CIBERSEGURIDAD DE LA IDENTIDAD DIGITAL EN LAS TRANSACCIONES ELECTRÓNICAS BANCARIAS EN COLOMBIA

DIEGO ANDRÉS SÁNCHEZ PEÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2023

CIBERSEGURIDAD DE LA IDENTIDAD DIGITAL EN LAS TRANSACCIONES ELECTRÓNICAS BANCARIAS EN COLOMBIA

DIEGO ANDRÉS SÁNCHEZ PEÑA

Proyecto de Grado – Monografía presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Edgar Mauricio López Rojas
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2023

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 21 de junio de 2023

DEDICATORIA

Dedico este trabajo a las personas que participaron en mi decisión de afrontar este compromiso nuevo.

AGRADECIMIENTOS

Agradezco a Dios las condiciones y circunstancias personales, académicas y profesionales favorables para la consecución de este logro.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZA: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

APT (ADVANCED PERSISTENT THREAT: Una amenaza persistente avanzada (*Advanced Persistent Threat* o APT, por sus siglas en inglés), es un ataque cibernético prolongado y dirigido en el que un intruso obtiene acceso a una red y permanece sin ser detectado por un período de tiempo. La intención de un ataque APT generalmente es monitorear la actividad de la red y robar datos en lugar de causar daños a la red u organización.

BANCA ELECTRÓNICA: Tipo de banca que se realiza por medios electrónicos como puede ser cajeros electrónicos, teléfono y otras redes de comunicación. Tradicionalmente, este término ha sido atribuido a la banca por Internet o banca online, pero conviene aclarar su significado. Algunos autores lo consideran como un constructo de orden superior que supone varios canales que incluyen también la banca telefónica, la banca por teléfono móvil (basada en tecnología Wireless *Application Protocol* –WAP– que traslada Internet al teléfono móvil) y la basada en televisión interactiva (iNet-television).

BANCA MÓVIL: Servicio proporcionado por un banco u otra institución financiera que le permite realizar transacciones financieras de manera remota usando un dispositivo móvil como un smartphone, una tableta o incluso un reloj pulsera de alta tecnología. La banca móvil permite realizar muchas de las mismas actividades que la banca por Internet; no obstante, a diferencia de la banca por Internet relacionada, la banca móvil usa un software, generalmente denominado app, proporcionado por la institución financiera.

BANCARIZACIÓN: Grado y nivel de utilización que una población dentro de una economía hace de productos y servicios bancarios. En el ámbito de la economía, el grado de bancarización expresa la intensidad e incidencia que la red bancaria tiene en la economía, y refleja además el grado de progreso del sistema financiero de un país.

BIG DATA: Gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional, ya que superan los límites y capacidades de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos. Dicho concepto engloba infraestructuras tecnológicas y servicios que han sido creados para dar solución al procesamiento de enormes

conjuntos de datos estructurados, no estructurados o semiestructurados (mensajes en redes sociales, señales de móvil, archivos de audio sensores, imágenes digitales, datos de formularios, emails, datos de encuestas, logs, etc.

CIBERDELINCUENCIA: Acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito.

CIBERDELINCUENTE: Persona que realiza actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.

CIBERSEGURIDAD: Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

CLONACIÓN DE TARJETAS: O *skimming* en inglés, sucede cuando se duplica una tarjeta (crédito o débito) mediante la falsificación de la banda magnética. Los estafadores copian la banda magnética pasándola por un *skimmer* (dispositivo que almacena los datos de la banda magnética). Además, se encargan de conocer la clave secreta (de diferentes maneras) y utilizan estos datos para generar una nueva tarjeta idéntica a la original, con la que podrán realizar diversos fraudes.

CLOUD COMPUTING: Cloud o la computación en la nube es acceso bajo demanda, a través de Internet, a recursos informáticos como aplicaciones, servidores (físicos y virtuales), almacenamiento de datos, herramientas de desarrollo, funciones de red y más, alojados en un centro de datos remoto gestionado por un proveedor de servicios en la nube (o CSP). El CSP ofrece estos recursos en un plan de suscripción mensual o los factura según el uso.

CONSUMIDOR FINANCIERO: Es todo cliente, usuario o cliente potencial de las entidades vigiladas, de acuerdo con lo establecido en la ley colombiana.

E-LEARNING: El *e-learning* es una modalidad educativa en donde el proceso de enseñanza-aprendizaje se encuentra apoyado en el uso de las tecnologías de información y comunicación -TIC-.

HACKING: Conjunto de técnicas utilizadas para introducirse en un sistema informático vulnerando las medidas de seguridad, con independencia de la finalidad con la cual se realice, puede ser lícito y solicitado.

HACKTIVISMO: El hacktivismo es la ideología o filosofía que sustenta la práctica del hacking, y que podemos entender como una extensión social del deseo de libertad de información y conocimiento propio de la práctica del *hacking*.

HIPERCONNECTIVIDAD: Es un término creado en 2001 y que se utiliza para designar los distintos medios de comunicación con los que contamos actualmente como el correo electrónico, las redes sociales, la mensajería instantánea, el teléfono y el internet.

INGENIERÍA SOCIAL: Técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.

MALWARE: Término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

PHARMING: Esta modalidad de malware es más elaborada ya que infecta el dispositivo del cliente por medio de un código malicioso que modifica algunos archivos del sistema operativo. Esta modificación hace que cuando el cliente digite en el navegador la página del banco sea dirigido a una página falsa sin que el cliente se percate para que ingrese sus datos bancarios.

PHISHING: Técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial.

RANSOMWARE: Término que hace referencia a un tipo de malware que luego de comprometer un equipo secuestra su información para extorsionar a las víctimas, solicitando el pago de una suma de criptomonedas para recuperar esos datos. La palabra es un acrónimo de las palabras ransom (rescate) y software.

RIESGO: Es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus. El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo.

SENDER POLICY FRAMEWORK: El protocolo SPF, que significa «*Sender Policy Framework*», es un protocolo que se basa en su nombre de dominio y se utiliza para certificar que la IP emisora está autorizada para el envío de e-mails. Este protocolo se utiliza para impedir el uso fraudulento de su nombre de dominio y evitar que terceros se hagan pasar por usted. Este protocolo es especialmente eficaz contra los ataques de suplantación de identidad o phishing.

SIM CARD: O *Subscriber Identity Module*, por sus siglas en inglés, es una pequeña tarjeta de plástico que tiene un chip pegado a ella. Este chip, almacena de manera segura el número de teléfono, así como las claves de acceso de un usuario concreto en una operadora de telefonía.

SIM SWAPPING: Fraude que permite a los criminales robar la identidad mediante el secuestro del número del número de teléfono al obtener un duplicado de la tarjeta *SIM Card*.

SIMPLE MAIL TRANSFER PROTOCOL: El protocolo SMTP (*Simple Mail Transfer Protocol*) o también conocido como “Protocolo de Transferencia simple de correo” es el protocolo utilizado cuando vamos a enviar un correo electrónico a través de un servidor de correo. Este protocolo se utiliza por los clientes locales de email para enviar los mensajes de email al servidor de correo remoto, por tanto, actúa únicamente en sentido salida.

SMISHING: Técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto.

SPOOFING: Consiste en usurpar una identidad digital y/o electrónica para ocultar la propia identidad y así cometer delitos en Internet. Existen 3 tipos: *spoofing* de correo electrónico, *spoofing* de IP y *smart-spoofing* IP. Es una técnica de suplantación de identidad en la red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las redes usando técnicas de *spoofing* ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

TECNOLOGÍA EMV: Conjunto de estándares de seguridad para las transacciones con tarjeta de débito y crédito, que también pueden usarse para los pagos móviles NFC. Comúnmente llamadas "tarjetas EMV" o "tarjetas de crédito EMV", estas tarjetas usan un chip inteligente en lugar de una banda magnética para alojar los datos requeridos para procesar una transacción.

TECNOLOGÍA NFC: Significa *Near Field Communication*, se trata de una tecnología inalámbrica que funciona en la banda de los 13.56 MHz y que deriva de las etiquetas RFID. Es una evolución de la tecnología *contactless* que no solo sirve para realizar pagos sino también intercambiar todo tipo de información. NFC es una plataforma abierta pensada desde el inicio para teléfonos y dispositivos móviles. Su tasa de transferencia puede alcanzar los 424 kbit/s por lo que su enfoque más que para la transmisión de grandes cantidades de datos es para comunicación instantánea, es decir, identificación y validación de equipos/personas.

TOKEN: Un token es un conjunto de datos que actúa en representación de otros más valiosos, para protegerlos y evitar vulnerabilidades. Se trata de un elemento sin valor por sí mismo, que actúa en representación, en cambio, de información valiosa.

VULNERABILIDAD: En términos de informática, es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.

WHALING: Método de ataque phishing de avanzada. Los piratas informáticos lo utilizan para hacerse pasar por ejecutivos de alto nivel dentro de una organización. El rol más común que asumen es el de ejecutivos nivel C como un Director de Contabilidad o un Director Ejecutivo. Este tipo de ataque también es conocido como fraude CEO, ya que el *Whaling* se vale de técnicas de suplantación de identidad de sitios web y direcciones de correo electrónico para engañar a sus objetivos y hacer que revelen información confidencial de la empresa o hacerles transferir dinero a una cuenta.

RESUMEN

El análisis de los aspectos relevantes a la ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia ante la amenaza de suplantación de la identidad, delito informático de mayor ocurrencia en las transacciones digitales bancarias en el país, es un trabajo de grado en modalidad de monografía que presenta el estado de las características o rasgos importantes a dicha gestión en operaciones bancarias virtuales disponibles a usuarios a través de teléfonos inteligentes e internet. El trabajo se realiza mediante una revisión sistemática de literatura dentro de los diferentes entornos jurídicos, de gobernanza y tecnológico en tiempos de incremento del uso intensivo de medios electrónicos y redes sociales, y en particular en presencia del aumento de servicios ofrecidos por el sector bancario.

El enfoque del presente trabajo revisa de manera novedosa la información presentada por los bancos en las secciones de seguridad de sus sitios web, relacionada con las amenazas, riesgos y vulnerabilidades de la identidad digital por ellos identificados, igualmente revisa y analiza las características de ciberseguridad, particularmente los mecanismos de cara al usuario como factores de autenticación de la identidad digital dentro del contexto de transacciones electrónicas con la banca. De la misma manera, se revisan y analizan las finalidades o usos de los datos de los usuarios de los servicios bancarios, declaradas por los mismos en sus políticas de tratamiento de datos, sobre el entendido que del adecuado manejo que se realice de la información personal suministrada o recaudada por los bancos, se pueden derivar implicaciones relacionadas con aspectos de gran importancia para una sociedad, como son la protección de la privacidad, la confianza entre los actores de transacciones bancarias, los costos económicos asociados al fraude por suplantación de persona y la inclusión ciudadana en favor de la población tradicionalmente excluida.

Palabras claves: Identidad digital, gestión de la identidad digital, suplantación de identidad, protección de datos.

ABSTRACT

The analysis of the relevant aspects of cybersecurity of digital identity in electronic banking transactions in Colombia in the face of the threat of identity theft, a computer crime of greater occurrence in digital banking transactions in the country, is a degree work in the form of monograph that presents the status of the characteristics or important features to such management in virtual banking operations available to users through smartphones and the Internet. This work is carried out through a systematic literature review within the different legal, governance and technological environments in times of increasing intensive use of electronic media and social networks, and in particular in the presence of increasing services offered by the banking sector.

The focus of this paper reviews in a novel way the information presented by banks in the security sections of their websites, related to the threats, risks and vulnerabilities of digital identity, identified by them, also reviews and analyzes the characteristics of cybersecurity, particularly the user-facing mechanisms as factors of authentication of digital identity, within the context of electronic transactions with the bank. Likewise, it reviews and analyzes the purposes or uses of the data of the users of banking services, declared by the same in their data processing policies, on the understanding that the proper management of personal information provided or collected by banks, may have implications related to aspects of great importance for a society, such as privacy protection, trust between the actors of banking transactions, the economic costs associated with fraud by impersonation and citizen inclusion in favor of the traditionally excluded population.

Keywords: Digital identity, digital identity management, impersonation, data protection.

INTRODUCCIÓN

La ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia está contextualizada en el momento histórico en el que la sociedad concibe los servicios bancarios como un servicio público, más que como una mera actividad económica de un sector productivo de la misma. Este enfoque implica una cobertura casi universal e incluye, en términos prácticos, la necesidad de disponer a los usuarios de estos servicios los recursos y los mecanismos jurídicos y tecnológicos idóneos que protejan la privacidad de los datos personales y eviten la suplantación de la identidad de los usuarios y con ello se minimicen las consecuencias personales y económicas.

En efecto, la universalidad del acceso a los servicios bancarios se extiende en la medida que evoluciona el enfoque social – económico de los estados a sociedades más incluyentes e igualmente, al ritmo constante de la evolución tecnológica del relacionamiento banco – cliente en acelerado ascenso en este principio de siglo, caracterizado por una exacerbada necesidad de conectividad y movilidad. Sin embargo, es un hecho demostrado ya, que la pandemia del Covid19 incrementó disruptivamente la necesidad de la virtualidad en casi todos los aspectos de la vida de los ciudadanos del planeta, y con ello el incremento de la interacción no presencial con la banca y el incremento de la amenaza de fraude a la identidad digital.

En este contexto y, por medio de una revisión sistemática de literatura se analizan las características de ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia, se identifican sus amenazas, riesgos y vulnerabilidades, se examinan los mecanismos y factores de ciberseguridad adoptadas por el ente regulador y la banca colombianos para la autenticación de la identidad digital de los usuarios y se presentan recomendaciones para la prevención de amenazas de suplantación de la personas.

En este orden de ideas, el contenido del documento ilustra elementos de la ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia, escenario de interés general, que son pertinentes a la seguridad informática de las infraestructuras y de las redes.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Es un hecho que la pandemia del COVID 19, reportada como tal en informe de la Organización Mundial de la Salud[1] del 11 de marzo de 2.020, el mundo cambió para siempre y, es que, a raíz de la aparición de esta infección, la virtualidad abarcó casi todos los aspectos de la vida de los ciudadanos del planeta, se debió intensificar el uso de las tecnologías de información en algunos casos de manera intempestiva y, en otros como un proceso alternativo a la presencialidad. Es así como para el año 2.020, periodo de mayor confinamiento, modalidades virtuales como el teletrabajo, el e-learning y el uso de redes sociales en general, presentaron un aumento de uso considerable, hecho citado por Bancolombia en relación con el uso de redes sociales en pandemia[2] en el cual informa como el "Informe Digital 2021" elaborado por "*Hootsuite*" y "*We are social*" expone como a enero de 2.021 4.660 millones de personas, casi un 60% de la población mundial, se constituían en usuarios de Internet, lo que supone un incremento de un 7,3% más respecto al mismo periodo en 2.020. Adicionalmente, el mencionado reporte anuncia para el mismo periodo 4.200 millones de usuarios de redes sociales, lo que representó un crecimiento interanual de más del 13% (490 millones de usuarios nuevos), y 5.220 millones de líneas móviles que representaron un crecimiento de 1,8%.

En Colombia, particularmente la pandemia afectó positivamente la bancarización e inclusión financiera a poblaciones tradicionalmente excluidas del uso de tecnologías de información. Es así como Portafolio,[3] prensa colombiana especializada, informa como durante los primeros nueve meses de 2.020 se duplicó el ingreso de personas al sistema financiero en relación con lo presentado durante todo el año 2.019. E igualmente en la pandemia se estableció en el imaginario de la ciudadanía la posibilidad de enviar/ recibir dinero masivamente a través de las llamadas billeteras digitales y como a través de estos mecanismos el gobierno nacional y los gobiernos locales pudieron distribuir subsidios económicos, hecho sin precedentes en el país. Es así como Daviplata, el banco nativo digital de Davivienda sumó 5,5 millones de clientes nuevos y alcanzando un total de 11,6 millones.

De otro lado, en abril de 2.021 en relación con los delitos informáticos los portales especializados citan como La Dirección de Investigación Criminal e INTERPOL o

[1] OMS, COVID-19: cronología de la actuación de la OMS, [En línea], 2020, Disponible en: https://www.who.int/es/news/item/27-04-2020-who-timeline---covid-19

[2] BANCOLOMBIA. Uso de redes sociales en pandemia: la transformación hacia lo digital. 2021. [En línea]. Disponible en https://www.bancolombia.com/wps/portal/negocios/actualizate/tendencias/uso-redes-sociales-pandemia-transformacion-digital

[3] PORTAFOLIO, Bancarización e inclusión, lo bueno que deja la pandemia, [En línea], 2021, Disponible en: https://www.portafolio.co/economia/finanzas/bancarizacion-e-inclusion-lo-bueno-que-deja-la-pandemia-549749

(DIJIN) de Colombia identificó el delito de suplantación de identidad como el de mayor aumento en Colombia para el año 2.020, presentando un crecimiento de 409% debido a la pandemia, el reporte revela que mientras en 2.019 hubo alrededor de 300 casos reportados de este tipo en 2.020 la cifra se disparó a 1.527 reportes.[4]

Finalmente, es necesario tener en cuenta que Colombia, como casi todos los países reconoce la titularidad de los datos personales y la existencia de derechos asociados a estos. Los derechos asociados también se vinculan a actividades de tratamiento de datos, entendiendo por tratamiento de datos "cualquier operación o conjunto de operaciones efectuadas sobre datos personales mediante procedimientos manuales o automatizados relacionados con la obtención, uso, organización, conservación, utilización, comunicación, difusión, almacenamiento o cualquier forma de habilitación de acceso, cotejo, interconexión o transferencia"[5].

1.2. FORMULACIÓN DEL PROBLEMA

¿Cuáles son las características de ciberseguridad que debe tener la identidad digital en las transacciones electrónicas bancarias en Colombia y las recomendaciones de seguridad a los usuarios de servicios digitales financieros para la prevención de amenazas de suplantación?

[4] ASUNTOS LEGALES. Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. 2021. [En línea]. Disponible en https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651
ASUNTOS LEGALES, Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia, [En línea], 2021, Disponible en: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651

[5] BANCO INTERAMERICANO DE DESARROLLO. Regulación de blockchain e identidad digital en América Latina | El futuro de la identidad digital. [sitio web]. Washington. [Consultado: 10 diciembre de 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Regulacion-de-blockchain-e-identidad-digital-en-America-Latina-El-futuro-de-la-identidad-digital.pdf.p.22

2. JUSTIFICACIÓN

La identidad de una persona en el ámbito humanitario se considera un derecho que se determina en términos de algunos atributos particulares y que implica la necesidad imperante de su protección. En el contexto digital, el de las redes sociales y la virtualidad, se entiende como el conjunto, no único, de datos gestionables, que se utilizan para interactuar y participar en relacionamientos en ambientes tecnológicos digitales que requieren, por supuesto su idónea administración.

Y es que, justamente la multiplicidad de elementos dinámicos, objetivos o subjetivos que pueden constituir la identidad digital de una persona en infinidad de contextos virtuales, aporta a la gestión de la identidad una gran complejidad si se pretende garantizar primordialmente la privacidad y la protección de los datos personales y evitar daños que atenten contra la veracidad de las transacciones y la confianza de las relaciones humanas.

Una de las principales amenazas contra la identidad digital es su suplantación o su apropiación indebida, delito que puede causar todo tipo de daños y pérdidas a cualquier ciudadano, siendo los más frecuentes por tener gran cobertura en toda la sociedad, los relacionados al uso de los servicios y transacciones electrónicas bancarias a través de internet y teléfonos inteligentes ofrecidos por las entidades financieras para satisfacer las necesidades de las personas en relación con la circulación del dinero.

Dentro de este contexto, es importante revisar y ordenar integralmente como aborda el sector bancario de Colombia la gestión de la identidad digital y los retos actuales que pudieran dar mayor confianza en operaciones virtuales.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Analizar las características de ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia, por medio de una revisión sistemática de literatura, conducente a la generación de recomendaciones de seguridad a los usuarios de servicios digitales financieros para la prevención de amenazas de suplantación.

3.2. OBJETIVOS ESPECÍFICOS

- Examinar por medio de una revisión sistemática de literatura las amenazas, riesgos y vulnerabilidades que presenta la identidad digital en las transacciones electrónicas bancarias.

- Recopilar información relacionada con las características de ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia.

- Establecer recomendaciones de seguridad para los usuarios de servicios digitales financieros, enfocadas a la prevención de las amenazas de suplantación en las transacciones electrónicas bancarias.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Todo inicio de actividad presencial entre humanos conlleva implícitamente a cada participante la gestión de la identidad de sí mismo y la gestión de la identidad del otro. Identificarse, en la mayoría de los relacionamientos humanos, suele realizarse de manera espontánea y hasta inconsciente en donde las formas y la etiqueta de cada cultura gobiernan la acción, y es en ambientes corporativos, profesionales, laborales, o de relaciones internacionales, en que el acto de identificarse obedece a estrictos protocolos entre las personas y/o entidades que quieren o deben relacionarse en la ejecución de las actividades.

De igual forma, en el entorno digital identificarse y administrar o gestionar la identidad con el fin de iniciar o mantener relaciones entre los humanos y/o entidades, obedece a estándares y protocolos que aseguran uniformidad de los desarrollos y soluciones tecnológicas y que, éstos dentro de los marcos regulatorios y normas establecidas por las sociedades, facilitan la veracidad de las transacciones digitales y fortalecen la confianza de los participantes.

Dentro de los estándares y recomendaciones técnicas más importantes que proponen modelos para la gestión de la identidad digital se encuentra pertinente mencionar los siguientes:

4.1.1. Serie ISO/IEC 24760

De la Serie ISO/IEC 24760 los estándares que establecen marcos de trabajo y requerimientos para la gestión de la identidad son los siguientes:

ISO/IEC 24760-1:2019 - *IT Security and Privacy — A framework for identity management* es el conjunto de documentos de la *International Organization for Standardization* y de la *International Electrotechnical Commission*[6]*:* Establece definiciones y requerimientos para formular, como su nombre lo indica, un marco de trabajo para la gestión de identidad que le permite a los interesados garantizar sus servicios y productos. Parte 1 - Terminología y conceptos, este apartado define los términos y especifica los conceptos básicos para la gestión de identidades.

