-
Cuentas CAES SF	**2,97**	**3,02**	**3,03**	**3**	3,0	3,0	3,0	Depósitos de bajo monto							
Cuentas CATS SF	**0,1**	**2,3**	**3,3**	**8,1**	9,2	10,5	11,8		**21,1**	21,7	22,4	23,0	23,5	**23,5**	-
Depósitos electrónicos	**4,2**	**4,9**	**6,7**	**11,6**	12,7	13,1	13,7								
Productos de ahorro a término (CDTs)	**0,78**	**0,81**	**0,85**	**…**	0,85	0,83	0,75	-	**-**	0,8	0,8	0,9	0,9	**0,9**	-
Crédito de consumo SF	**8,0**	**6,8**	**6,9**	**6,8**	6,86	6,9	6,9	6,9	**6,9**	7,1	7,4	7,7	7,8	**7,8**	-
Tarjeta de crédito SF	**9,2**	**8,9**	**8,4**	**8,1**	8,11	8,1	7,7	7,9	**7,9**	8,0	8,2	8,4	8,5	**8,5**	-
Microcrédito SF	**3,3**	**3,1**	**2,5**	**2,4**	2,44	2,4	2,3	2,3	**2,3**	2,30	2,34	2,36	2,3	**2,3**	-
Crédito de vivienda SF	**1,1**	**1,1**	**1,1**	**1,2**	1,19	1,1	1,2	1,2	**1,2**	1,23	1,25	1,27	1,3	**1,3**	-
Crédito comercial SF	**0,8**	**-**	**0,7**	**0,4**	0,54	0,5	0,4	0,2	**0,2**	0,46	0,45	0,44	0,5	**0,5**	-
Uso															
Productos personas															
Adultos con: (%)															
Algún producto activo SF	**68,6**	**68,5**	**66**	**72,6**	74,4	74,6	75,5	74,8	**74,8**	76,2	76,9	77,7	77,2	**77,2**	-
Cuentas de ahorro activas SF	**71,8**	**68,3**	**70,1**	**64,2**	62,2	65,3	65,8	65,7	**65,7**	65,9	65,2	64,9	51,9	**52**	-
Cuentas corrientes activas SF	**83,7**	**85,5**	**85,6**	**82,3**	82,3	80,2	78,5	73,7	**73,7**	76,9	76,5	76,3	74,5	**75**	-
Cuentas CAES activas SF	**89,5**	**89,7**	**82,1**	**82,1**	82,1	82,2	82,1	Depósitos de bajo monto							
Cuentas CATS activas SF	**96,5**	**67,7**	**58,3**	**74,8**	72,3	73,8	75,1		**76,3**	77,8	78,6	80,2	78,6	**78,6**	-
Depósitos electrónicos	**95,0**	**39,0**	**38,3**	**65,5**	70,1	71,4	71,7								
Productos de ahorro a término (CDTs)	**62,7**	**61,2**	**62,8**	**-**	69,5	64,6	75,6	-	**-**	77,5	79,3	80,1	73,2	**73,2**	-

Colombia

Principales indicadores de inclusión financiera

	2016	2017	2018	2019	2020	2021					2022				
	Total	Total	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total
Acceso															
Productos empresas															
Empresas con: (en miles)															
Al menos un producto SF	**751,8**	**935,8**	**947,4**	**939,6**	**925,2**	926,3	924,2	923,8	1028,6	**1028,6**	1029,0	1038,7	1065,7	1077,1	**1077,1**
*Productos de depósito SF	**436,2**	**498,5**	**925,3**	**908,9**	**898,9**	899,2	897,6	898,2	997,9	**998,9**	1004,0	1013,0	1039,8	1046,4	**1046,4**
*Productos de crédito SF	**221,1**	**231,5**	**323,105**	**286,192**	**284,2**	368,9	287,4	282,8	280,2	**280,2**	289,6	294,2	300,6	380,2	**380,2**
Uso **Productos empresas** Empresas con: (%)															
Algún producto activo SF	**74,7**	**72,1**	**71,6**	**68,4**	**68,1**	68,3	68,2	68,1	70,5	**70,5**	71,4	71,2	72,1	72,4	**72,4**
Operaciones (semestral)															
Total operaciones (millones)	**4.926**	**5.462**	**6.334**	**8.194**	**9.915**	-	4.939	-	6.222	**11.161**	-	6.668	-	7.769	**14.397**
No monetarias (Participación)	**48**	**50,3**	**54,2**	**57,9**	**61,7**	-	55,4	-	56,7	**56,1**	-	55,4	-	56,0	**55,8**
Monetarias (Participación)	**52**	**49,7**	**45,8**	**42**	**38,2**	-	44,6	-	43,3	**43,8**	-	44,6	-	44,0	**44,2**
No monetarias (Crecimiento anual)	**22,22**	**16,01**	**25,1**	**38,3**	**28,9**	-	-8,7	-	12,4	**2,3**	-	34,0	-	23,2	**27,9**
Monetarias (Crecimiento anual)	**6,79**	**6,1**	**6,7**	**18,8**	**10**	-	30,5	-	29,3	**29,1**	-	33,1	-	27,1	**29,8**
Tarjetas															
Crédito vigentes (millones)	**14,9**	**14,9**	**15,3**	**16,1**	**14,7**	14,9	14,6	15,0	15,6	**15,6**	15,9	16,0	16,1	16,0	**16,0**
Débito vigentes (millones)	**25,2**	**27,5**	**29,6**	**33,1**	**36,4**	39,2	38,4	39,7	40,8	**40,8**	41,1	42,6	43,7	45,8	**45,8**
Ticket promedio compra crédito ($miles)	**205,8**	**201,8**	**194,4**	**203,8**	**207,8**	197,6	208,2	201,4	219,9	**219,9**	215,3	225,2	209,5	225,6	**225,6**
Ticket promedio compra débito ($miles)	**138,3**	**133,4**	**131,4**	**126,0**	**129,3**	116,8	118,1	114,5	124,9	**124,9**	119,1	116,5	112,5	108,1	**108,1**