ISO/IEC 24760-2:2015(en) - *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and*

[6] ISO/IEC 24760-1:2019(en) IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts, [En línea], Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en

requirements.[7] Esta parte del estándar suministra una guía para la implementación de sistemas de gestión de la información de identidad, y especifica los requisitos para la implementación y operación de un marco para la gestión de identidades

ISO/IEC 24760-3:2016(en) *Information technology — Security techniques — A framework for identity management — Part 3: Practice* [8], este estándar proporciona directrices para asegurar que un sistema de gestión de identidad es concordante o cumple con lo establecido en la ISO/IEC 24760-1 e ISO/IEC 24760-2. Esta parte es aplicable a un sistema de gestión de identidad donde los identificadores o información relacionada con las entidades se adquiere, procesa, almacena, transfiere o utiliza con el fin de identificar o autenticar a las mismas y/o con el fin de tomar decisiones.

4.1.2. Reglamento 910/2014 (eIDAS)

El reglamento (Unión Europea) No. 910/2014 eIDAS (*electronic IDentification, Authentication and trust Services)* del Parlamento Europeo y del Consejo[9] establece lo relacionado con la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior europeo, teniendo como propósitos particulares, entre otros reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones seguras entre los ciudadanos, y garantizar que sean posibles la identificación y la autenticación confiables para el acceso a los servicios transfronterizos en línea ofrecidos por los estados miembros.

El reglamento presenta en el capítulo I, entre otros, las definiciones y términos que conforman su base conceptual, en el capítulo II las disposiciones relacionadas con la identificación electrónica siendo relevante los niveles de seguridad de los sistemas de identificación electrónica y, en el capítulo III lo correspondiente a los servicios de confianza, en particular la responsabilidad y carga de la prueba y la autenticación de sitios web.

[7] ISO, ISO/IEC 24760-2:2015(en) Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements, [En línea], Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-2:ed-1:v1:en

[8] ISO, ISO/IEC 24760-3:2016(en) Information technology — Security techniques — A framework for identity management — Part 3: Practice, [En línea], Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-3:ed-1:v1:en

[9] GOBIERNO DE ESPAÑA, AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO. REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. [sitio web]. Madrid. [Consultado: 6 de febrero de 2022]. Disponible en: https://www.boe.es/doue/2014/257/L00073-00114.pdf

4.1.3. La serie documental SP 800-63-3 (NIST)

El paquete SP 800-63-3 NIST *(National Institute of Standards and Technology)*, por sus siglas en inglés,[10] es el conjunto de pautas o recomendaciones y requisitos técnicos para las agencias federales de Los Estados Unidos que implementan servicios de identidad digital. Las recomendaciones implican la demostración de la identidad y la autenticación de los usuarios que interactúan con los sistemas de TI del gobierno a través de redes abiertas. Igualmente, estas pautas establecen los requisitos técnicos en cada una de las áreas como serían la de demostración de identidad, registro, autenticadores, procesos de gestión, protocolos de autenticación, federación y las confirmaciones relacionadas.

Este conjunto de pautas están compiladas en cuatro grandes temas: identidad digital, inscripción y demostración de identidad, autenticación y gestión del ciclo de vida, Federación y afirmaciones.

4.1.4. Recomendación UIT-T Series X

Las recomendaciones para la gestión de la identidad digital de la UIT (sigla en inglés) Unión Internacional de Telecomunicaciones, organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación – TIC, se destacan las siguientes:

La recomendación ITU X.1251 Marco para el control por el usuario de la identidad digital[11] provee una serie de guías para asegurar el control y el intercambio de información relacionada con la identidad digital por parte del usuario, lo que implica tener la capacidad de controlar también la divulgación de esta información.

La recomendación ITU X.1253 Directrices de seguridad para los sistemas de gestión de la identidad[12] establece indicaciones de seguridad en relación a cómo deben instalarse y utilizarse mecanismos de seguridad en los sistemas de gestión de identidad (IdM,), estas indicaciones se establecen para contextos de interoperabilidad de los mismos sistemas de gestión de identidad en el ciberespacio.

Finalmente, la recomendación ITU X.1254: Marco de garantía de autenticación de entidad [13] determina tres niveles para garantizar la autenticación de una entidad y

[10] NIST, Digital Identity Guidelines, [En línea], Disponible en: https://pages.nist.gov/800-63-3/
[11] ITU, X.1251: Marco para el control por el usuario de la identidad digital, [En línea], Disponible en: https://www.itu.int/rec/T-REC-X.1251/es
[12] ITU, X.1253: Directrices de seguridad para los sistemas de gestión de identidades, [En línea], Disponible en: https://www.itu.int/rec/T-REC-X.1253-201109-I/es
[13] ITU, X.1254: Marco de garantía de autenticación de entidad, [En línea], Disponible en: https://www.itu.int/rec/T-REC-X.1254/es

define sus correspondientes *frameworks*, criterios y amenazas, y consecuentemente la tecnología de control apropiado.

4.2. MARCO CONCEPTUAL

4.2.1. Identidad de una persona

Semánticamente, la Real Academia Española da a la identidad varias acepciones, entre éstas, se considera pertinente mencionar que la identidad, de manera genérica es el "conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás", también y, con un enfoque más humano, la identidad vendría a ser la "conciencia que una persona o colectividad tiene de ser ella misma y distinta a las demás" y existencialmente, podría señalarse como el "hecho de ser alguien o algo".[14]

En contextos de la actividad humana en los actuales tiempos de entornos presenciales y virtuales, resulta oportuno tener en cuenta la definición dada por el *World Economic Forum* para la identidad como "el producto de la consolidación de diferentes aristas objetivas y subjetivas que permiten individualizar a un referente biológico como sujeto en la sociedad"[15] y cuyos atributos clasifica como inherentes o de la personalidad, atributos acumulados y atributos asignados.

4.2.2. Identidad digital e identidad digital auto soberana

En el contexto digital existen varias definiciones o aproximaciones según el organismo o comunidad que aborde el problema de la identificación digital, a continuación, las definiciones que se consideran relevantes a este enfoque:

La ISO / IEC 24760-1 define la identidad como el "Conjunto de atributos relacionados con una Entidad. Una Entidad puede tener más de una identidad. Muchas entidades pueden tener la misma Identidad".[16]

El Instituto Nacional de Estándares y Tecnología – NIST (NIST-IDG, 2017) señala que "La identidad digital es la representación única de un sujeto involucrado en una transacción en línea. Una identidad digital siempre es única en el contexto de un servicio digital, pero no necesariamente identifica de manera única al sujeto en

---

[14] REAL ACADEMIA ESPAÑOLA, Diccionario de la lengua española, [En línea], Disponible en: https://dle.rae.es/identidad

[15] BANCO INTERAMERICANO DE DESARROLLO, Op.cit.,p.16

[16] CUNO, Álvaro. SAAVEDRA, Ricardo. Modelos de Gestión de la Identidad Digital. En: RESEARCHGATE [online], enero 2016 [citado 1 enero 2016]. Disponible en: https://www.researchgate.net/publication/329733403_Modelos_de_Gestion_de_la_Identidad_Digital. ISSN 2313-3465.p. 24.

todos los contextos. En otras palabras, acceder a un servicio digital no significa que se conozca la identidad de la vida real del sujeto". [17]

Igualmente, el *Open Identity Exchange* (OIX) – OIX (OIX-TOOLS, 2019) señala como "La identidad digital es la suma de toda la información disponible digitalmente con respecto a un individuo, independientemente de su grado de validez, su forma o su accesibilidad, que comprende datos directos e inferidos (o indirectos)"[18]

El concepto de identidad digital auto soberana implica, como su nombre lo indica un entorno virtual de relacionamientos digitales, como definición es pertinente la presentada por el Banco Interamericano de Desarrollo(BID) en el artículo "El futuro de la identidad digital" donde señala a la identidad autogestionada (auto soberana) como el " término utilizado para describir el movimiento digital que reconoce que un individuo debe poseer y controlar su identidad sin la intervención de las autoridades administrativas".[19]

En un sentido práctico, el concepto de identidad digital soberana podría asimilarse a la noción de identidad descentralizada que, compañías como Okta,[20] actor tecnológico de relevancia en la gestión del acceso, define como aquella identidad digital en donde el usuario recibe credenciales de varios emisores (por ejemplo, gobierno, educación, empleador) y las almacena en una billetera digital. El usuario presenta esas credenciales a la autoridad emisora pertinente, quien luego verifica su identidad a través de un libro mayor basado en *blockchain* que no almacena los datos del usuario.

4.2.3. Gestión de la identidad digital y su ciclo de vida

La identidad como unidad en un contexto digital determinado debe ser administrada, lo que implica funciones y capacidades de la organización o de la entidad responsable para garantizar el adecuado tratamiento durante todo el ciclo de vida de la información correspondiente. La ISO/IEC 24760-1:2019[21] establece como gestión de la identidad (*identity management IdM*) los procesos y políticas involucradas en el manejo del ciclo de vida de los atributos (valor, tipo, etc.) de las identidades conocidas para un dominio particular.

La base de la gestión de la identidad digital es la naturaleza cambiante de la información que la constituye y la dinámica de las relaciones entre las diferentes entidades actuantes. En el documento "Identidad Digital: El nuevo usuario en el

[17] BANCO INTERAMERICANO DE DESARROLLO, Op.cit., p.12
[18] Ibid.
[19] Ibid., p. 27
[20] OKTA, What is Decentralized Identity?, [En línea], 2021, Disponible en: https://www.okta.com/blog/2021/01/what-is-decentralized-identity/
[21] ISO,Op.cit.

mundo digital" de propiedad de la Fundación Telefónica[22] se mencionan como fases del ciclo de vida de la identidad digital, etapas que incluyen la provisión o enrolamiento inicial pasando por su propagación, uso, mantenimiento y teniendo en cuenta finalmente, su eliminación, cuando fuere del caso.

4.2.4. Dato personal y protección de datos

En Colombia el concepto de datos personales se encuentra señalado en la Ley 1581 de octubre de 2012 o Ley Colombiana de Protección de Datos Personales, artículo 3, donde se define el dato personal como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"[23] y sobre los cuales se reconoce el derecho que tienen las mismas personas de conocer, actualizar y rectificar.

4.2.5. Transacción electrónica bancaria

La transacción electrónica bancaria hace relación, como cita "La Revista Contribuciones a la Economía (enero-marzo 2016)", [24] al uso por parte de un usuario o consumidor financiero, de herramientas que la banca pone a su disposición con el fin de facilitar operaciones cotidianas desde una computadora o dispositivo en línea, que cuenta con acceso a internet en uso de una plataforma segura y con alta tecnología. En este contexto, las transacciones electrónicas bancarias obedecerían a las típicas transacciones relacionadas con verificación de saldos y de estados de cuenta, pago de servicios públicos y privados, pago de impuestos, pagos de obligaciones financieras, inversiones en línea, transferencias, depósitos a nómina.

4.3. ANTECEDENTES

La seguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia se circunscribe dentro del entorno bancario de Latinoamérica, región que según el informe de 2018 de la OEA - "Estado de la Ciberseguridad en el Sector

[22] ESPAÑA DIGITAL. IDENTIDAD DIGITAL: EL NUEVO USUARIO EN EL MUNDO DIGITAL. [sitio web]. Madrid. [Consultado: 10 diciembre de 2021]. Disponible en: .https://publiadmin.fundaciontelefonica.com/media/es/que_hacemos/media/publicaciones/identidad_digital.pdf?.p.39-40

[23] GOBIERNO DE COLOMBIA, FUNCIÓN PUBLICA. Ley 1581 de 2012. [sitio web]. Bogotá. [Consultado: 10 diciembre de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=La%20presente%20ley%20tiene%20por,el%20art%C3%ADculo%2015%20de%20la

[24] SURIAGA SANCHEZ, Marco Antonio BONILLA FREIRE, Janet SANCHEZ PARRALES, Luis Alberto. Banca electrónica. [En línea]. En: CE Revista Contribuciones a la Economía, enero-marzo de 2016. [Consultado: 6 de febrero de 2022]. Disponible en: http://eumed.net/ce/2016/1/banca.html.ISSN: 1696-8360

Bancario en América Latina y el Caribe"[25] presentó, en un análisis realizado a 191 bancos de los diferentes países miembro, el *malware* y el *phishing* como los dos principales eventos de seguridad de mayor ocurrencia contra sus servicios al igual que los dos eventos de ocurrencia diaria contra sus usuarios.

En efecto, en la extensión del mencionado informe para Colombia se señala a la ciberseguridad como una de las principales preocupaciones del sector bancario en Latinoamérica, sin embargo y de manera paradójica el informe presenta mediciones que llaman la atención sobre la real preparación de las entidades bancarias ante las amenazas cibernéticas:

- El 70% de las organizaciones no han desarrollado un plan de respuesta a incidentes cibernéticos.
- El 46% de las organizaciones no han implementado o mejorado su capacitación sobre concienciación de la suplantación de identidad (*phishing)* para empleados en los últimos 12 a 24 meses.
- El 43% de las organizaciones carecían de responsabilidad a nivel de la junta directiva para la revisión y gestión del riesgo cibernético.
- El 37% de las organizaciones aún no han estimado el impacto financiero de un ataque cibernético.
- El 34% de las organizaciones no evalúa a sus proveedores o clientes en riesgo cibernético.[26]

Ahora bien, los incidentes cibernéticos más reportados en Colombia son el *phishing* con un 42%, la suplantación de identidad 28%, el envío de *malware* 14% y los fraudes en medios de pago en línea con 16%, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca, cifras que se enmarcan dentro del 90% de los ciberataques que sufren las empresas en este país con causa directa en la ingeniería social.

Finalmente, es conveniente señalar que el costo económico de los delitos o del fraude en canales digitales que tienen que ver con la identidad digital, según informe de Asobancaria[27] tuvo un incremento del 10,7% pasando de $0,26 por cada

---

[25] ORGANIZACIÓN DE ESTADOS AMERICANOS. Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. [sitio web]. Washington. [Consultado: 10 diciembre de 2021]. Disponible en: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf.p. 8

[26] CSIRT FINANCIERO. Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. [sitio web]. Bogotá. [Consultado: 6 de febrero de 2022]. Disponible en: https://csirtasobancaria.com/sala-de-prensa/201cdesafios-del-riesgo-cibernetico-en-el-sector-financiero-para-colombia-y-america-latina201d-publicacion-conjunta-entre-asobancaria-y-la-organizacion-de-estados-americanos-oea.p.43

[27] ASOBANCARIA. Impacto económico y social del phishing y el smishing en Colombia y el mundo. [sitio web]. Bogotá. [Consultado: 6 de febrero de 2022]. Disponible en: https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf. p.8

$10 mil transados en el período enero a agosto de 2019 a $0,29 pesos en el mismo periodo de 2020. En este sentido, *el phishing* representa el 74,2% de las reclamaciones por posible fraude y constituye la principal amenaza de seguridad para los usuarios del sistema financiero que realizan transacciones.

4.4. MARCO TECNOLÓGICO

4.4.1. Sistema de administración de la identidad digital

Un sistema de administración de accesos e identidad digital es aquel que implementa el actuar de agentes, usuarios, proveedores de identidad, receptores de información y entidades de control, que operan relacionadamente bajo reglas y estándares definidos con el fin de cumplir, entre otros, las siguientes funcionalidades:

- Identificar o reconocer y acreditar entidades en un dominio particular como distinta de otras entidades.

- Autenticar la identidad del agente mediante un procedimiento formal de verificación, que se realiza generalmente cuando se ingresa al sistema o a la red, y/o accede a una base de datos. La autenticación, como lo menciona el portal especializado RZ Redes Zones[28] puede realizarse de maneras diversas y, según el nivel de implementación del sistema de gestión de la identidad se acude a verificar, como principio, que el actor o agente responda de manera correcta información o data que se supone debe saber, que pueda presentar algún elemento que, de manera única, está en su posesión y complementariamente, que demuestre alguna característica (s) propia que permita determinar quién es y por lo que se considera un agente único.

- Autorizar el acceso a los recursos organizados en niveles de autorización que, como indica el Observatorio Tecnológico del Ministerio de Educación Cultura y Deporte de España,[29] es el procedimiento por el cual el sistema determina qué, cómo y cuándo, un agente o usuario autenticado puede utilizar los recursos de la organización.

Los sistemas de gestión de accesos de identidad deben incluir la funcionalidad o la existencia de un “proveedor de identidad” como lo recomienda la norma ISO/IEC 24760-1, correspondiendo este proveedor a “una entidad que proporciona

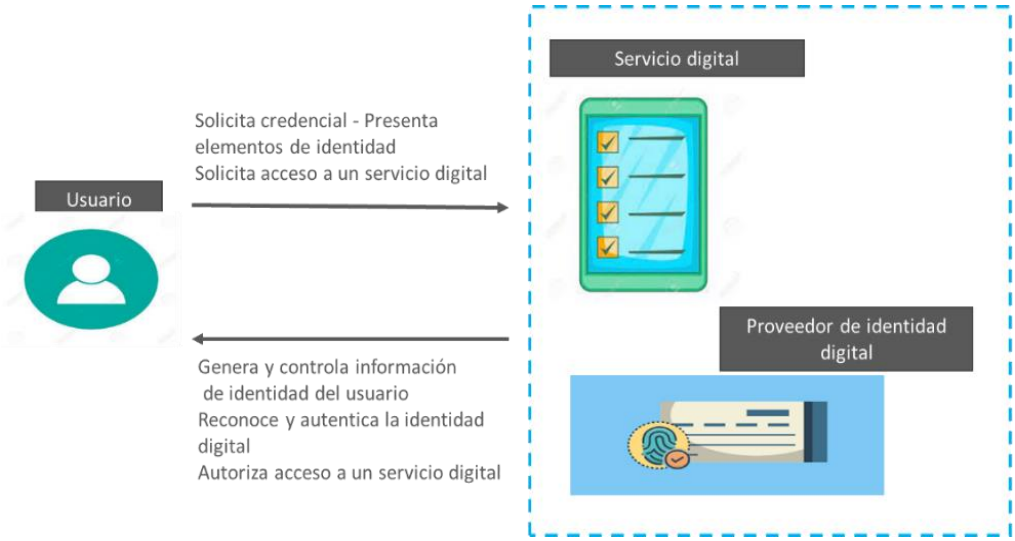
[28] RZ, Qué significa autenticación y la autorización, [En línea], 2021, Disponible en: https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/

[29] GOBIERNO DE ESPAÑA, MINISTERIO DE EDUCACIÓN CULTURA Y DEPORTE, Introducción a la seguridad informática - Mecanismos básicos de seguridad, [En línea], 2012, Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=2

información sobre identidad", es decir el elemento o subsistema que administra y mantiene la información de identidad, gestiona las credenciales en nombre de personas físicas o jurídicas y ofrece los servicios de autenticación del usuario propietario de la identidad a las aplicaciones de otros servicios digitales[30]. Es así como, dependiendo de la topología o la forma como se estructuran los elementos del sistema de administración de identidades y accesos, en particular del lugar donde se ubica la función del "proveedor de identidad" y su relación con el prestador de servicios digitales, pueden diferenciarse modelos de gestión de identidad digital, que pueden concebirse, según la citada publicación[31], unos centralizados, otros en los que la identidad es provista por un tercero(s), algunos otros poniendo en el centro el usuario y los llamados modelos de identidad autogestionados.

Así pues, en la **Figura 1** se ilustra el modelo de gestión de identidad centralizado en el que los servicios digitales y los servicios relacionados con el proveedor de identidad son ofrecidos y administrados por el mismo actor.

Figura 1. Sistema de administración de la identidad digital - Modelo centralizado



Fuente: Propia adaptado de https://publications.iadb.org/publications/ spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf. p.17

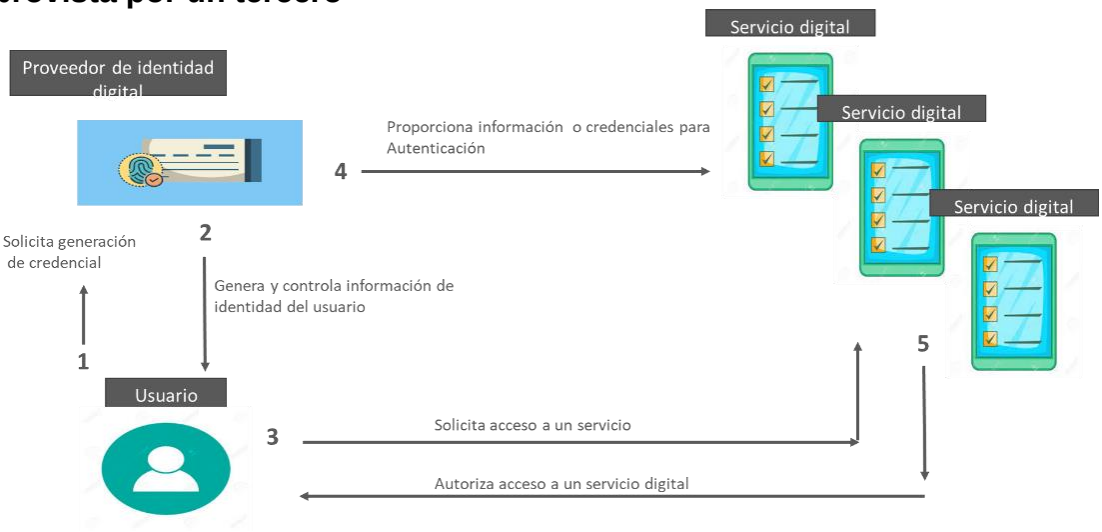
[30] INTER -AMERICAN DEVELOPMENT BANK. IDENTIDAD DIGITAL AUTO-GESTIONADA El futuro de la identidad digital: autogestión, billeteras digitales y blockchain. [sitio web].Washington. [Consultado: 10 diciembre de 2021].Disponible en: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf. p.16

[31] INTER -AMERICAN DEVELOPMENT BANK, Op.cit., p.17-22

De otro lado, en el modelo de gestión de identidad provista por un tercero, las funciones del proveedor de identidad son cumplidas por una entidad, o varias confederadas, diferentes a aquel actor o entidad que presta el servicio digital, existiendo una comunicación entre estos dos. Este modelo es muy usado actualmente por los servicios digitales que recurren a la autenticación que realizan Facebook o Google en lugar de hacerlo dentro de sus propios servicios.

La **Figura 2** ilustra el modelo de identidad provista por un tercero.

Figura 2. Sistema de administración de la identidad digital - Identidad provista por un tercero



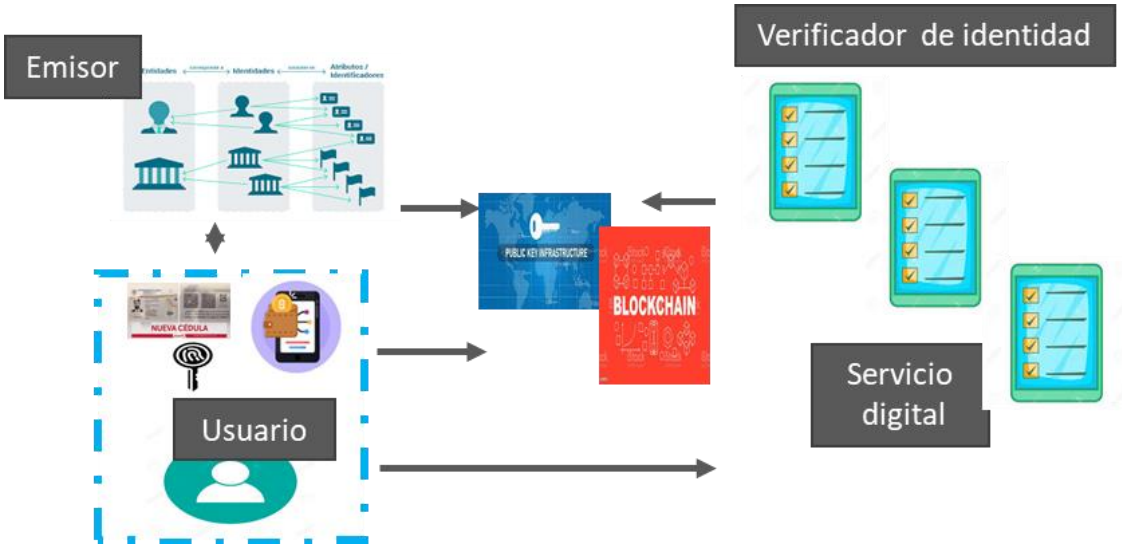
Fuente: Propia adaptado de https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf. p.19

Es relevante a esta forma de administración que el usuario solo deba identificarse ante el proveedor de identidad, quien lo autenticará para el resto de los servicios.

También, se encuentran los modelos de gestión de la identidad auto – gestionados o auto- soberanos o centrados en los usuarios. En estas topologías los usuarios son, precisamente, los encargados de administrar y en general custodiar sus propios datos personales y particularmente sus autenticadores y credenciales emitidas con las tecnologías apropiadas, como por ejemplo las suministradas por la Infraestructura de llave pública y con la tecnología de *Blockchain*, entre otros, que asegurarían la confiabilidad y certeza de identidad digital.

El modelo autogestionado se evidencia en la **Figura 3.**

Figura 3. Sistema de administración de la identidad digital auto - gestionada



Fuente: Propia adaptado de https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf. p.22

En la medida que este modelo implemente esquemas en los que el usuario sea más o menos autónomo para generar sus propios identificadores y determinar los elementos que lo identifican y/o las credenciales a presentar ante un prestador del servicio digital, podría configurarse sistemas más o menos autogestionados.

4.4.2. Componentes tecnológicos de un sistema de administración de accesos e identidades

Un esquema típico para un sistema de gestión de accesos e identidades implementa componentes mínimos que cohesionan la funcionalidad requerida. A continuación, los componentes presentados por *VMware End-User Computing* en su video *Identity and Access Management: Technical Overview:*

- Primeramente, se estructura un almacén o repositorio con la información de los usuarios basado, muy frecuentemente, en protocolos de amplia aceptación como Directorio Activo y LDAP.

- Seguidamente y en un ambiente corporativo, la gestión de identidades despliega la capacidad de *Single Sign On* (SSO) o acceso único a múltiples aplicaciones, sistemas y recursos a través de una única cuenta y contraseña.

- De otro lado, y en la medida que las organizaciones operen en ambientes de alta interacción con terceras partes, proveedores y aplicaciones en la nube, se crean esquemas federados de *Single Sign On* habilitados a través de estándares abiertos de interoperabilidad.

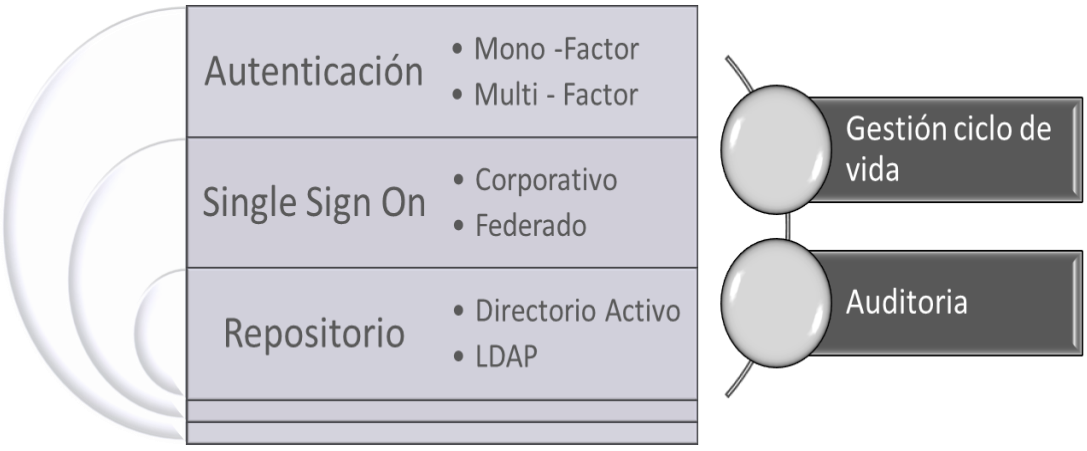
- De tal suerte que, una vez estructurados los componentes sobre los que reposa la información del usuario y los protocolos de interacción corporativa y externa, se suman medidas y mecanismos que deben garantizar la máxima certeza sobre la identidad del usuario. De la implementación de uno o más de los llamados factores de autenticación, se puede hablar o no de autenticación fuerte o autenticación multifactorial.

- Ahora bien, como la información de la identidad digital es dinámica, se hace necesario incorporar componentes funcionales que aprovisionen y den cuenta del ciclo de vida de los datos personales, identificadores y demás información de los usuarios de los servicios digitales. Corporativamente, es muy frecuente acometer el mencionado aprovisionamiento y gestión desde los sistemas de recursos humanos.

- Finalmente, el esquema podría implementar componentes que auditen y permitan hacer seguimiento a la actividad de toda la solución y, con todo esto asegurar el fin último de un sistema de administración de accesos e identidades, que la persona correcta está accediendo el recurso correcto en el momento correcto.

La **Figura 4** permite observar los componentes tecnológicos descritos para un sistema de administración de accesos e identidades.

Figura 4. Componentes tecnológicos de un sistema de administración de accesos e identidades



Fuente: Propia adaptado de Identity and Access Management: Technical Overview ttps://www.youtube.com/watch?v=Tcvsefz5DmA

4.4.3. Métodos de autenticación

Como se mencionó anteriormente, un sistema de administración de acceso e identidades tiene entre sus principales funciones la de autenticar la identidad del agente o usuario de servicios digitales mediante uno más procedimientos formales de verificación, que se activan en eventos específicos como al ingresar al sistema o la red, acceder una base de datos, o utilizar un servicio o aplicación.

En la práctica, estos procedimientos formales se materializan en esquemas de autenticación agrupados en factores, que dependen de los métodos utilizados para la verificación de elementos y/o características del usuario o actor a autenticar. En efecto, como se muestra en el documento de grado "Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor"[32]" los esquemas o factores de autenticación pueden categorizarse de acuerdo con características comunes, por ejemplo, aquellos factores que se agrupan dentro de la categoría de "conocimiento" son métodos de verificación soportados en información que el agente o usuario conoce de manera exclusiva. Igualmente, la categoría de factores denominada de "posesión", está constituida por los métodos de verificación que se basan en la tenencia de algún elemento particular, también de forma única. Finalmente, existen los factores categorizados y agrupados por el

[32] VELÁSQUEZ, Ignacio. Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor. [En línea]. Trabajo de grado. Chillan, Chile. Universidad del Bío-Bío Facultad de Ciencias Empresariales Departamento de Ciencias de la Computación y Tecnologías de la Información.2017.87 p. [Consultado 2 de julio de 2022]. Disponible en: http://mcc.ubiobio.cl/docs/tesis/ignacio_andr%C3%A9s_vel%C3%A1squez_lagos_-2017_velasquez_lagos_ignacio.pdf. p.20-21

concepto de “inherencia”, correspondiendo consecuentemente a métodos de verificación de algún atributo personalísimo del usuario o agente.

Así pues, puede decirse que la combinación usuario y contraseña es el mecanismo de autenticación por excelencia que pertenece a la categoría de factores agrupados al “conocimiento”, este mecanismo implica claves que, corrientemente pueden ser alfanuméricas o gráficas. Dentro del grupo de factores caracterizados por el conocimiento, son también muy utilizados los pines y las preguntas personales.

De otro lado, entre la categoría de factores de autenticación por tenencia o posesión de algún elemento se encuentran los métodos que se soportan en dispositivos, entre otros, los tokens por hardware, los teléfonos y las tabletas móviles, a través de los cuales se comunican las claves únicas y los OTPs. Igualmente, se encuentran las llaves que se proveen a través de tarjetas inteligentes o llaves de infraestructura pública PKI.

En relación con los factores utilizados con mayor frecuencia que tienen que ver con la categoría asociada a atributos inherentes al usuario, son ampliamente conocidos el reconocimiento de huellas dactilares, los mecanismos para reconocimiento soportados en biométricas del rostro y del iris. Igualmente, se incluyen características biométricas asociadas a reconocimiento de patrones, entre las más usadas se encuentran patrones de pulsación de teclas y el ritmo de la voz, entre otros.

De todas formas, hay procesos y servicios como las transacciones electrónicas bancarias, que requieren esquemas de “autenticación fuerte” o autenticación multifactorial (MFA) que deberían, al suministrar mayor seguridad que aquella basada en un solo factor; dificultar el fraude en dichas transacciones. Implementar un esquema de autenticación multifactorial requiere utilizar al menos dos métodos diferentes de al menos dos grupos o factores diferentes[33], lo que debe atenuar las vulnerabilidades asociadas a mecanismos de autenticación basados, únicamente en el conocimiento de contraseñas.

[33] ONESPAN. Autenticación fuerte. [En línea].2022. Disponible en: https://www.onespan.com/es/topics/autenticacion-fuerte#:~:text=%C2%BFQu%C3%A9%20es%20la%20autenticaci%C3%B3n%20fuerte,y%20la%20autorizaci%C3%B3n%20de%20transacciones.fuerte#:~:text=%C2%BFQu%C3%A9%20es%20la%20autenticaci%C3%B3n%20fuerte,y%20la%20autorizaci%C3%B3n%20de%20transacciones.

4.5. MARCO LEGAL

4.5.1. La identidad en Colombia

A nivel global, según la "Comisión Nacional de los Derechos Humanos de México,[34] el derecho a la identidad define a la persona humana y guarda un vínculo estrecho con el resto de los derechos humanos, particularmente con aquellos que tienen que ver con la imposibilidad de ser discriminado/a, con la salud, la intimidad, la vida digna, con la necesidad de poseer propias creencias religiosas, de pensamiento y de opinión. Sin embargo, la inclusión en 1989 del Artículo 8 de la "Convención sobre los Derechos del Niño"[35] hace el reconocimiento formal de la identidad como un derecho, señalando para los estados parte el compromiso de preservar en los niños su identidad, incluidos la nacionalidad, el nombre y las relaciones familiares de conformidad con la ley sin injerencias ilícitas.

En Colombia, el derecho a la identidad de los niños está contenida en el Artículo 25 de la Ley 1098 de 2006 con la que se expidió el Código de la Infancia y la Adolescencia[36], en el cual se establece que los niños, las niñas y los adolescentes tienen derecho a tener una identidad y a conservar los elementos que la constituyen como el nombre, la nacionalidad y filiación conformes a la ley. Para estos efectos deberán ser inscritos inmediatamente después de su nacimiento, en el registro del estado civil (…)

Sin embargo, una definición formal de identidad y/o identidad digital de una persona en Colombia no es expresa, al respecto de la identificación el inciso tercero del artículo 266 de la Constitución Política establece que el Registrador Nacional del Estado Civil "Ejercerá las funciones que establezca la ley, incluida la dirección y organización de las elecciones, el registro civil y la identificación de las personas,..."[37], que se complementa con la disposición vigente del Artículo 1 de la Ley 39 de 1961, que señala, entre otros que "… solo a través de la cédula de

---

[34] " CNDH MÉXICO. El derecho a la identidad de las personas y los pueblos indígenas. [En línea].2018. Disponible en: https://www.cndh.org.mx/documento/el-derecho-la-identidad-de-las-personas-y-los-pueblos-indigenas#:~:text=El%20derecho%20a%20la%20identidad%20de%20la%20persona%20y%20su,digna%20y%20a%20tener%20sus%20propias

[35] UNICEF COMITÉ ESPAÑOL. CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO. [sitio web]. Madrid. [Consultado: 3 de julio de 2022]. Disponible en: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf.https://www.un.org/es/events/childrenday/pdf/derechos.pdf.p.12

[36] CONGRESO DE LA REPÚBLICA DE COLOMBIA. LEY 1098 DE 2006, Por la cual se expide el Código de la Infancia y la Adolescencia. [En línea].2006. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1098_2006.htm#25

[37] CONSTITUCIÓN POLÍTICA DE COLOMBIA. Artículo 266. [En línea].2015. Disponible en: https://www.constitucioncolombia.com/titulo-9/capitulo-2/articulo-266

ciudadanía laminada será posible identificarse en todos los actos civiles, políticos, administrativos y judiciales."[38]

4.5.2. Protección de datos personales en Colombia

Colombia desarrolla la protección de datos personales con la Ley No 1581 de 17 del octubre de 2012, tomando como marco constitucional lo establecido, principalmente en el Artículo 15 de la Carta Magna del país[39] que señala como derechos los que tienen todas las personas a su intimidad personal y familiar y a su buen nombre, señalando también al Estado el deber de respetarlos y hacerlos respetar. Igualmente, existe el derecho relacionado con conocer, actualizar y rectificar las informaciones que se hayan recogido sobre las personas en bancos de datos y en archivos de entidades públicas y privadas, estableciéndose también la necesidad del respeto por la libertad y demás garantías consagradas en la Constitución en lo que tenga que ver con la recolección, tratamiento y circulación de datos, entre otros.

En efecto, el desarrollo que hace la citada Ley[40] incluye en su Artículo 17, entre otros muchos aspectos, los deberes de los responsables del tratamiento de datos siendo particularmente relevantes las exigencias expresadas en los literales j, sobre el respeto de las condiciones de seguridad y privacidad de la información del titular o dueño de la información personal, y literal m) sobre el deber de informar al titular del uso dado a sus datos, uso que debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley.

4.5.3. Verificación de la identidad digital en transacciones electrónicas bancarias en Colombia

En Colombia los establecimientos bancarios se catalogan como entidades vigiladas por la Superintendencia Financiera, autoridad que establece las obligaciones y requerimientos que velan por su adecuado funcionamiento y la protección de los derechos de los consumidores financieros. Particularmente, para el caso de la verificación de la identidad digital de los citados consumidores como usuarios de las transacciones electrónicas bancarias dispuestas por los bancos, la Superintendencia Financiera de Colombia con la Circular Externa No. 29 de 2019

---

[38] CONGRESO DE LA REPÚBLICA DE COLOMBIA. LEY 39 DE 1961, Por la cual se dictan normas para la cedulación, y otras de carácter electoral. [En línea].2022. Disponible en: https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/ley_0039_1961.htm#:~:text=ART%C3%8DCULO%201o.,%2C%20pol%C3%ADticos%2C%20administrativos%20y%20judiciales./ley_0039_1961.htm#:~:text=ART%C3%8DCULO%201o.,%2C%20pol%C3%ADticos%2C%20administrativos%20y%20judiciales.

[39]CONSTITUCIÓN POLÍTICA DE COLOMBIA. Artículo 15. [En línea].2003. Disponible en: https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

[40] CONGRESO DE LA REPÚBLICA DE COLOMBIA. LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. [En línea].. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

“modifica la Circular Básica Jurídica en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones y acceso e información al consumidor financiero y uso de factores biométricos”.[41]

La Circular mencionada esgrime el fortalecimiento del uso de canales digitales para la prestación de servicios financieros en condiciones de seguridad y con apego a estándares internacionales en la materia. Específicamente, incluye como canales e instrumentos de prestación de servicios financieros los ofrecidos a través de internet, banca móvil y sistemas de audio respuesta, entre otros.

Igualmente, la citada Circular establece en su numeral 2.2.6 como mecanismos fuertes de autenticación los siguientes:

- Biometría en combinación con un segundo factor de autenticación para operaciones no presenciales.

- Certificados de firma digital de acuerdo con lo establecido en la Ley 527 de 1999 y sus decretos reglamentarios.

- OTP (*One Time Password*) en combinación con un segundo factor de autenticación.

- Tarjetas que cumplan el estándar EMV en combinación con un segundo factor de autenticación.

- Registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizarán las operaciones en combinación con un segundo factor de autenticación.

[41] SUPERINTENDENCIA FINANCIERA DE COLOMBA. Circulares Externas. [En línea].2015. Disponible en: https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/circulares-externas--10082461

5. DESARROLLO DE LOS OBJETIVOS

5.1. AMENAZAS, RIESGOS Y VULNERABILIDADES DE LA IDENTIDAD DIGITAL EN TRANSACCIONES ELECTRÓNICAS BANCARIAS

En el contexto digital de transacciones electrónicas bancarias, la identidad de las partes que se relacionan comercialmente - clientes y bancos- es un elemento esencial cuya gestión adquiere gran complejidad en razón, entre otros a los constantes cambios tecnológicos y a la evolución de los preceptos jurídicos relacionados con la privacidad, la protección de datos y la seguridad de la información, que son de imperativo cumplimiento en Colombia.

En relación con la evolución tecnológica, el relacionamiento cliente – banco no siempre obedece a una planeación de productos que satisfacen las necesidades de la sociedad, si no como en el caso de la pandemia del Covid19, puede suceder de manera intempestiva produciendo importantes cambios en dicho relacionamiento e, implícitamente propiciando nuevas formas con las que la delincuencia intenta aprovechar las vulnerabilidades de los actores para hacerse con sus activos, incluida la información personal que constituye la identidad.

En este sentido, el **Cuadro 1** presenta una relación cronológica de las modalidades delincuenciales que amenazan la identidad de las personas en concordancia con las tecnologías presentes en dicho momento del tiempo y los correspondientes servicios ofrecidos por el sector bancario.

Cuadro 1. Evolución de las amenazas contra la identidad en los servicios bancarios

Periodo	Amenaza contra la identidad	Tecnología	Servicios bancarios
Antes de los años 90s	Robo de documento de identificación, chequeras y libretas de ahorro.	Sistemas no interconectados. Identificación y autenticación presencial. Documentos físicos, Firma autógrafa Huella dactilar impresa.	Atención en oficina. Dinero en metálico o físico. Cobro de cheques.
90s - 2000	Robo de documento de identificación, chequeras y libretas de ahorro. Robo de tarjetas plásticas. Robo de contraseñas.	Cajeros electrónicos. Servicios telefónicos. Identificación presencial. Autenticación con usuario y contraseña.	Dinero físico. Atención presencial y asistida por canales electrónicos y de telecomunicaciones.
2000 -2012	Robo de imagen de la entidad bancaria. Robo de tarjetas plásticas. Clonación de tarjetas plásticas. Robo de datos de usuarios y contraseñas (Virus).	Tecnología web. Interoperabilidad de servicios. Identificación presencial o semipresencial. Autenticación en línea.	Dinero plástico. Atención y transacciones en línea. Procesamiento colaborativo, botones y pasarelas de pago.
>2012	Técnicas de Hacking. Técnicas de robo de información personal combinadas ingeniería social - *malware*. Falsas aplicaciones APT (*advanced persistent threat*) …..	Tarjetas EMV. Tecnología NFC (*Near Field Comunication.)* Big Data. Ciencias de datos. Computación en la nube. Identificación digital. Autenticación digital multifactor. Blockchain Identidad autogestionada.	Dinero bancario. Banca Móvil. Redes Sociales. Criptomonedas. Billeteras digitales. …

Fuente: Propia adaptado de “Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe]. Disponible en: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

En efecto, en el anterior cuadro puede verse la evolución de las amenazas a la identidad desde los años noventa, época en que el robo de documentos con fines de suplantación tenía como propósito hacerse con el dinero en metálico o efectivo dentro de un entorno totalmente físico de oficinas presenciales, credenciales en papel, firmas y huellas impresas, hasta el periodo posterior al 2012, momento actual en el que las amenazas a la identidad, aunque mantienen fines delincuenciales en relación con activos económicos, contrastan por suceder en ambientes puramente digitales, relaciones no presenciales, hiperconectadas y totalmente móviles.

Dentro de esta dinámica mundial de amenazas a la identidad se ha movido la banca colombiana. Por ello y, con el fin de identificar de primera mano las amenazas, riesgos y vulnerabilidades de la identidad digital en transacciones electrónicas bancarias dentro del entorno del país en estos tiempos que corren, se aborda el tema a partir de, primero, la revisión y análisis de los sitios web de los bancos, en particular de la narrativa de las secciones de seguridad, con el fin de establecer en dichas comunicaciones, campañas y/o *tips*, las principales amenazas, y las falencias o vulnerabilidades de los clientes a los que podrían dirigirse las acciones comunicativas de estos establecimientos y, segundo, la revisión y análisis de los usos de los datos declarados explícitamente en las políticas de protección de datos, que en su condición de responsables, deben hacer los bancos según lo establecido por la Ley. La información revisada, en ambos sentidos, es la publicada en los sitios web de veintiocho establecimientos bancarios vigilados por la Superfinanciera vigentes a marzo de 2022 (Anexo A).

Como primera medida, se determinó que bancos presentan un vínculo hacia la sección y/o recomendaciones de seguridad en sus páginas principales, con el fin de facilitar al cliente o usuario encontrar de primera mano el material correspondiente publicado. (Anexo B).

El **Cuadro 2** presenta el porcentaje de bancos que priorizan la información relacionada con la seguridad en su home.

Cuadro 2. Porcentaje de bancos con vínculo de sección de seguridad en home

Vinculo en home?	Cantidad de bancos	Porcentaje
NO	10	36%
SI	18	64%

Fuente: Elaboración propia

Llama la atención que, aunque la mayoría de los bancos presentan en sus páginas principales un link a las secciones de seguridad, persiste un 36% que no prioriza esta información.

Seguidamente, y con el fin de decantar las modalidades de amenazas con las que se pone en riesgo la identidad digital en el contexto colombiano, se revisaron las piezas comunicativas relacionadas con la seguridad publicadas por los veintiocho bancos, buscando particularmente la presencia o mención de las diferentes modalidades.

En el **Cuadro 3** se relacionan, en orden de porcentaje de mención, las modalidades de amenaza contra la identidad encontradas.

Cuadro 3. Modalidades de amenazas contra la identidad mencionadas por los bancos en sus micrositios de seguridad

Modalidad de Amenaza	Porcentaje de mención
Phishing X Correo electrónico	82%
Smishing	71%
Programas maliciosos -malware	64%
Ingeniería Social	61%
Vishing	43%
Cambiazo	39%
Skimming	36%
SIM Swapping	14%
Pharming	11%
Whaling	4%

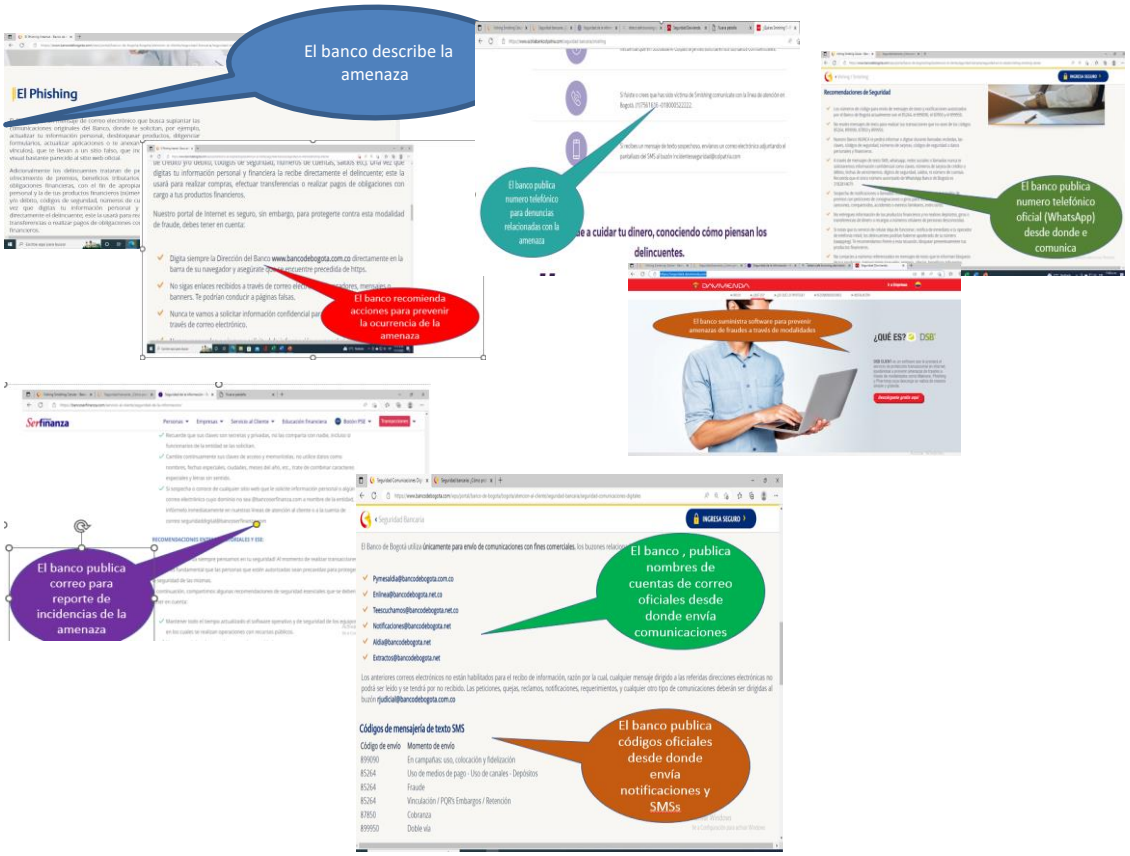
Fuente: Elaboración propia

El análisis presentado en este cuadro revela como el 82% de los bancos colombianos hizo referencia, en sus apartados sobre seguridad bancaria, al *phishing* por correo electrónico como amenaza, lo que permitiría asumir que esta modalidad de fraude tiene una presencia importante en el país. Igualmente, se pudo observar la concentración de las campañas comunicativas alrededor de las modalidades que se asocian a la "ingeniería social" - *Phishing, Smishing, vishing* -, de la que pudieran ser víctimas los clientes o consumidores financieros, lo que es totalmente concordante con los datos presentados como antecedentes para Latinoamérica.

De otro lado y, con el fin de identificar, en lo posible, las vulnerabilidades del usuario de las transacciones electrónicas bancarias a quienes van dirigidas las campañas y secciones de seguridad y que, a su vez, el sector bancario pretende intervenir para minimizar el riesgo de fraude por suplantación de identidad, se procedió a revisar el sentido o el mensaje de los contenidos publicados en los micrositios o piezas comunicativas relacionadas. Esta revisión permitió identificar los diferentes tipos de mensajes con propósitos de comunicación diferentes, desde los mensajes informativos genéricos aplicables a cualquier banco hasta los mensajes preventivos particulares al contexto del banco analizado, Anexo C.

La **Figura 5** ejemplifica el proceso de revisión del sentido de las publicaciones de seguridad de los bancos.

Figura 5. Ejemplos de tipos de mensajes comunicados por los bancos



Fuente: Elaboración propia

El resultado de la revisión y la clasificación del propósito y sentido de los mensajes comunicados por los bancos en sus secciones de seguridad, permitió la determinación de eventuales vulnerabilidades de los usuarios de las transacciones electrónicas bancarias, pudiendo establecer por ejemplo, que los bancos en sus comunicaciones pretenden atenuar o disminuir su desconocimiento en relación con las diferentes modalidades de amenaza y, en otros casos, paliar con recomendaciones y acciones prácticas la falta de experiencia o impericia de los usuarios de las transacciones electrónicas.

En **Cuadro 4** relaciona los tipos de mensajes utilizados por los bancos señalando su propósito, enfoque y posible vulnerabilidad de los usuarios de las transacciones bancarias electrónicas

Cuadro 4. Clasificación de mensajes de acuerdo con su propósito publicados por los bancos en sus sitios web

Clase de mensaje de acuerdo con su propósito	Contexto	Enfoque	Eventual vulnerabilidad del usuario
Informa o describe en que consiste la amenaza	General a cualquier banco	Información	Desconocimiento
Recomienda acciones para prevenir la ocurrencia de la amenaza	General a cualquier banco	Información	Impericia
Publica nombres de cuentas de correo oficiales desde donde el banco envía comunicaciones	Particular al propio banco	Prevención	Imprevisión
Publica número telefónico oficial (WhatsApp) desde donde el banco se comunica	Particular al propio banco	Prevención	Imprevisión
Publica códigos oficiales desde donde el banco envía notificaciones y SMSs	Particular al propio banco	Prevención	Imprevisión
Publica correo para reporte de incidencias de la amenaza	Particular al propio banco	Reacción	Imprevisión
Informa de suministro de software para prevenir amenazas de fraudes a través de modalidades como Malware, Phishing y Pharming	Particular al propio banco	Prevención	Imprevisión
Publica número exclusivo para denuncias relacionadas con la amenaza	Particular al propio banco	Reacción	Imprevisión

Fuente: Elaboración propia.

Una vez identificadas las modalidades de amenaza contra la identidad digital de mayor mención por los bancos y analizados los propósitos comunicacionales en relación con eventuales vulnerabilidades de los usuarios de transacciones electrónicas bancarias, se encontró procedente cuantificar en que porcentaje los establecimientos bancarios de Colombia acudieron al uso de cada clase de mensaje por cada amenaza identificada. El **Cuadro 5** presenta la cuantificación realizada.

Cuadro 5. Porcentaje de bancos que hacen uso de clases de mensajes por amenaza identificada

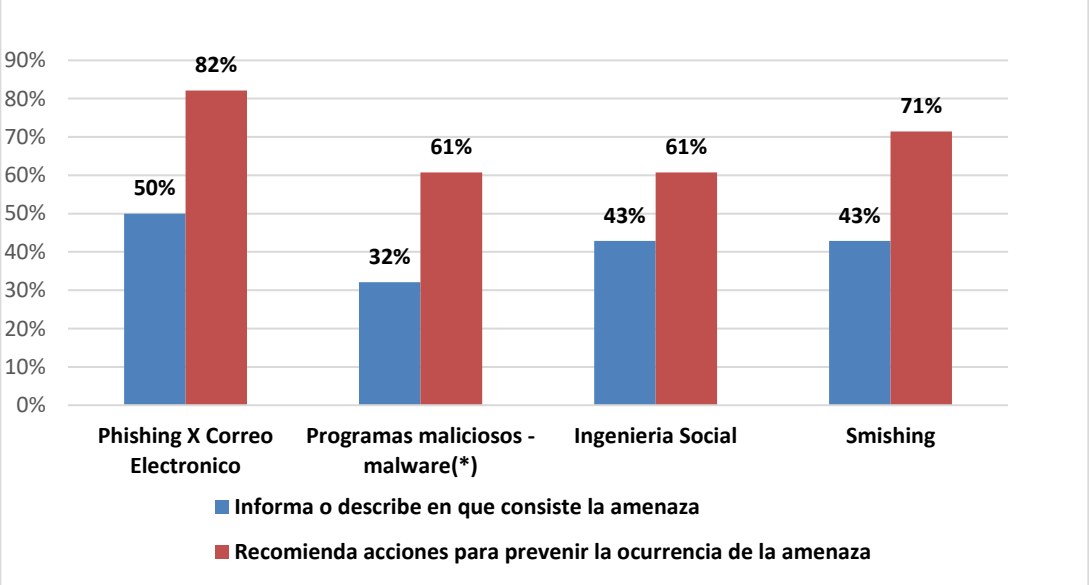
Tipo Mensaje / Amenaz	Phishin	Malwar	Ingenie a Socia	Skimi ing	Vishi g	Smisl ng	Camb azo	Fharn ng	Sim Swappi g	Whalin
Informa o describe en que consiste la amenaza	50%	32%	43%	29%	36%	43%	32%	7%	14%	4%
Recomienda acciones par prevenir la ocurrencia de l amenaza	82%	61%	61%	36%	43%	71%	39%	7%	14%	4%
Publica nombres de cuentas de correo oficiale desde donde el banco envía comunicaciones	14%									
Publica número telefónic oficial (WhatsApp) desde donde el banco se comunica					7%					
Publica códigos oficiales desde donde el banco envía notificaciones y SMSs						18%				
Publica correo para repor de incidencias de la amenaza	18%	4%		4%	4%	11%	4%			
Suministra software para prevenir amenazas de fraudes a través de modalidades como Malware, Phishing y Pharming	21%	21%						21%		
Publica número telefónico exclusivo para denuncias relacionadas con la amenaza	4%				4%	7%				

Fuente: Elaboración propia

Un primer análisis sobre los porcentajes de utilización de mensajes por parte de los bancos mostró como los mensajes comunicacionales más utilizados son aquellos de contexto general y enfoque informativo, es decir mensajes que podrían aplicar a cualquier transacción electrónica bancaria en cualquier banco y, que a su vez están dirigidos a contrarrestar el desconocimiento e impericia de cualquier usuario en relación con las amenazas y el fraude contra la identidad digital. Los mayores porcentajes de utilización de mensajes con información y recomendaciones genéricas, 82%, 71% y 61%, se asocian al *Phishing* por correo electrónico, el *Smishing,* el *Malware* y a la Ingeniería Social.

La **Figura 6** evidencia la utilización de mensajes con información y recomendaciones genéricas.

Figura 6. Presencia de mensajes de contexto general y enfoque informativo en secciones de seguridad de los bancos

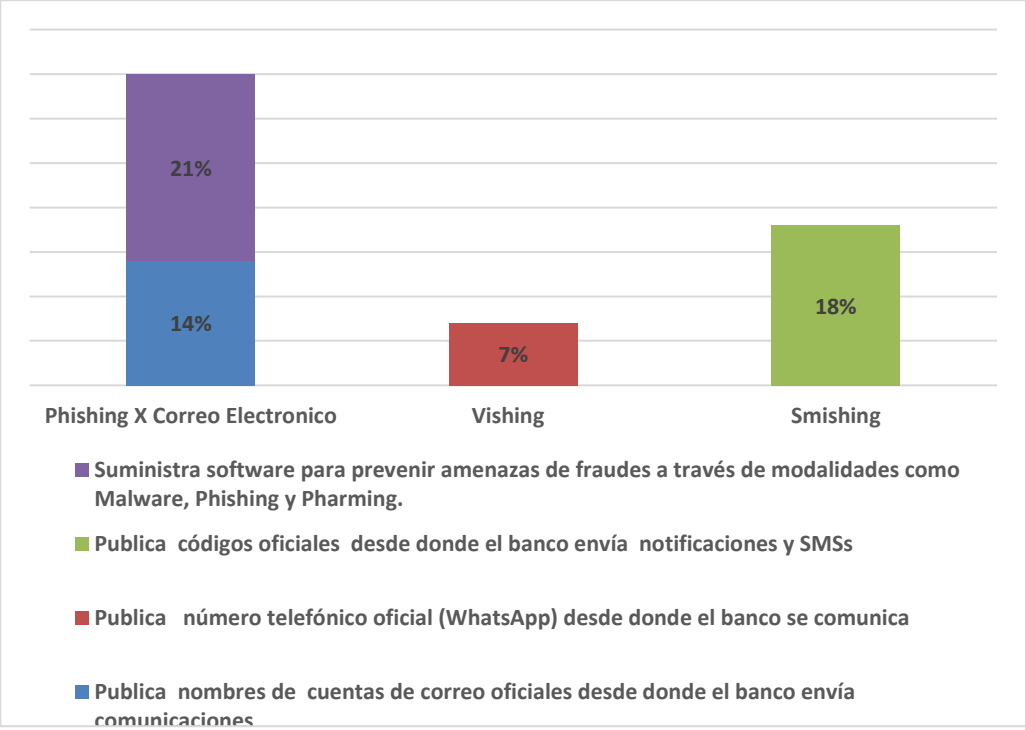


Fuente: Elaboración propia

En contraste, se observa la escasa utilización por parte de los bancos de mensajes que comunican medidas de contexto particular, todos los porcentajes de uso de estos mensajes son menores al 25%, que aplican únicamente al entorno del banco que los publica. Estos tipos de mensajes pudieran inducir a los usuarios de las transacciones electrónicas bancarias a validar el origen de las comunicaciones de manera expedita y, con este acto de cautela, evitar caer en la trampa y con ello "prevenir" de manera eficaz la ocurrencia del fraude por *Phising, Vishing Y Smishing*.

la **Figura 7** presenta los porcentajes de utilización de mensajes preventivos de contexto particular al propio banco.

Figura 7. Presencia de mensajes de contexto particular y enfoque preventivo en secciones de seguridad de los bancos

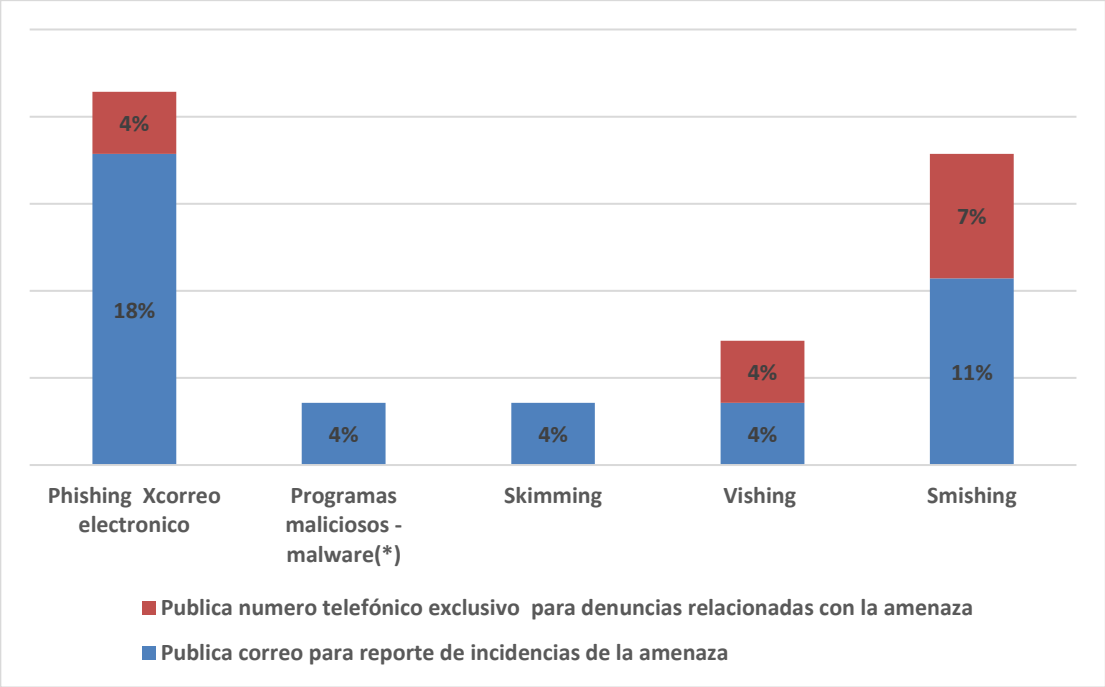


Fuente: Elaboración propia

Igualmente, en el análisis realizado sobre el sentido, propósito y enfoque de los mensajes comunicados por los bancos, llama la atención el hecho que el máximo porcentaje de los bancos que publican en sus secciones de seguridad mensajes que comunican disposiciones específicas para atender los usuarios que pudieron estar expuestos o fueron víctimas de fraude contra la identidad digital, alcanza como máximo un 18%, lo cual es notoriamente bajo.

La **Figura 8** presenta los porcentajes alcanzados en el análisis de los mensajes reactivos en caso de ocurrencia del incidente por modalidad de amenaza contra la identidad.

Figura 8. Presencia de mensajes de contexto particular y enfoque reactivo en secciones de seguridad de los bancos



Fuente: Elaboración propia

Finalmente y, para complementar el examen y la revisión de las amenazas, riesgos y vulnerabilidades de la identidad digital en transacciones electrónicas bancarias se procedió a analizar los usos o “finalidades” que los bancos realizan sobre los datos personales de sus usuarios, ya que es un hecho que la sobreexposición de estos datos facilita actividades delincuenciales de ingeniería social, técnica sobre la que se apoyan las principales modalidades de amenazas a la identidad digital ya identificadas.

Para este efecto, se revisaron los documentos contentivos de las veintiocho políticas de tratamiento de datos de igual cantidad de bancos vigentes a marzo de

2022 según la Superfinanciera. En principio, se examinó la prioridad que dan los bancos en sus sitios web a las mencionadas políticas - Anexo E-, dado que estas políticas deben ser conocidas y aceptadas por los titulares o dueños de los datos previamente a la realización de las transacciones bancarias electrónicas. Es notorio como solo la mitad de los bancos analizados publica en su home un vínculo que dirige a las políticas de protección de datos.

El **Cuadro 6** relaciona los porcentajes de bancos analizados que publican en su home un vínculo que dirige a las políticas de protección de datos.

Cuadro 6. Bancos con vínculo en la página principal dirigido a las políticas de protección de datos personales

Vinculo en home?	Cantidad de bancos	Porcentaje
NO	14	50%
SI	14	50%

Fuente: Elaboración propia

Ahora bien, para llevar a cabo el análisis del uso que los bancos pueden hacer de los datos personales de sus clientes o usuarios, se desglosó el contenido de los apartados relacionados con “las finalidades” correspondientes en las políticas de cada banco y, con el fin de facilitar la presentación del análisis, se asoció cada glosa a una categoría de uso. El Anexo D, recopila trescientas treinta y cinco (335) sentencias o declaraciones de todo el universo examinado asociadas a una categoría de uso determinada.

En el **Cuadro 7** se relacionan en orden alfabético las categorías de uso que se determinaron en este trabajo para el respectivo análisis.

Cuadro 7. Categorías de uso de los datos personales de los clientes por parte de los bancos

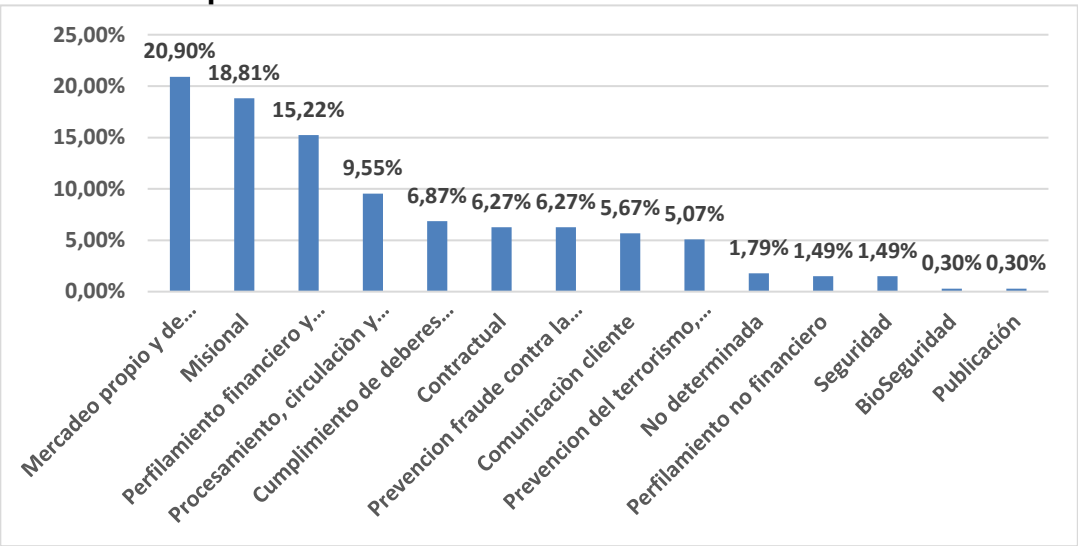
Orden Alfabético	Categoría de uso
1	Bioseguridad
2	Comunicación cliente
3	Contractual
4	Cumplimiento de deberes ante autoridades
5	Mercadeo propio y de terceros autorizados
6	Misional
7	No determinada
8	Perfilamiento financiero y comercial
9	Perfilamiento no financiero
10	Prevención del terrorismo, lavado de activos, actividades ilegales
11	prevención fraude contra la identidad
12	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior
13	Publicación
14	Seguridad

Fuente: Elaboración propia

En este ejercicio de asociación de glosas o finalidades a categorías de uso resultó muy llamativa la frecuencia de aparición de unas categorías en relación con las otras. Es claramente notorio como el 20.90% de glosas (70 de 335) pertenecen al grupo de “Mercadeo propio banco y de terceros autorizados”, en tanto que solo el 6. 27% (21 de 335 glosas) corresponden a la categoría “Prevención del fraude contra la identidad”.

la **Figura 9** permite visualizar las categorías de uso de los datos personales en los que fue posible agrupar las finalidades declaradas por los bancos.

Figura 9. Frecuencia de mención de finalidades o glosas por categoría de uso de datos personales



Fuente: Elaboración propia

En consecuencia, y a partir de todos los anteriores análisis con el propósito de examinar las amenazas, riesgos y vulnerabilidades de la identidad digital en transacciones electrónicas bancarias en el contexto colombiano, se pudo establecer como relevantes las siguientes observaciones:

Hay una cantidad importante de bancos que no ubican un vínculo a las secciones y recomendaciones de seguridad en sus páginas principales o *home* de sus sitios web, hecho que implicaría que sus usuarios tendrían que navegar en su búsqueda, lo cual no se compadece con la importancia de estas campañas para prevenir el fraude de suplantación de la identidad.

Las principales amenazas y vulnerabilidades identificadas por los bancos contra la identidad digital de los clientes sus usuarios de transacciones electrónicas bancarias son las que tienen que ver con modalidades asociadas a la llamada ingeniería social, actualmente el *Phishing*, el *Smishing* y el Vishing.

Las campañas de seguridad, recomendaciones y *tips* que realizan la mayoría de los bancos están enfocadas a informar y recomendar acciones de manera general y están dirigidas sobre todo a minimizar el desconocimiento e impericia de los usuarios de transacciones electrónicas bancarias y con ello la probabilidad de fraude contra la identidad digital. También, se pudo observar que algunos pocos bancos comunican información particular al banco y de prevención y, que solo dos bancos van más allá de la comunicación y suministran software para prevenir amenazas de fraudes a través del *Malware, el Phishing y el Pharming*.

En relación con las finalidades o usos de los datos personales declarados en las políticas de tratamiento de los bancos, se observó que solo la mitad de estas entidades analizadas publica en su página principal un vínculo que lleva a la sección respectiva, lo que podría dificultar el conocimiento que de estas políticas debe tener el cliente antes de realizar transacciones electrónicas o cualquier otro relacionamiento con la banca.

Finalmente, puede decirse que el análisis de los tipos de uso de los datos personales permitió observar la importante diversidad de finalidades que dan los bancos a esta información de sus clientes. Es notorio el énfasis que dan los bancos a la posibilidad de usar la información personal para realizar mercadeo de productos y servicios propios y de terceros autorizados, siendo la categoría de uso con mayor frecuencia de mención en las correspondientes políticas. El uso de los datos personales en actividades de mercadeo dentro y fuera del contexto del banco podría implicar un mayor grado de exposición de esta información en un eventual detrimento de la privacidad de los consumidores financieros o usuarios.

5.2. CARACTERÍSTICAS DE CIBERSEGURIDAD DE LA IDENTIDAD DIGITAL EN TRANSACCIONES ELECTRÓNICAS BANCARIAS

La Ciberseguridad de la identidad digital en las transacciones bancarias es un asunto de gobernanza del Estado, por ello el Gobierno Nacional a través de la Superintendencia Financiera, vigila y controla los establecimientos bancarios y, señala requerimientos mínimos en todos los aspectos que aseguren a la sociedad la viabilidad de estos. En particular la citada entidad ha fijado los mínimos técnicos para la gestión del riesgo cibernético que, en su cumplimiento, deberían incrementar la seguridad de las transacciones electrónicas bancarias y la confianza de la ciudadanía.

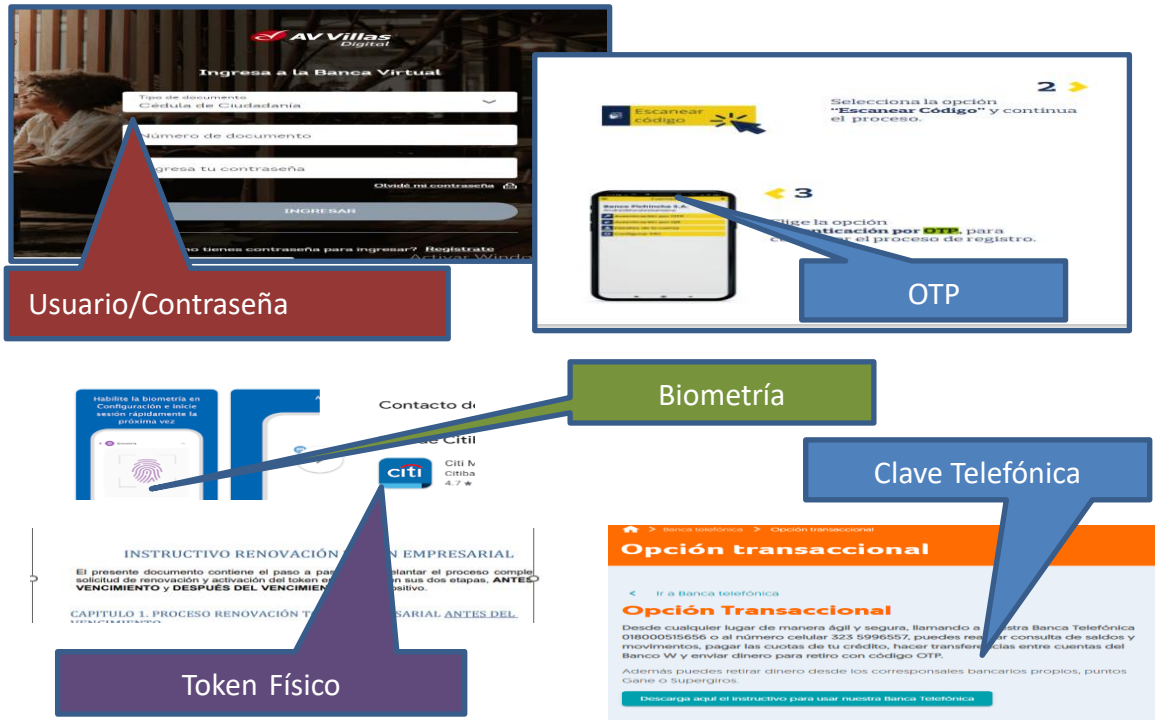
En efecto, las características de ciberseguridad de la identidad digital en transacciones electrónicas bancarias que deben cumplir los bancos en sus relaciones con usuarios de transacciones electrónicas bancarias, están señaladas en la Circular Externa No.029 de 2019, norma que establece el deber de uso de mecanismos como la biometría, los certificados de firma digital de acuerdo a lo establecido en la Ley 527 de 1999, las claves de un único uso OTP (*One Time Password*), el registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizarían las operaciones, todas y cada uno de los anteriores mecanismos, en combinación con un segundo factor de autenticación.

Con este contexto regulatorio particular y encontrando posible examinar a través de los portales de los bancos, de las descripciones de las apps y de los instructivos disponibles, los mecanismos con los cuales cada banco verifica la identidad digital

y, al mismo tiempo, cumplir las disposiciones del gobierno asegurando con ello la identidad de quienes intervienen en las citadas transacciones, se recopiló y analizó - Anexo F- los tipos de banca que se ofrecen en el país, así como las medidas de autenticación y autenticación fuerte implementadas por los veintiocho establecimientos bancarios vigentes a marzo de 2022.

La **Figura 10** presenta gráficamente ejemplos de los mecanismos que los bancos utilizan para autenticar la identidad digital en transacciones electrónicas.

Figura 10. Ejemplos de mecanismos de autenticación de la identidad digital utilizados en transacciones electrónicas bancarias



Fuente: Elaboración propia

El análisis anterior permitió, en principio, identificar los tipos de banca a través de los cuales se ofrecen servicios digitales para realizar transacciones bancarias electrónicas, siendo estos tipos los correspondientes a la banca virtual, móvil y telefónica. Es claro que casi la totalidad de los bancos ofrecen banca virtual en contraste con la banca telefónica, la cual solo es ofrecida por un banco de los estudiados.

En el **Cuadro 8** se expone el porcentaje de bancos del universo revisado que ofrece cada tipo de banca.

Cuadro 8. Modalidades de banca ofrecida por la red bancaria en Colombia

Tipo de Banca	Número de Bancos	Porcentaje de Bancos
Banca virtual	27	96%
Banca móvil	21	75%
Banca telefónica	1	4%

Fuente: Elaboración propia

En relación con la revisión de los factores de autenticación de la identidad digital que implementan los bancos colombianos, el análisis permitió establecer los mecanismos de mayor utilización en los servicios ofrecidos a través de las modalidades de banca virtual, móvil y telefónica.

El **Cuadro 9** relaciona en orden alfabético los distintos mecanismos que implementados para autenticar la identidad del usuario y la identidad de su sitio web.

Cuadro 9. Mecanismos más usados en la autenticación de identidad en transacciones electrónicas bancarias

Mecanismo de autenticación de identidad digital	Del usuario	Del banco
Biometría en banca móvil	X	
Clave telefónica	X	
Clave único uso (One Time Password - OTP)	X	
Imagen /pregunta/ frase de seguridad	X	
Registro direcciones IPs /Móvil	X	
Certificación de página web		X
Token físico	X	
Token por software	X	
Usuario y Clave/contraseña	X	

Fuente: Elaboración propia

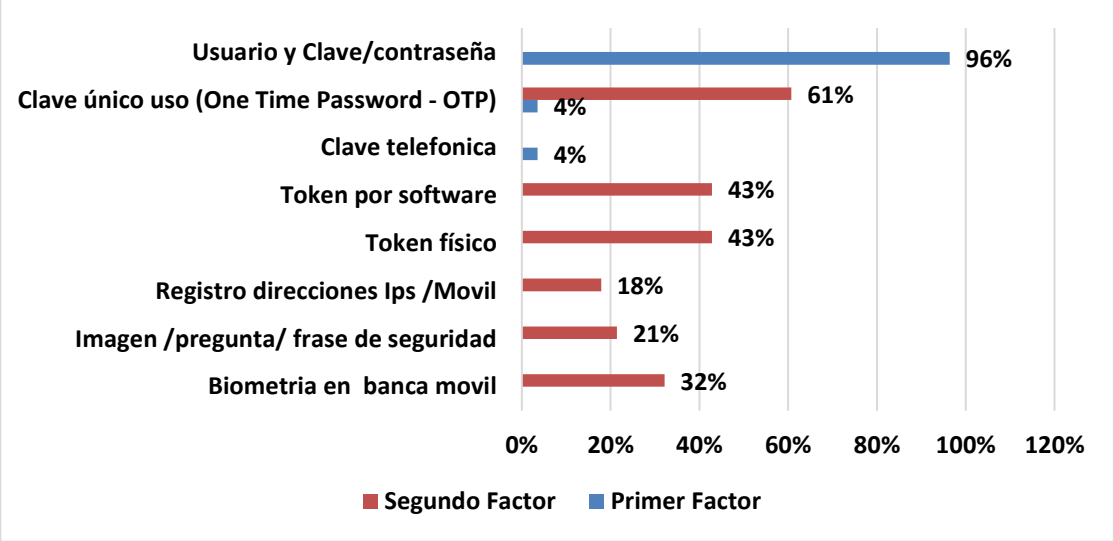
Ahora bien, una vez identificados los mecanismos de autenticación de mayor uso por la banca colombiana, fue importante revisar como se combinan como factores dentro de un concepto multifactorial de ciberseguridad de la identidad digital en transacciones electrónicas bancarias, por lo que se procedió a revisar el uso de estos mecanismos en roles de primer o segundo factor. Es importante mencionar, que, en la modalidad de banca virtual, la totalidad de los bancos que la ofrecen utiliza como primer factor de autenticación el mecanismo denominado “usuario y clave/contraseña” y, solo un banco utiliza como primer factor la “clave telefónica”, que además corresponde al único banco que ofrece, de manera exclusiva, la banca telefónica.

Igualmente, se identificó al mecanismo denominado “Certificación de página web” como la forma en que todos los establecimientos bancarios acreditan su propia identidad digital, lo que le permite al cliente asegurar, solamente constatando con

la imagen de un candado cerrado en la URL, que ciertamente está utilizando un servicio ofrecido por su banco.

En la **Figura 11** puede visualizarse el uso de los diferentes mecanismos de autenticación de la identidad por los bancos colombianos.

Figura 11. Mecanismos de autenticación de identidad digital utilizados por los bancos en un esquema multifactorial



Fuente: Elaboración propia

Del uso combinado de factores que pudieran permitir la autenticación fuerte del usuario de las transacciones electrónicas bancarias en Colombia, pudo observarse que la combinación preferida por los bancos es claramente, la que utiliza el "Usuario y Clave/contraseña" como primer factor y la "Clave de único uso (OTP)" como segundo factor, seguido en este sentido por la utilización de tokens digitales o generados por software y tokens generados en dispositivos o hardware independiente.

En lo que tiene que ver con la autenticación de los sitios web de los bancos, pudo observarse que el 100% de los bancos certifican sus páginas web con certificados digitales emitidos por autoridades certificadoras de amplio reconocimiento mundial.

En lo que corresponde al uso de la biometría, factor que cuenta con alta percepción de confiabilidad en relación con la autenticidad de la identidad digital, el análisis arrojó que solo un 32% de los bancos la activa como un segundo factor en servicios de banca móvil, aprovechando las capacidades de los teléfonos móviles, hecho que siendo representativo no es necesariamente el óptimo.

Así las cosas, pudo encontrase que en la actualidad la banca colombiana protege la identidad digital suya y de sus usuarios en las transacciones electrónicas bancarias, de la manera más tradicional, ya que se inclina por el uso de factores muy maduros y accesibles al usuario, y de pronto menos costosos como el OTP y el token por software.

Igualmente, no se encontró que en el proceso de autenticación de la identidad digital en transacciones electrónicas bancarias se hiciera a través de credenciales certificadas por terceros, como los certificados digitales de los que trata la ley 527 de 1999. Tampoco se halló que en dichas transacciones electrónicas se autenticara en línea la identidad del usuario por parte de la Registraduría Nacional del Estado Civil de Colombia, entidad encargada de identificar a los ciudadanos en este país.

Finalmente, puede decirse a partir de la revisión realizada que actualmente la autenticación de la identidad digital en las transacciones electrónicas bancarias se apalanca sobre - cargadamente en un elemento vulnerable como es el teléfono celular y la tarjeta SIM, hecho que puede aportar mayor exposición o vulnerabilidad ante las amenazas como el *SIM Swapping*, amenaza que aprovecha falencias y ausencia de rigores por parte de operadores de telefonía celular facilitando la clonación de este elemento.

5.3. RECOMENDACIONES PARA PREVENIR LA SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO DE TRANSACCIONES ELECTRÓNICAS BANCARIAS

El consumidor financiero en Colombia tiene derechos y deberes relacionados con el tratamiento de su información personal y, en particular con el cuidado y la protección de su identidad digital. Minimizar el riesgo de ser suplantado en su relacionamiento con las entidades bancarias, particularmente en las transacciones electrónicas bancarias, es un objetivo que debe estar en la cabeza y accionar de todo usuario de transacciones digitales.

Con el fin de aportar elementos que den contexto a las recomendaciones que pudieran hacerse para prevenir la suplantación de la identidad del usuario de transacciones electrónicas bancarias se procedió a establecer los ámbitos o productos y servicios bancarios donde se presenta la mayor proclividad a la suplantación de la identidad. Con este propósito se revisaron las estadísticas de quejas para el periodo comprendido entre el año 2018 y el año 2021, publicadas por la Superintendencia Financiera de Colombia, particularmente las quejas que esta entidad cataloga como de “suplantación presunta de persona”.

El **Cuadro 10** presenta los principales productos bancarios implicados en quejas de suplantación de la identidad de las personas.

Cuadro 10. Productos bancarios con mayor número de quejas por suplantación presunta de persona, periodo 2018 – 2021

Producto bancario	Porcentaje promedio
Tarjetas de crédito	72,10%
Cuenta de ahorros	20,04%
Crédito de consumo y/o comercial	6,24%
Cuenta corriente	0,82%

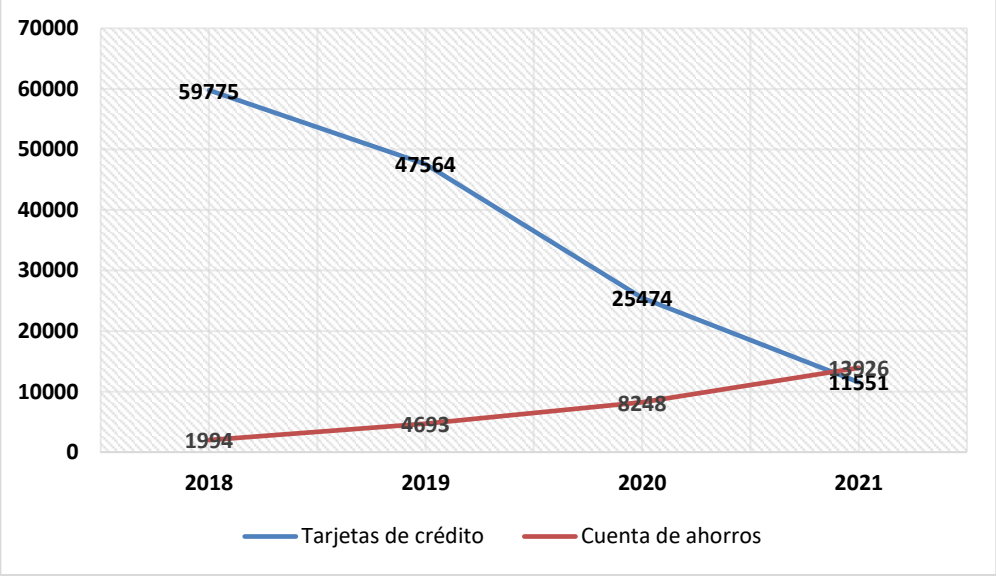
Fuente: Elaboración propia

El cuadro señala los cuatro productos bancarios sobre las que recaen en promedio de los cuatro años analizados el 99.21% de las quejas por la suplantación a la identidad.

En efecto, analizada la cantidad de quejas asociadas a los dos productos en los que hay mayor proclividad de suplantación, las tarjetas de crédito y las cuentas de ahorro, pudo notarse en su comportamiento tendencias claramente contrarias.

La **Figura 12** ilustra las tendencias de las quejas asociadas a la tarjeta de crédito y cuentas de ahorro.

Figura 12. Comportamiento del número de quejas por suplantación presunta de persona, periodo 2018 – 2021



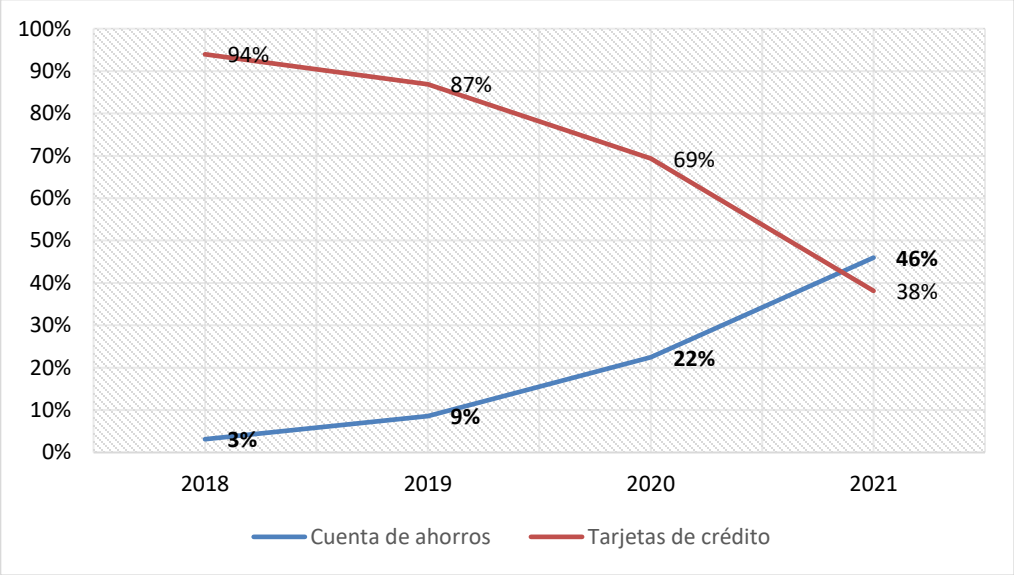
Fuente: Elaboración propia

Así pues, para el periodo 2018 -2021 las quejas relacionadas con la suplantación asociadas a tarjetas de crédito descienden, en tanto que las asociadas a las cuentas de ahorro crecen, llegando incluso a sobrepasarlas para el año 2021.

También pudo observarse, que el crecimiento porcentual de las quejas por suplantación presunta de persona en el periodo mencionado para la “cuenta de ahorros” paso de un 3% a un 46%, llegando en el 2021 a representar casi la mitad del total de las quejas interpuestas y, que este aumento es notoriamente alto en el periodo 2020-2021, momento agudo de la pandemia del Covid19 cuando la bancarización tuvo un aumento considerable en Colombia.

La **Figura 13** evidencia el comportamiento de las quejas interpuestas por suplantación de la identidad de las personas.

Figura 13. Comportamiento del porcentaje de quejas por suplantación presunta de persona, periodo 2018 – 2021



Fuente: Elaboración propia

Finalmente, puede decirse que examinadas las amenazas, los riesgos y las vulnerabilidades de la identidad digital, recopiladas las características de ciberseguridad implementadas por los bancos del país para autenticar la identidad digital en transacciones electrónicas bancarias y determinados los productos bancarios que presentan mayor número de quejas por suplantación de la persona, es posible presentar una perspectiva asociada a un concepto integral que se ha llamado “Círculo dorado de cuidado de la identidad digital en transacciones electrónicas bancarias” en el que se señalan recomendaciones que podrían ayudar al usuario de dichas transacciones a reconocer la necesidad de acometer acciones integrales para evitar ser víctima de las amenazas identificadas.

La **Figura 14** ilustra los tres tipos de acciones necesarios al cuidado de la identidad digital.

Figura 14. Círculo dorado de cuidado de la identidad digital en transacciones electrónicas bancarias

Fuente: Elaboración propia

Efectivamente, desde el ámbito del conocimiento y para evitar fraudes por suplantación de la identidad de los usuarios de transacciones electrónicas bancarias, se proponen las siguientes recomendaciones generales:

- Conocer y documentarse frecuentemente sobre sus derechos y deberes en relación con la protección de sus datos personales y, en particular, tomar conciencia de las finalidades o usos que declaran los establecimientos bancarios en sus políticas de tratamiento de datos.

- Hacer uso de los mecanismos y canales que disponen los bancos, cuando se suponga, se hayan comprometido sus datos por parte de estos establecimientos.

- Exigir de los bancos el informe(s) sobre los incidentes cibernéticos que se hayan presentado y en los que se hubiera podido ver afectada la confidencialidad o integridad de su información, al igual que el informe de las medidas adoptadas para solucionar la situación.

- Atender las campañas y tomar en serio las recomendaciones que se hacen, por parte de los bancos, con el fin de prevenir el fraude o suplantación de identidad digital relacionadas con la ingeniería social en modalidades de *Phishing, Smishing y Vishing*, entre otros.

- Seguir las recomendaciones particulares de los bancos en relación con las contraseñas, su conformación y cuidado y cambiarlas con frecuencia utilizando claves robustas, incluidas las de los correos relacionados.

- Conocer y tener a mano la URL de su banco, verificando que corresponda a un sitio de servidor seguro o con protocolo //https. Igualmente, tener presente que los bancos nunca solicitan información personal a través de llamadas, correos, mensajes de texto, mensajes de WhatsApp, etc. Es importante y necesario conocer los canales de ayuda o asistencia, los nombres de cuenta de correos, números telefónicos y códigos de mensajería SMS desde donde se comunica el establecimiento bancario.

- Conocer las funcionalidades y seguridad de los servicios ofrecidos por el banco en sus modalidades virtual, móvil y telefónica y utilizar los servicios de bloqueo desde estos servicios en caso de sospecha o de un eventual compromiso de las credenciales o la información de la identidad.

- Hacer uso de los canales dispuestos por los bancos cuando haya sido víctima de suplantación, teniendo claro que las campañas masivas de renovación de plásticos o actualización de datos no existen. Igualmente, informar a las autoridades a través de las páginas de la Fiscalía y la Policía: www.fiscalia.gov.co y www.policia.gov.co

De otra parte y, de igual relevancia al conocimiento o grado de información relacionada con la protección de la identidad digital que deben adquirir los usuarios de transacciones electrónicas bancarias, se encuentra el comportamiento personal, es decir aquellos hábitos conscientes e interiorizados que los citados usuarios deberían observar principalmente en su vida pública y en su exposición en redes sociales, para no ser víctimas fáciles de fraude por suplantación de identidad digital. Por ello, es altamente recomendable:

- Desconfiar de cualquier comunicación por correo, llamada y/o mensaje de texto que apele a emociones como el miedo, la ira o la urgencia. Son muy frecuentes aquellas comunicaciones que en tono o sentido alarmante amenazan con asuntos jurídicos, comunican de problemas con terceros y familiares, o informan de cambios en los estados de la SIM *card*. Específicamente, en temas bancarios estos mensajes preocupantes advierten de bloqueos de cuentas y productos, ofrecimientos de beneficios en créditos y/o tipos de servicios adicionales tipo seguro o asistencial, entre otros.

- En caso de recibir comunicaciones en el sentido anteriormente mencionado, abstenerse de seguir las instrucciones impartidas en estas comunicaciones por los posibles ciberdelincuentes y validar con el banco cualquier comunicación recibida, utilizando los canales dispuestos por los establecimientos bancarios como correos y líneas de ayuda, que permitan confirmar la información recibida.

- Ejercitarse en las recomendaciones dadas por los bancos en relación con correos, mensajes SMSs, links, llamadas y, en general con cualquier comunicación que se reciba y que pretenda que se actúe de manera inmediata y urgente, así no se relacione con un banco.

- Minimizar o eliminar la sobreexposición de la información personal en redes sociales, la cual puede ser utilizada por delincuentes a través de la ingeniería social. En caso de moverse en redes sociales, utilizar funcionalidad en modo de privacidad.

- Como la autenticación de la identidad digital en transacciones electrónicas bancarias en Colombia se apalanca principalmente en el "usuario y contraseña" como primer factor en combinación con un segundo factor, generalmente un código temporal OTPs o un tokens por software, se recomienda abstenerse de bajar software y/o aplicaciones de dudosa reputación, juegos, etc., a los dispositivos electrónicos desde donde se realizan las transacciones, en razón a que estas piezas de código pueden ser los vectores de infección de virus y *malware* con los cuales los ciberdelincuentes pueden acceder a esta información que el banco envía como mecanismo de autenticación.

- Atender con la debida diligencia aspectos relacionados con la SIM *card,* el teléfono móvil y el operador de telefonía. Funcionalidades como el bloqueo oportuno y/o remoto de las tarjetas y teléfonos, el uso de las herramientas de biometría, servicios de encriptación, entre otros deberían ser activados y utilizados.

Igualmente, se proponen las siguientes recomendaciones en relación con elementos, mecanismos y/o protocolos tecnológicos que, mediante un adecuado aprovisionamiento, permitirían evitar o minimizar los incidentes de fraude o de suplantación de la personal y cerrar así, el circulo dorado del cuidado de la identidad digital, responsabilidad que debe estar presente en la cultura de todo usuario de transacciones electrónicas:

- Mantener actualizados el sistema operativo del dispositivo y el navegador desde donde se realizan las transacciones electrónicas bancarias.

- Siempre realizar las transacciones electrónicas bancarias a través de redes seguras, teniendo la precaución de no efectuarlas a través de redes públicas. Configurar filtros en el *router* para controlar el acceso y el tráfico de paquetes.

- Contar y mantener actualizado el software antivirus y un detector de *malware*, que puedan ofrecer protección en tiempo real.

- Activar protocolos de verificación *Sender Policy Framework* -SPF-, para evitar que envíen e-mails desde una cuenta suplantada. El dominio tendrá que autorizar al servidor de correo *Simple Mail transfer Protocol* – SMTP- para enviar o, en su caso, para recibir un correo.

- Verificar que en todos los lugares o web sites que se visiten a través de internet siempre se haya implementado un sitio de servidor seguro o con protocolo //https e igualmente, revisar las políticas de cookies que anuncian estos sitios dándose el tiempo de reflexionar y escoger que permitiría o no hacer a través de estas piezas de software.

- Desactivar la ejecución de código en JavaScript del navegador en los momentos en los que haya que exponer datos, si hubiera sospecha de estar ante un ataque *Web Spoofing* o de suplantación de identidad electrónica.

Finalmente, debe resaltarse el hecho que solo desde la conciencia y las acciones complementarias desde el conocimiento, el comportamiento y el aprovisionamiento de elementos tecnológicos podrá el usuario de transacciones electrónicas bancarias minimizar el costoso fraude de suplantación de su identidad digital del que puede ser víctima.

6. CONCLUSIONES

Esta monografía se realizó sobre una revisión sistemática y novedosa del enfoque y sentido de la información publicada por los bancos en relación con las recomendaciones de seguridad en transacciones electrónicas, de los mecanismos de autenticación de la identidad del usuario en estas transacciones, de las políticas de protección de datos personales declaradas por los establecimientos bancarios, al igual que la revisión de las quejas que, por suplantación presunta de persona, se recopilan por la Superintendencia Financiera. Esta mirada complementaria permitió analizar integralmente la ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia y aportar los elementos relevantes que se concluyen a continuación:

De la revisión sistemática y análisis realizados sobre la información publicada por los bancos a través de sus sitios web oficiales, piezas comunicativas, portales transaccionales, y aplicaciones móviles, se concluye que las principales amenazas contra la identidad digital en transacciones electrónicas bancarias son las identificadas como *Phishing, Smishing y Vishing* en asocio de técnicas de ingeniería social. Así mismo, puede concluirse que las vulnerabilidades más importantes se encuentran en el desconocimiento, falta de previsión e impericia de los usuarios de las transacciones electrónicas bancarias.

También se concluye, que el mayor esfuerzo comunicacional de los bancos para contrarrestar el fraude por las amenazas identificadas se concentra en la publicación de información general y recomendaciones igualmente generarles, relacionados con su prevención. Que hay muy poco despliegue comunicativo de acciones particulares o del contexto propio de cada banco, que pudiera informar de medidas específicas para facilitar a su cliente evitar la ocurrencia de incidentes asociados al *Phishing, Vishing y Smishing* y/o dar apoyo una vez ocurridos estos incidentes, si fuera el caso.

Es importante concluir en relación con el tratamiento de datos personales, que los bancos dan a éstos una diversidad importante de finalidades, siendo el “Mercadeo propio y de terceros autorizados” el uso al que estos establecimientos dan mayor énfasis, lo que permitiría suponer que los datos personales de los usuarios bancarios pudieran caracterizarse por un grado de exposición importante que implicaría un, igualmente importante, grado de compromiso de la privacidad.

En relación con las características de ciberseguridad implementadas por los bancos colombianos para autenticar la identidad digital de los usuarios de las transacciones electrónicas, se concluye que el método tradicional conocido como “Usuario y Clave/contraseña” es el mecanismo que, empleado desde principio de este siglo, se constituye por excelencia como el primer factor de autenticación. Al respecto,

también es concluyente que la autenticación fuerte o la combinación de factores de autenticación a través de esquemas multifactoriales en las transacciones electrónicas bancarias se realiza principalmente a través de mensajes a teléfonos móviles con mensajes tipo SMS que contienen claves temporales de único uso u OTPs y Tokens generados por software.

En consecuencia, de lo anterior, podría concluirse que el teléfono celular es un dispositivo electrónico privilegiado, sobre el cual reposa la autenticación fuerte de la identidad digital de los usuarios de transacciones electrónicas bancarias, elemento que siendo personal es altamente vulnerable a daños, pérdidas y clonación, entre otros.

Se podría concluir también, que la autenticación fuerte de la identidad digital en las transacciones electrónicas bancarias utilizando la biometría, mecanismo de muy alta percepción de confiabilidad, es incipiente, ya que solo se ofrecen en modalidad de banca móvil en un pequeño porcentaje de aplicaciones.

De otro lado, es posible concluir que los esquemas multifactorial de autenticación de la identidad digital de usuarios en transacciones electrónicas bancarias en Colombia, basados en certificados digitales e interacción on-line con entidades de confianza, como entidades emisoras o certificadoras digitales y con la misma Registraduría Nacional del Estado Civil, no están documentados lo que podría permitir suponer que estos esquemas no han sido implementados aún.

Debe concluirse igualmente, que la posibilidad de fraude por suplantación presunta de persona es mayor en uso de productos bancarios asociados a transacciones electrónicas, que en la medida que crece la bancarización y, con ello la utilización de tarjetas de crédito y cuentas de ahorro, los esquemas robustos y novedosos de autenticación fuerte de la identidad digital y la disposición cuidadosa de los datos personales de los usuarios bancarios son factores críticos que tienen implicaciones importantes en el relacionamiento banco – cliente.

Finalmente, puede concluirse que en las actuales condiciones y características de la ciberseguridad de las transacciones electrónicas bancarías en Colombia, el actor más importante sigue siendo el usuario, cliente o consumidor financiero, ya que, de la conciencia que tenga sobre el cuidado de su identidad digital en redes sociales y con su proveedor de servicios bancarios, del conocimiento de las modalidades de fraude, de su comportamiento y del aprovisionamiento de los elementos tecnológicos idóneos dependerá, no solo la protección de activos dinerarios, sino también su buen nombre, su tranquilidad y en últimas su calidad de vida financiera.

7. RECOMENDACIONES

Como las amenazas y los fraudes en transacciones electrónicas bancarias son dinámicas en el tiempo y sus características de ciberseguridad dependen de los contextos económico, social y tecnológico en que se presten los servicios bancarios, se recomienda al sector bancario publicar en todas sus páginas principales las recomendaciones generales y particulares relacionadas con la seguridad de la identidad digital, así como la presentación de las políticas de tratamiento de datos personales y las formas como los titulares pueden hacer sus reclamos y solitudes relacionadas.

Sería altamente recomendable a las transacciones electrónicas bancarias en Colombia, diversificar y aumentar el uso de otros mecanismos como segundos factores de autenticación, de manera que se desconcentre del teléfono móvil, elemento altamente vulnerable, los elementos que permiten determinar e manera certera, en un momento dado, que un usuario o cliente es quien dice ser por lo que “lo distingue, lo que tiene y lo que sabe”.

Se recomienda a la universidad acometer nuevos trabajos de grado que aborden el enfoque integral que ha dado esta monografía a la revisión y análisis de la identidad digital en transacciones electrónicas bancarias en Colombia, que implicó una mirada desde la óptica de los derechos humanos, el uso de la tecnología que puede salvaguardarla y la conciencia de las personas en relación con el autocuidado.

Finalmente y, dado que sobre el usuario de las transacciones electrónicas bancarias recae, en mayor medida, la responsabilidad del cuidado de la protección de su información personal y de su identidad digital, se recomienda a la sociedad en general impulsar acciones de responsabilidad social que fortalezcan y apoyen a las personas en el conocimiento, comportamiento y aprovisionamiento de los elementos necesarios para la protección de la identidad digital y, con ello, la minimización del riesgo de fraude por suplantación de la identidad digital.

8. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia puedan acceder al documento.

9. BIBLIOGRAFÍA

ASOBANCARIA. [En línea]. Impacto económico y social del phishing y el smishing en Colombia y el mundo. [Consultado el 6 de febrero de 2022]. Disponible en: https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf

ASUNTOS LEGALES. [En línea]. Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651

BANCO AGRARIO. [En línea]. Banco Agrario App. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancoagrario.gov.co/canales/bancoagrarioapp/Paginas/default.aspx

BANCO AGRARIO. [En línea]. INSTRUCTIVO SEGUNDO FACTOR DE AUTENTICACIÓN POR ENROLAMIENTO DE MÁQUINAS. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancoagrario.gov.co/BancaVirtual/Documents/Verificaci%C3%B3n%20de%20instalaci%C3%B3n%20de%20maquina%20de%20JAVA.pdf

BANCO AGRARIO. [En línea]. MANUAL DE USUARIO BANCA VIRTUAL. [Consultado el 12 de mayo de 2022]. Disponible en: https://ebanking.bancoagrario.gov.co/BA.ICBanking.WebUI/Files/Manual%20de%20Usuario%20Persona%20Natural%20y%20Jur%C3%ADdica.pdf

BANCO AGRARIO. [En línea]. Tips de seguridad. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.bancoagrario.gov.co/canales/Seguridad/Paginas/default.aspx

BANCO AGRARIO DE COLOMBIA. [En línea]. Política Protección de Datos Personales Banco Agrario de Colombia. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancoagrario.gov.co/SAC/Documents/DocTratamientoDatosPersonales.pdf

BANCO AV VILLAS. [En línea]. Centro de Entrenamiento - Antifraude AV Villas. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.avvillas.com.co/avvillas/seccionseguridad/index.html

BANCO AV VILLAS. [En línea]. Entrénate para evitar ser víctima de fraude con Claves OTP. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.avvillas.com.co/avvillas/seccionseguridad/transacciones2.html

BANCO AV VILLAS. [En línea]. Ingresa a la Banca Virtual. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.avvillas.com.co/bancadigital/inicio

BANCO AV VILLAS. [En línea]. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.avvillas.com.co/wps/wcm/connect/avvillas/b3326505-307e-403c-8c5c-f3e46681eec8/Politica-Proteccion-Datos-Personales-def.pdf?MOD=AJPERES&CVID=m8L62VU#:~:text=El%20Banco%20AV%20Villas%20garantiza,autorizados%20conforme%20a%20la%20ley.

BANCO AV VILLAS. [En línea]. Ser digital es llevar tu oficina en tu bolsillo. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.avvillas.com.co/av-villas-app

BANCO BANCAMÍA. [En línea]. OFICINA VIRTUAL. [Consultado el 12 de mayo de 2022]. Disponible en: https://oficinavirtual.bancamia.com.co/ASPortalFrontWeb/#no-back-button

BANCO BANCAMÍA. [En línea]. POLÍTICA PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancamia.com.co/uploads/default/files/2e94defc2a493a5631d6a1c2a6d89476.pdf

BANCO BANCAMÍA. [En línea]. SERVICIO AL CLIENTE. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancamia.com.co/servicio-clientes

BANCO BANCOLOMBIA. [En línea]. Política para el tratamiento de datos personales de BANCOLOMBIA S.A. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/personas/documentos-legales/proteccion-datos/bancolombia-sa#:~:text=Principios%20Rectores%20del%20Tratamiento%20De%20Datos%20Personales&text=Principio%20de%20libertad%3A%20BANCOLOMBIA%20S.A.,de%20mandato%20legal%20o%20judicial.

BANCO BANCOLOMBIA. [En línea]. Seguridad informática - Protección frente a ataques cibernéticos. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/educacion-financiera/seguridad-bancaria

BANCO BANCOLOMBIA. [En línea]. ¿Cómo activo el ingreso con huella a App Bancolombia? [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/centro-de-ayuda/preguntas-frecuentes/ingreso-con-huella-app-personas

BANCO BANCOLOMBIA. [En línea]. ¿Para qué sirve la Clave Dinámica Bancolombia? [Consultado el 12 de mayo de 2022]. Disponible en:

https://www.bancolombia.com/centro-de-ayuda/preguntas-frecuentes/para-que-sirve-clave-dinamica

BANCO BANCOLOMBIA. [En línea]. App Bancolombia. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/centro-de-ayuda/canales/app-bancolombia

BANCO BANCOLOMBIA. [En línea]. OTP. [Consultado el 12 de mayo de 2022]. Disponible en: https://soportedevs.bancolombia.com/hc/es-419/articles/4542053601556-OTP

BANCO BANCOLOMBIA. [En línea]. Protección de Claves Bancolombia. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/educacion-financiera/seguridad-de-la-informacion/proteccion-claves

BANCO BANCOLOMBIA. [En línea]. Uso de redes sociales en pandemia: la transformación hacia lo digital. [Consultado el 10 de diciembre de 2021]. Disponible en https://www.bancolombia.com/wps/portal/negocios/actualizate/tendencias/uso-redes-sociales-pandemia-transformacion-digital

BANCO BANCOOMEVA. [En línea]. Banca Móvil Bancoomeva A donde vayas, contigo. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancoomeva.com.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=24148

BANCO BANCOOMEVA. [En línea]. Banca móvil. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancoomeva.com.co/publicaciones/163473/banca-movil/

BANCO BANCOOMEVA. [En línea]. Bienvenido -Ingrese sus credenciales para entrar a la oficina virtual. [Consultado el 12 de mayo de 2022]. Disponible en: https://oficinavirtual.bancoomeva.com.co/IB/presentation/bccp_mb/index.htm

BANCO BANCOOMEVA. [En línea]. ¿Qué pasa si la imagen y frase de seguridad que aparecen al momento de ingresar a la Oficina Virtual no son las que asigné durante mi registro? [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancoomeva.com.co/preguntas-frecuentes/122/oficina-virtual/

BANCO BANCOOMEVA. [En línea]. Tips de seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancoomeva.com.co/publicaciones/163467/tips-de-seguridad/

BANCO BBVA COLOMBIA. [En línea]. Política de tratamiento de datos personales. [Consultado el 3 de mayo de 2022]. Disponible en: DO-01-Politica-tratamiento-datos-personales.pdf (bbva.com.co)

BANCO BBVA. [En línea]. ¿Cómo ingresar a BBVA móvil? [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bbva.com.co/personas/preguntas-frecuentes/servicios/digitales/movil/ingresar.html

BANCO BBVA. [En línea]. En tu celular encuentras todo lo que necesitas de tu banco. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bbva.com.co/personas/servicios-digitales/movil.html

BANCO BBVA. [En línea]. Token ¿Qué es y cómo funciona? [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bbva.com.co/personas/blog/educacion-financiera/digital/token.html

BANCO BBVA. [En línea]. Recomendaciones de seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bbva.com.co/personas/recomendaciones-de-seguridad.html

BANCO BTG PACTUAL COLOMBIA. [En línea]. Política para el Tratamiento de Datos Personales. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.btgpactual.com.co/sites/default/files/2022-03/Pol%C3%ADtica%20para%20el%20Tratamiento%20de%20Datos%20Personales%20-%20Banco%20BTG%20Pactual%20Colombia%20S.A.pdf

BANCO BTGPACTUAL. [En línea]. Inicio de sesión. [Consultado el 12 de mayo de 2022]. Disponible en: https://wwws.btgpactual.com.co/Account/Login

BANCO CAJA SOCIAL. [En línea]. Aplicación Móvil. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancocajasocial.com/portalserver/aplicacion-movil

BANCO CAJA SOCIAL. [En línea]. AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: AUTORIZACION-TRATAMIENTO-DATOS-PERSONALES.pdf (bancocajasocial.com)

BANCO CAJA SOCIAL. [En línea]. El portal Internet Empresarial le ofrece más de una solución para hacer del manejo de su empresa algo fácil y seguro. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancocajasocial.com/portalserver/bcs-public/medidas-de-seguridad-para-internet/plataforma-de-seguridad-informatica-usada-por-el-banco

BANCO CAJA SOCIAL. [En línea]. Ingresar. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancocajasocial.com/portalserver/bcs-public/inicio?gclid=EAIaIQobChMIuJ69k-LV-AIVqnxvBB1x9A0XEAAYASAAEgJiL_D_BwE

BANCO CAJA SOCIAL. [En línea]. INSTRUCTIVO RENOVACIÓN TOKEN EMPRESARIAL. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancocajasocial.com/portalserver/content/atom/ed3567c4-64a3-462a-93a4-7c6466ef50e8/content/8-ASSETS-PRODUCTOS/1.Anexos-Descargables/4-Banca-Empresarial/BE-Instructivo_Renovacion_de_Token_Empresarial.pdf?id=8243d0c3-c498-4fcc-9668-63e2fa9adc08

BANCO CAJA SOCIAL. [En línea]. Medidas de Seguridad en el Canal de Internet. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancocajasocial.com/portalserver/medidas-de-seguridad-en-el-canal-de-internet#:~:text=REVISE%20que%2C%20al%20ingresar%20a,computador%20personal%20actualizado%20con%20antivirus.

BANCO CAJA SOCIAL. [En línea]. Nunca está de más tomar la decisión de proteger la información sobre las transacciones de su empresa. Así, para mantener el control y restringir accesos, puede contar con un plan de seguridad que nosotros le ofrecemos. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancocajasocial.com/portalserver/bcs-public/medidas-de-seguridad-para-internet/opciones-de-seguridad-adicionales

BANCO CAJA SOCIAL. [En línea]. PROCESO PARA REALIZAR PAGOS VÍA PSE DESDE COMERCIOS, CON CARGO A RECURSOS EN CUENTAS DE LA BANCA DE PERSONAS. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancocajasocial.com/portalserver/content/atom/ed3567c4-64a3-462a-93a4-7c6466ef50e8/content/14.%20CONTINGENCIA%20COVID%20-19/2.%20Canales%20Digitales/Descargables%20instructivos%20Portal/Realizar%20un%20pago%20v%C3%ADa%20PSE%20internet%20Banca%20Personas.pdf?id=979f3bc9-d3f7-49b4-9d48-2ba351fe34e9

BANCO CITIBANK N.A. [En línea]. CitiDirect. [Consultado el 12 de mayo de 2022]. Disponible en: https://play.google.com/store/apps/details?id=com.citi.mobile.cdbe&hl=es_CO&gl=US

BANCO CITIBANK. [En línea]. Banca Electrónica. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.citibank.com/icg/sa/latam/dominican-republic/digital-banking.html

BANCO CITIBANK. [En línea]. Cash Management - RECOMENDACIONES DE SEGURIDAD. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.citibank.com/icg/sa/latam/colombia/electronic-banking/

BANCO CITIBANK. [En línea]. CitiDirect BE. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.citibank.com/icg/sa/latam/colombia/electronic-banking/citidirect-be.html

BANCO CITIBANK. [En línea]. MisPagosalDia. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.mispagosaldia.com/COGCB/JPS/portal/Index.do

BANCO CITIBANK-COLOMBIA. [En línea]. MANUAL/POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.citibank.com/icg/sa/latam/colombia/institutional-info/assets/docs/Politica-de-tratamiento-de-datos-personales-citibank.pdf

BANCO COOMEVA. [En línea]. Política de protección de datos personales. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.coomeva.com.co/publicaciones/41275/importante-politica-de-proteccion-de-datos-personales/

BANCO COOPCENTRAL. [En línea]. SMISHING. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.coopcentral.com.co/apps_web/portal/pdf/smishing.pdf

BANCO COOPCENTRAL. [En línea]. Banca Móvil App Red Coopcentral. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.coopcentral.com.co/index.asp?id_pagina=304

BANCO COOPCENTRAL. [En línea]. RECOMENDACIONES DE SEGURIDAD: [Consultado el 3 de mayo de 2022]. Disponible en: https://www.coopcentral.com.co/apps_web/portal/natural/pdf/seguridad.pdf

BANCO COOPCENTRAL. [En línea]. SEGURIDAD FUERTE FORTINET. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.coopcentral.com.co/apps_web/juridicos_web/seguridad/seguridad1.php

BANCO COOPERATIVO COOPCENTRAL. [En línea]. PROTECCIÓN DE SUS DATOS PERSONALES EN COOPCENTRAL. [Consultado el 3 de mayo de 2022]. Disponible en: Filef_linka.asp (coopcentral.com.co)

BANCO CREDIFINANCIERA. [En línea]. Manual de Integración. [Consultado el 12 de mayo de 2022]. Disponible en:

https://www.credifinanciera.com.co/sites/default/files/pdf/general/2021-03/MANUAL%20DE%20INTEGRACION%20BCF.pdf

BANCO CREDIFINANCIERA. [En línea]. ¡Cuidado! [Consultado el 12 de mayo de 2022]. Disponible en: https://www.credifinanciera.com.co/recomendaciones-seguridad

BANCO CREDIFINANCIERA. [En línea]. POLÍTICAS PARA EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.credifinanciera.com.co/sites/default/files/pdf_upload/DE-ARI-SIC-001-Politicas-para-el-Tratamiento-y-Proteccion-de-Datos-Personales.pdf

BANCO CREDIFINANCIERA. [En línea]. Te damos la bienvenida a Banco Credifinanciera. [Consultado el 12 de mayo de 2022]. Disponible en: https://sucursalvirtual.credifinanciera.com.co/Administration.WebUI/Pages/General/Login.aspx?ReturnUrl=%2f

BANCO DAVIVIENDA. [En línea]. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: Política de Protección de Datos Personales (corporacionfinancieradavivienda.com)

BANCO DAVIVIENDA. [En línea]. App Davivienda Móvil. [Consultado el 12 de mayo de 2022].Disponible en: https://www.davivienda.com/wps/portal/personas/nuevo/personas/canales_de_atencion/para_todos/app_m%C3%B3vil/!ut/p/z1/jVLBbsIwDP2VcOA0VU5pKeNYEGxCYhWgFpoLCkk6ZWuT0naw_f1caYeNjbJcYjvP9rPzgMEOmOEn_cwbbQ3P0U9ZsPfuV_7TYjJY-tHao-EsmS4Sd-1FKxe2PwGb-RgBS7qZhuPIjR4GwP6TT6-ckN7KTyCdQCpycZecL8n8RrPuXltgnf0i_wbgnl4C_lhIF4DOR1-ADpopjjm6yiH2YHvS6gyxsVWBf7hpK5ZCS0ipJwQd8cxxgyBw_ExQhw_HwsmGh0xy16fiMIBHCotba0dd6JfjkYXAhDWNem9gdxbFXqNdGdXsS1XVqKC6T7XRQts-_R7JWmYYNYTL9hWl1qeC46VqIhXhjTJtGLN4xUljpa2JeVN1U6Ehcq2wD1biZUkk6hXnNZKTwp50DmURx-bDeV3PsuXM81ka9nqfSzWN-w!!/dz/d5/L2dBISEvZ0FBIS9nQSEh/

BANCO DAVIVIENDA. [En línea]. ENCUENTRE TIPS - PARA CUIDAR SUS DATOS E INFORMACIÓN DE CUALQUIER INTENTO DE FRAUDE. [Consultado el 12 de mayo de 2022]. Disponible en: https://comunicaciones.davivienda.com/Tia-segura-tips?utm_source=davivienda.com&utm_medium=selfpromoted&utm_campaign=site-davivienda_slf&utm_content=2021_na_na&utm_term=na

BANCO DAVIVIENDA. [En línea]. Preguntas frecuentes - ¿Qué son los códigos de confirmación? [Consultado el 12 de mayo de 2022]. Disponible en:

https://www.davivienda.com/wps/portal/personas/nuevo/personas/preguntas_frecuentes

BANCO DAVIVIENDA. [En línea]. Seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.davivienda.com/wps/portal/empresas/nuevo/seguridad/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zijS0CTfy8nIx8TQy8zA0cQz0DHEN8vIy9_Yz1w8EKDHAARwP9KGL041EQhd_4cP0oVCucHb2NDBxdXQOCvJ2CjJy8jKEK8JhRkBsaYZDpqAgAbB8RKA!!/dz/d5/L2dBISEvZ0FBIS9nQSEh/

BANCO DE BOGOTÁ. [En línea]. Así funciona el Token de Banco de Bogotá. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/atencion-al-cliente/canales-electronicos/beneficios/token

BANCO DE BOGOTÁ. [En línea]. Banca Móvil - SMS. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/atencion-al-cliente/canales-electronicos/canales/banca-movil-sms#tab-2

BANCO DE BOGOTÁ. [En línea]. Banca Móvil APP. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/atencion-al-cliente/canales-electronicos/canales/bancamovil

BANCO DE BOGOTÁ. [En línea]. Ingreso a Transacciones - Esta pantalla le permite ingresar sus datos para realizar transacciones por Internet. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodebogota.com/Banking/pb/logon?a=00010016&pbold=true

BANCO DE BOGOTÁ. [En línea]. Seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/atencion-al-cliente/seguridad-bancaria

BANCO DE BOGOTÁ. [En línea]. Términos y Condiciones Política de Tratamiento de Datos. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancodebogota.com/wps/themes/html/banco-de-bogota/pdf/atencion-al-cliente/terminos-y-condiciones-politica-tratamiento-datos.pdf

BANCO DE OCCIDENTE. [En línea]. Banco de Occidente Móvil. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodeoccidente.com.co/banco-de-occidente/landing/banca-movil/

BANCO DE OCCIDENTE. [En línea]. Conoce nuestras herramientas de autenticación. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodeoccidente.com.co/wps/portal/banco-de-

occidente/bancodeoccidente/canales-servicios/seguridad-en-canales/seguridad-en-banco-de-occidente

BANCO DE OCCIDENTE. [En línea]. Portal Transaccional Banca Personas. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodeoccidente.com.co/wps/portal/banco-de-occidente/bancodeoccidente/canales-servicios/canales-y-transacciones-para-personas/portal-transaccional

BANCO DE OCCIDENTE. [En línea]. Recomendaciones de seguridad con tus productos financieros. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodeoccidente.com.co/wps/portal/banco-de-occidente/bancodeoccidente/footer/otros/educacion-financiera/manejo-de-canales-eletronicos/recomendaciones-canales-electronicos

BANCO DE OCCIDENTE. [En línea]. POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: politicas-de-tratamiento-de-datos-personales.pdf (bancodeoccidente.com.co)

BANCO FALABELLA. [En línea]. BANCA EN LÍNEA. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancofalabella.com.co/cmr-banco-falabella?cmrkeywords=&gclid=EAIaIQobChMIsKCP3MyC-AIVCvSzCh3qIAE6EAAYASAAEgI8gvD_BwE&gclsrc=aw.ds

BANCO FALABELLA. [En línea]. Banco Falabella Colombia. [Consultado el 12 de mayo de 2022]. Disponible en: https://play.google.com/store/apps/details?id=co.com.bancofalabella.mobile.omc&hl=es_CO&gl=US

BANCO FALABELLA. [En línea]. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DE BANCO FALABELLA. [Consultado el 3 de mayo de 2022]. Disponible en: https://assets.ctfassets.net/ex6ts2p2j0ib/5PQItRWGp9i9srvsEUFpP0/7811c5e18ba875bb896cf23aa0181020/BFCO.PE.PO.2.PL.33_Poli__tica_de_Tratamiento_de_Datos_Personales.pdf

BANCO FALABELLA. [En línea]. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL SITIO WEB. [Consultado el 3 de mayo de 2022]. Disponible en: https://assets.ctfassets.net/ex6ts2p2j0ib/4CP5iGur6dJLbjce5PtIKs/a57472dcddfe2832bf9d25818c09fd85/PROCURADURIA-POLITICAS.pdf

BANCO FINANDINA. [En línea]. ¡Bienvenido a tu Banca Digital! [Consultado el 12 de mayo de 2022]. Disponible en: https://transacciones.bancofinandina.com/BP/login

BANCO FINANDINA. [En línea]. Beneficios. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancofinandina.com/docs/default-source/empresas/instructivo-token.pdf

BANCO FINANDINA. [En línea]. Libérate de tanto papeleo. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancofinandina.com/

BANCO FINANDINA. [En línea]. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES Y TRATAMIENTO DE DATOS DEL BANCO FINANDINA S.A. [Consultado el 3 de mayo de 2022]. Disponible en: politica-tratamiento-de-datos-banco-finandina-2020-i.pdf

BANCO FINANDINA. [En línea]. Recomendaciones de seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancofinandina.com/servicio-al-cliente/educacion-y-consumidor-financiero/recomendaciones-de-seguridad/

BANCO FINANDINA. [En línea]. Token Banco Finandina. [Consultado el 12 de mayo de 2022]. Disponible en: https://appagg.com/android/finance/token-banco-finandina-33419303.html?hl=en

BANCO GNB SUDAMERIS. [En línea]. POLÍTICAS Y LINEAMIENTOS GENERALES DE TRATAMIENTO DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: Politicas_Lineamientos_Generales_Proteccion_Datos_Personales_19092014.pdf (gnbsudameris.com.co)

BANCO INTERAMERICANO DE DESARROLLO. [En línea]. Regulación de blockchain e identidad digital en América Latina | El futuro de la identidad digital. [Consultado:12 de mayo de 2022]. Disponible en: https://publications.iadb.org/publications/spanish/document/Regulacion-de-blockchain-e-identidad-digital-en-America-Latina-El-futuro-de-la-identidad-digital.pdf

BANCO ITAÚ CORPBANCA COLOMBIA. [En línea]. POLÍTICAS DE TRATAMIENTO DE LA INFORMACIÓN. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.itau.co/documents/10282/1023825/Manual_Politicas_y_procedimientos_datos_personales_Itau_281221.pdf

BANCO ITAÚ. [En línea]. Cuenta Básica. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itau.co/personal/cuentas/cuenta-basica

BANCO ITAÚ. [En línea]. Más seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.itau.co/comun/mas-seguridad

BANCO ITAÚ. [En línea]. Personas. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itau.co/index

BANCO ITAÚ. [En línea]. Uso Obligatorio de Token. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itau.co/empresas/pagos/uso-obligatorio-de-token

BANCO J.P. MORGAN COLOMBIA. [En línea]. J.P. Morgan Access® Credential Services User Guide. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.jpmorgan.com/content/dam/jpm/ts-change-readiness/documents/JP_Morgan_Access_-_Credential_Services_User_Guide_-_2020-04-14.pdf

BANCO J.P. MORGAN COLOMBIA. [En línea]. Cybersecurity Awareness. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.jpmorgan.com/wealth-management/wealth-partners/cybersecurity-awareness

BANCO J.P. MORGAN COLOMBIA. [En línea]. Manténgase informado con sus inversiones online. [Consultado el 12 de mayo de 2022]. Disponible en: https://privatebank.jpmorgan.com/gl/es-es/services/banking/digital-capabilities/digital-capabilities-for-non-u-s--clients

BANCO J.P. MORGAN COLOMBIA. [En línea]. Welcome to Morgan Money. [Consultado el 12 de mayo de 2022]. Disponible en: https://smuauth.jpmorgan.com/smuSSWeb/logonController.do?appName=GCP&clientName=AM2&TYPE=33554433&REALMOID=06-0000a07d-b2f0-1c01-8584-a51ba9605a5a&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=ag_gcpam2&TARGET=SMhttps%3a%2f%2fgcp2%2ejpmorgan%2ecom%2fgcp2%2fstart

BANCO J.P. MORGAN COLOMBIA. [En línea]. Lineamientos Generales del Tratamiento de la Información y Datos Personales. [Consultado el 3 de mayo de 2022]. Disponible en: colombia-tratamiento-de-información-y-datos-personales.pdf (jpmorgan.com)

BANCO LULO BANK. [En línea]. Política de tratamiento de Datos personales. [Consultado el 3 de mayo de 2022]. Disponible en: Política de tratamiento de Datos Personales (lulo-cms-assets-wpprod.s3.amazonaws.com)

BANCO LULO BANK. [En línea]. ¿Cuáles son las características de la contraseña? [Consultado el 12 de mayo de 2022]. Disponible en: https://ayuda.lulobank.com/hc/es/articles/4403995899796--Cu%C3%A1les-son-las-caracter%C3%ADsticas-de-la-contrase%C3%B1a-

BANCO LULO BANK. [En línea]. ¿Dónde puedo actualizar mi correo electrónico? [Consultado el 12 de mayo de 2022]. Disponible en: https://ayuda.lulobank.com/hc/es/articles/4403995755284--D%C3%B3nde-puedo-actualizar-mi-correo-electr%C3%B3nico-

BANCO LULO BANK. [En línea]. Código de autenticación o verificación. [Consultado el 12 de mayo de 2022]. Disponible en: https://ayuda.lulobank.com/hc/es/sections/4403981060116-C%C3%B3digo-de-autenticaci%C3%B3n-o-verificaci%C3%B3n

BANCO LULO BANK. [En línea]. Ten en cuenta estos tips de seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.lulobank.com/tips-de-seguridad

BANCO LULO BANK. [En línea]. Un banco que llevas en tu bolsillo. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.lulobank.com/features/usa-tu-app

BANCO MIBANCO. [En línea]. Iniciar sesión. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.serviciosempresariales.mibanco.com.co/webclient/Login.xhtml

BANCO MIBANCO. [En línea]. Seguridad bancaria. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.mibanco.com.co/#!seguridad-bancaria

BANCO MIBANCO. [En línea]. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.mibanco.com.co/upload/pdf/quienes-somos/2.POLIITICAS-PARA-TRATAMIENTO-DE-LA-INFORMACION-13042015.pdf

BANCO MUNDO MUJER. [En línea]. Política de Protección de Datos Personales. [Consultado el 12 de mayo de 2022]. Disponible en: Política de Protección de Datos Personales | Banco Mundo Mujer (bmm.com.co)

BANCO MUNDO MUJER. [En línea]. Porque valoramos su tiempo y queremos que lo disfrute - la APP del Banco Mundo Mujer llega para darle la mano. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bmm.com.co/app-movil.html

BANCO MUNDO MUJER. [En línea]. SEGURIDAD BANCARIA. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bmm.com.co/seguridad-bancaria.html

BANCO PICHINCHA. [En línea]. MANUAL REGULATORIO POLÍTICA PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en:

https://www.bancopichincha.com.co/documents/158147/641503/Política+Protección+de+Datos+Personales.pdf/c4ddb5f4-12d3-1de4-e867-b4863d46cf2a?t=1642447325723

BANCO PICHINCHA. [En línea]. EMPRESAS - Banca Electrónica.2020. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.pichincha.com/portal/Portals/0/manuales/InstructivoAutogestionToken.pdf?ver=2021-01-14-134250-533

BANCO PICHINCHA. [En línea]. Tutoriales del Portal Transaccional. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancopichincha.com.co/documents/158126/271185/Manual+Transacciones+banco+pichincha.pdf/62d9843b-63cd-009b-4293-facdb87805e9?t=1637337751680

BANCO PICHINCHA. [En línea]. Recomendaciones de Seguridad -Entérese de cómo protegerse de los ataques informáticos. [Consultado el 3 de mayo de 2022]. Disponible en: https://bancopichincha.com.co/documents/158147/260656/Recomendaciones+de+seguridad.pdf/3349b4ce-c650-c401-de75-d104ad94d7bb?t=1565277047750

BANCO PICHINCHA. [En línea]. Soluciones que optimizan su tiempo - Banca Virtual. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancopichincha.com.co/web/empresas/banca-virtual-aplicacion-movil

BANCO POPULAR. [En línea]. CAMBIA TU CONTRASEÑA DE FORMA SEGURA. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancopopular.com.co/wps/wcm/connect/bancopopular/1a16126e-1516-4d54-8f1c-a67b6a2c297f/Cambio+Contrasena+copy.pdf?MOD=AJPERES&CVID=nxbliNt

BANCO POPULAR. [En línea]. Recomendaciones de Seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancopopular.com.co/wps/portal/bancopopular/inicio/informacion-interes/recomendaciones-seguridad

BANCO POPULAR. [En línea]. Recuerda que debes tener estas recomendaciones para poder acceder a tu Banca Móvil en Banco Popular. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancopopular.com.co/wps/portal/bancopopular/inicio/canales-atencion-servicio/app-banca-movil/

BANCO POPULAR. [En línea]. Recuerda que debes tener estas recomendaciones para poder acceder a tu Portal transaccional en Banco Popular. [Consultado el 12 de mayo de 2022]. Disponible en:

https://www.bancopopular.com.co/wps/portal/bancopopular/inicio/canales-atencion-servicio/internet-persona-natural/

BANCO POPULAR. [En línea]. Tratamiento de Datos Personales. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancopopular.com.co/wps/portal/bancopopular/inicio/informacion-interes/tratamiento-datos-personales

BANCO SANTANDER DE NEGOCIOS COLOMBIA. [En línea]. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES ADOPTADA POR EL BANCO SANTANDER DE NEGOCIOS COLOMBIA S.A. [Consultado el 3 de mayo de 2022]. Disponible en: Normativo (santander.com.co)

BANCO SANTANDER. [En línea]. CONTRATO DE SERVICIOS DE SUPERNET. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.santander.com.co/recursos/archivos/reglamento-super-net.pdf

BANCO SANTANDER. [En línea]. Nuestros 5 consejos de seguridad online. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.santander.com.co/pg/5-consejos-de-seguridad-online.html

BANCO SANTANDER. [En línea]. SuperNet. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.santander.com.co/pg/supernet.html

BANCO SCOTIABANK COLPATRIA. [En línea]. Política de Tratamiento de Datos Personales Clientes y Posibles Clientes. [Consultado el 3 de mayo de 2022]. Disponible en: Politica-de-tratamiento-de-datos-Red-Scotiabank.pdf (azureedge.net)

BANCO SCOTIABANK COLPATRIA. [En línea]. ¿Cuáles son las modalidades de fraude? [Consultado el 12 de mayo de 2022]. Disponible en: https://www.scotiabankcolpatria.com/seguridad-bancaria

BANCO SCOTIABANK COLPATRIA. [En línea]. Cómo recuperar el usuario y la contraseña para el ingreso a la Banca Virtual: [Consultado el 12 de mayo de 2022]. Disponible en: https://www.scotiabankcolpatria.com/canales-digitales/web/cambio-de-clave

BANCO SCOTIABANK COLPATRIA. [En línea]. Genera tu código PIN y retira dinero sin necesidad de tu tarjeta. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.scotiabankcolpatria.com/canales-digitales/retiros-con-pin

BANCO SCOTIABANK COLPATRIA. [En línea]. Nueva App Scotiabank Colpatria. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.scotiabankcolpatria.com/canales-

digitales/app?_branch_match_id=1053077692611059297&utm_medium=marketing&_branch_referrer=H4sIAAAAAAAAA8soKSkottLXL07OL8lMTErMy07OzylILCnKTNRLLCjQy8nMy9ZPtPR2NA1zCckwBACfLT13LwAAAA%3D%3D

BANCO SERFINANZA. [En línea]. CONTRATO DE USO Y REGLAMENTO SERFINANZA VIRTUAL EMPRESAS. [Consultado el 3 de mayo de 2022]. Disponible en: https://bancoserfinanza.com/wp-content/uploads/2020/07/Contrato-de-Uso-y-Reglamento-Serfinanza-Virtual-Empresas.pdf

BANCO SERFINANZA. [En línea]. MANUAL DE USO BANCO SERFINANZA SERFINANZA MÓVIL PERSONAS. [Consultado el 3 de mayo de 2022]. Disponible en: https://bancoserfinanza.com/wp-content/uploads/2019/05/MANUAL-DE-USO-SERFINANZA-MOVIL.pdf

BANCO SERFINANZA. [En línea]. MANUAL DE USO SERFINANZA VIRTUAL - PERSONAS. [Consultado el 3 de mayo de 2022]. Disponible en: https://bancoserfinanza.com/wp-content/uploads/2019/05/MANUAL-USO-SERFINANZA-VIRTUAL-PERSONAS.pdf

BANCO SERFINANZA. [En línea]. Política De Protección De Datos Personales. [Consultado el 12 de mayo de 2022]. Disponible en: Política de protección de datos personales - Banco Serfinanza

BANCO SERFINANZA. [En línea]. Seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://bancoserfinanza.com/servicio-al-cliente/seguridad-de-la-informacion/

BANCO SUDAMERIS. [En línea]. Banca Móvil. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.gnbsudameris.com.co/personas/servicios/banca-movil

BANCO SUDAMERIS. [En línea]. Formas frecuentes para iniciar el fraude. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.gnbsudameris.com.co/guia-practica-de-seguridad/canales

BANCO SUDAMERIS. [En línea]. Herramientas de Seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.gnbsudameris.com.co/guia-practica-de-seguridad/herramientas-de-seguridad

BANCO SUDAMERIS. [En línea]. ¡Su TOKEN DIGITAL es práctico y seguro! [Consultado el 12 de mayo de 2022]. Disponible en: https://www.gnbsudameris.com.co/personas/servicios/token-digital

BANCO W. [En línea]. IN F O R M E D E GESTIÓN 2019. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancow.com.co/wp-content/uploads/2021/03/2.-Informe-de-Gestion-2019.pdf

BANCO W. [En línea]. Banca telefónica - Recomendaciones de seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancow.com.co/canales-de-servicio/banca-telefonica/

BANCO W. [En línea]. Consultas y transacciones por la Línea de Servicio Transaccional. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancow.com.co/consultas-y-transacciones-por-la-banca-telefonica/?lang=en

BANCO W. [En línea]. FINALIDADES DE BASES DE DATOS. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancow.com.co/wp-content/uploads/2021/07/ANX-GDR-023-FINALIDADES-BASES-DE-DATOS-.pdf

BEEDIGITAL. [En línea]. ¿Qué es un token y para qué sirve? [Consultado el 12 de mayo de 2022]. Disponible en: https://www.beedigital.es/tendencias-digitales/que-es-un-token-y-para-que-sirve/

CNDH MÉXICO. [En línea]. El derecho a la identidad de las personas y los pueblos indígenas. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.cndh.org.mx/documento/el-derecho-la-identidad-de-las-personas-y-los-pueblos-indigenas#:~:text=El%20derecho%20a%20la%20identidad%20de%20la%20persona%20y%20su,digna%20y%20a%20tener%20sus%20propias

CONGRESO DE LA REPÚBLICA DE COLOMBIA. [En línea]. LEY 1098 DE 2006, Por la cual se expide el Código de la Infancia y la Adolescencia. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1098_2006.htm#25

CONGRESO DE LA REPÚBLICA DE COLOMBIA. [En línea]. LEY 39 DE 1961, Por la cual se dictan normas para la cedulación, y otras de carácter electoral. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/ley_0039_1961.htm#:~:text=ART%C3%8DCULO%201o.,%2C%20pol%C3%ADticos%2C%20administrativos%20y%20judiciales.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. [En línea]. LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CONSTITUCIÓN POLÍTICA DE COLOMBIA. [En línea]. Artículo 15. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

CONSTITUCIÓN POLÍTICA DE COLOMBIA. [En línea]. Artículo 266. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.constitucioncolombia.com/titulo-9/capitulo-2/articulo-266

CSIRT FINANCIERO. [En línea]. Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. [Consultado: 6 de febrero de 2022]. Disponible en: https://csirtasobancaria.com/sala-de-prensa/201cdesafios-del-riesgo-cibernetico-en-el-sector-financiero-para-colombia-y-america-latina201d-publicacion-conjunta-entre-asobancaria-y-la-organizacion-de-estados-americanos-oea

EASYDMARC. [En línea]. Whaling: ¿cómo funciona este ataque y cómo podemos evitarlo? [Consultado el 10 de diciembre de 2021]. Disponible en: https://easydmarc.com/blog/es/whaling-como-funciona-este-ataque-y-como-podemos-evitarlo/

EL TIEMPO. [En línea]. La apuesta tecnológica del Banco de Bogotá para mejorar su seguridad. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.eltiempo.com/economia/sector-financiero/reconocimiento-facial-la-apuesta-tecnologica-del-banco-de-bogota-577947

ESPAÑA DIGITAL. [En línea]. IDENTIDAD DIGITAL: EL NUEVO USUARIO EN EL MUNDO DIGITAL. [Consultado: 10 de diciembre de 2021]. Disponible en: https://publiadmin.fundaciontelefonica.com/media/es/que_hacemos/media/publicaciones/identidad_digital.pdf?

GOBIERNO DE COLOMBIA, FUNCIÓN PUBLICA. [En línea]. Ley 1581 de 2012. [Consultado: 10 de diciembre de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=La%20presente%20ley%20tiene%20por,el%20art%C3%ADculo%2015%20de%20la

GOBIERNO DE ESPAÑA, AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO. [En línea]. REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. [Consultado: 6 de febrero de 2022]. Disponible en: https://www.boe.es/doue/2014/257/L00073-00114.pdf

GOBIERNO DE ESPAÑA, MINISTERIO DE EDUCACIÓN CULTURA Y DEPORTE. [En línea]. Introducción a la seguridad informática - Mecanismos básicos de seguridad. [Consultado el 10 de diciembre de 2021]. Disponible en:

http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=2

INTER -AMERICAN DEVELOPMENT BANK. [En línea]. IDENTIDAD DIGITAL AUTOGESTIONADA El futuro de la identidad digital: autogestión, billeteras digitales y blockchain. [Consultado: 10 de diciembre de 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf

ISO. [En línea]. ISISO/IEC 24760-1:2019(en) IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en

ISO. [En línea].ISO/IEC 24760-2:2015(en) Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-2:ed-1:v1:en

ISO. [En línea].ISO/IEC 24760-3:2016(en) Information technology — Security techniques — A framework for identity management — Part 3: Practice. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-3:ed-1:v1:en

ITU. [En línea].
X.1251: Marco para el control por el usuario de la identidad digital. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itu.int/rec/T-REC-X.1251/es

ITU. [En línea]. X.253: Directrices de seguridad para los sistemas de gestión de identidades. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itu.int/rec/T-REC-X.1253-201109-I/es

ITU. [En línea]. X1254: Marco de garantía de autenticación de entidad. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itu.int/rec/T-REC-X.1254/es

NIST. [En línea]. Digital Identity Guidelines. [Consultado el 10 de diciembre de 2021]. Disponible en: https://pages.nist.gov/800-63-3/

OKTA. [En línea]. What is Decentralized Identity? [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.okta.com/blog/2021/01/what-is-decentralized-identity/

OMS. [En línea]. COVID-19: cronología de la actuación de la OMS. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.who.int/es/news/item/27-04-2020-who-timeline---covid-19

ONESPAN. [En línea]. Autenticación fuerte. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.onespan.com/es/topics/autenticacion-fuerte#:~:text=%C2%BFQu%C3%A9%20es%20la%20autenticaci%C3%B3n%20fuerte,y%20la%20autorizaci%C3%B3n%20de%20transacciones.

ORGANIZACIÓN DE ESTADOS AMERICANOS. [En línea]. Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. [Consultado: 10 de diciembre de 2021]. Disponible en: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

PORTAFOLIO. [En línea]. redes-sociales-pandemia-transformacion-digital. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.portafolio.co/economia/finanzas/bancarizacion-e-inclusion-lo-bueno-que-deja-la-pandemia-549749

REAL ACADEMIA ESPAÑOLA. [En línea]. Diccionario de la lengua española. [Consultado el 10 de diciembre de 2021]. Disponible en: https://dle.rae.es/identidad

RZ. [En línea]. Aprende cómo funciona el protocolo SMTP para correo saliente. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.redeszone.net/tutoriales/internet/que-es-protocolo-smtp-email-configuracion/

RZ. [En línea]. Qué significa autenticación y la autorización. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/

SENDINBLUE. [En línea]. Información sobre la autenticación de dominios (DKIM, SPF). [Consultado el 10 de diciembre de 2021]. Disponible en: https://help.sendinblue.com/hc/es/articles/209577385-Informaci%C3%B3n-sobre-la-autenticaci%C3%B3n-de-dominios-DKIM-SPF-

SUPERINTENDENCIA FINANCIERA DE COLOMBA. [En línea]. Circulares Externas. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/circulares-externas--10082461

SUPERINTENDENCIA FINANCIERA DE COLOMBA. [En línea]. Datos Estadísticos - Cifras, Información estadística - Anual. [Consultado el 8 de junio de

2022]. Disponible en: https://www.superfinanciera.gov.co/inicio/consumidor-financiero/informacion-general/quejas-contra-entidades-vigiladas/datos-estadisticos-cifras/informacion-estadistica-anual-11129

SURIAGA SANCHEZ, Marco Antonio BONILLA FREIRE, Janet SANCHEZ PARRALES, Luis Albert. [En línea]. Banca electrónica. En:.CE Revista Contribuciones a la Economía, enero-marzo de 2016. [Consultado: 6 de febrero de 2022]. Disponible en;.http://eumed.net/ce/2016/1/banca.html.ISSN: 1696-8360

UNICEF COMITÉ ESPAÑOL. [En línea]. CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO. [Consultado: 3 de julio de 2022]. Disponible en: https://www.un.org/es/events/childrenday/pdf/derechos.pdf

VELÁSQUEZ, Ignacio. [En línea]. Chillan, Chile. 2017.87 p. Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor. Universidad del Bío-Bío. Facultad de Ciencias Empresariales Departamento de Ciencias de la Computación y Tecnologías de la Información. [Consultado el 3 de mayo de 2022]. Disponible en: .http://mcc.ubiobio.cl/docs/tesis/ignacio_andr%C3%A9s_vel%C3%A1squez_lagos_-2017_velasquez_lagos_ignacio.pdf

VMWARE END-USER COMPUTING. [En línea]. Identity and Access Management: Technical Overview. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.youtube.com/watch?v=Tcvsefz5DmA

XATAKA. [En línea]. NFC: qué es y para qué sirve en este 2022. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.xataka.com/moviles/nfc-que-es-y-para-que-sirve

10. ANEXOS

Anexo A. Listado establecimientos bancarios de Colombia vigentes a marzo de 2022 según la Superintendencia Financiera

Código	Denominación social de la Entidad	Página Web
1	Banco de Bogotá	www.bancodebogota.com.co
2	Banco Popular S.A.	www.bancopopular.com.co
6	ITAÚ CORPBANCA COLOMBIA S.A. podrá utilizar cualquiera de las siguientes siglas ITAÚ; BANCO CORPBANCA; o CORPBANCA	Notificaciones.juridico@itau.co www.bancocorpbanca.com.co
7	Bancolombia S.A. o Banco de Colombia S.A. o Bancolombia	gciari@bancolombia.com.co www.bancolombia.com.co
9	Citibank-Colombia - Expresión Citibank	legalnotificaciones@citi.com www.citibank.com.co
12	BANCO GNB SUDAMERIS S.A. Quien podrá utilizar el nombre BANCO GNB SUDAMERIS o SUDAMERIS, seguidos o no de las expresiones sociedad anónima o la sigla S.A.	www.gnbsudameris.com.co jecortes@gnbsudameris.com.co
13	Banco Bilbao Vizcaya Argentaria Colombia S.A. podrá utilizar el nombre BBVA Colombia (Antes Banco Ganadero S.A. o BBVA Banco Ganadero)	notifica.co@bbva.com www.bbva.com.co
23	Banco de Occidente S.A.	djuridica@bancodeoccidente.com.co www.bancodeoccidente.com.co
30	BANCO CAJA SOCIAL S.A. Y podrá usar el nombre BANCO CAJA SOCIAL	contactenos@bancocajasocial.com www.bancocajasocial.com
39	Banco Davivienda S.A. "Banco Davivienda" o "Davivienda"	notificacionesjudiciales@davivienda.com www.davivienda.com
42	SCOTIABANK COLPATRIA S.A.	www.scotiabankcolpatria.com notificbancolpatria@colpatria.com
43	Banco Agrario de Colombia S.A. -Banagrario-	attnclie@bancoagrario.gov.co www.bancoagrario.gov.co

49	Banco Comercial AV Villas S.A. o Banco de Ahorro y Vivienda AV Villas, Banco AV Villas o AV Villas	angeljc@bancoavvillas.com.co NotificacionesJudiciales@bancoavvillas.com.co NotificacionesComerciales@bancoavvillas.com.co www.avvillas.com.co
51	BANCO CREDIFINANCIERA S.A. pudiendo utilizar indistintamente y para todos los efectos legales los nombres "CREDIFINANCIERA S.A.." y "CREDIFINANCIERA" (la "Sociedad")	impuestos@credifinanciera.com.co www.bancoprocredit.com.co
52	Banco de las Microfinanzas -Bancamía S.A.	servicioalclientes@bancamia.com.co www.bancamia.com.co
53	Banco W S.A.	correspondenciabancow@bancow.com.co www.bancow.com.co
54	Banco Coomeva S.A. - Sigla "BANCOOMEVA"	notificacionesfinanciera@coomeva.com.co 1-54_bancoomeva@coomeva.com.co www.coomeva.com.co
55	Banco Finandina S.A. o Finandina Establecimiento Bancario, pero podrá identificarse simplemente con la sigla Finandina Bic o Banco Finandina Bic o Finandina.	gerenciageneral@bancofinandina.com www.finandina.com
56	Banco Falabella S.A.	CumplimientoNormativo@bancofalabella.com.co www.bancofalabella.com.co
57	Banco Pichincha S.A.	notificacionesjudiciales@pichincha.com.co embargosBPichincha@pichincha.com.co www.bancopichincha.com.co
58	El Banco Cooperativo Coopcentral Sigla: COOPCENTRAL	Coopcentral@coopcentral.com.co www.coopcentral.com.co
59	BANCO SANTANDER DE NEGOCIOS COLOMBIA S. A	notificaciones@santander.com.co www.santander.com.co
60	"BANCO MUNDO MUJER S.A." Denominación de "MUNDO MUJER EL BANCO DE LA COMUNIDAD " o "MUNDO MUJER"	cumplimiento.normativo@bmm.com.co www.bmm.com.co
62	Banco de la Microempresa de Colombia S.A. Sigla: "Mibanco S.A."	notificaciones@bancompartir.co

63	BANCO SERFINANZA S.A.	hyunis@serfinansa.com.co aartela@serfinansa.com.co www.serfinansa.com.co
64	BANCO J.P. MORGAN COLOMBIA S.A., (la "Sociedad")	
65	Lulo Bank S.A.	contacto@lulobank.com
66	Banco BTG Pactual Colombia S.A.	sh-legal-colombia@btgpactual.com

Anexo B. Listado de establecimientos bancarios con vínculo de sección de seguridad en la página web principal

Banco	En home?
BANCO BOGOTÁ	Si
BANCO POPULAR	Si
BANCO ITAÚ	Si
BANCO SUDAMERIS	Si
BANCO BBVA	Si
BANCO DAVIVIENDA	Si
BANCO SCOTIABANK COLPATRIA	Si
BANCO AGRARIO	Si
BANCO AV VILLAS	Si
BANCO CREDIFINANCIERA.	Si
BANCO FALABELLA	Si
BANCO PICHINCHA	Si
BANCO COOPCENTRAL	Si
BANCO SANTANDER	Si
BANCO MUNDO MUJER	Si
BANCO MIBANCO	Si
BANCO SERFINANZA	Si

Anexo C. Listado de establecimientos bancarios con vínculo de Políticas de tratamiento de datos personales en la página web principal

Banco	En home?
BANCO AV VILLAS	SI
BANCO POPULAR	SI
BANCO ITAÚ	SI
BANCO BANCOLOMBIA	SI
BANCO SCOTIABANK	SI
BANCO CREDIFINANCIERA	SI
BANCO COOMEVA	SI
BANCO FINANDINA	SI
BANCO FALABELLA	SI
BANCO PICHINCHA	SI
BANCO COOPCENTRAL	SI
BANCO LULO BANK	SI
BANCO BTG PACTUAL COLOMBIA	SI
BANCO AGRARIO	SI

Anexo D. Matriz de publicaciones de seguridad desplegados en los sitios web de los establecimientos bancarios de Colombia, por amenaza

Banco	Phishing X Correo Electrónico	Programas maliciosos -malware(*)	Ingeniería Social	Skimming	Vishing /
BOGOTÁ	Informa	Informa	Informa	Informa	Informa
	Recomienda	Recomienda	Recomienda	Recomienda	Recomienda
	Publica nombres de cuentas de correo desde donde el banco envía correos				Publica número telefónico oficial (WA) desde donde el banco se comunica
POPULAR	Informa		Informa	Informa	Informa
	Recomienda		Recomienda	Recomienda	Recomienda
ITAÚ	Informa				
	Recomienda	Recomienda	Informa		
	Publica nombre de cuenta de correo del banco para reenvío de correos		Recomienda		

	fraudulentos llegados a clientes				
BANCOLOMBIA		Informa			
		Recomienda			
CITIBANK-COLOMBIA	Recomienda	Recomienda			
SUDAMERIS	Informa	Informa	Informa		
	Recomienda	Recomienda	Recomienda		
BBVA COLOMBIA	Informa		Informa		Informa
	Recomienda		Recomienda		Recomienda
OCCIDENTE	Recomienda		Recomienda		
CAJA SOCIAL	Informa		Informa		
	Recomienda		Recomienda		
DAVIVIENDA	Informa	suministra software para prevenir amenazas de fraudes a través de modalidades como Malware, Phishing y Pharming			Informa
	Recomienda				Recomienda
	suministra software para prevenir amenazas de fraudes a través de modalidades como Malware, Phishing y Pharming				
	Publica número para denuncias				Publica número para denuncias

SCOTIABANK COLPATRIA S.A.	Informa	Informa	Informa	Informa	Informa
	Recomienda	Recomienda	Recomienda	Recomienda	Recomienda
BANCO AGRARIO		Recomienda	Recomienda		
AV VILLAS	Informa		Recomienda	Recomienda	
	Recomienda				
	Publica nombres de cuentas de correo desde donde el banco envía correos				
CREDIFINANCIERA	Informa	Informa	Informa	Informa	Informa
	Recomienda	Recomienda	Recomienda	Recomienda	Recomienda
	Publica correo para reporte de incidencias				
BANCAMÍA	Informa	Informa	Informa	Informa	Informa
	Recomienda	Recomienda	Recomienda	Recomienda	Recomienda
	Publica correo para reporte de incidencias	Publica correo para reporte de incidencias		Publica correo para reporte de incidencias	Publica correo para reporte de incidencias
W (*)					
COOMEVA	Recomienda	Recomienda		Recomienda	
FINANDINA	Recomienda		Recomienda		
FALABELLA	Recomienda	Recomienda			
PICHINCHA COLOMBIA	Informa	Informa	Informa	Informa	Informa

	Recomienda	Recomienda	Recomienda	Recomienda	Recomienda
COOPCENTRAL	Publica correo para reporte de incidencias				
	Recomienda	Recomienda			
SANTANDER COLOMBIA	Informa	Informa	Informa		Informa
	Recomienda	Recomienda	Recomienda		Recomienda
MUNDO MUJER	Informa	Informa	Informa	Informa	Informa
	Recomienda	Recomienda	Recomienda	Recomienda	Recomienda
MIBANCO				Informa	
				Recomienda	
SERFINANZA	Publica nombres de cuentas de correo desde donde el banco envía correos	Recomienda	Recomienda		Recomienda
	Recomienda				
	Publica correo para reporte de incidencias				
J.P. MORGAN COLOMBIA	Recomienda	Recomienda			
LULO BANK	Publica nombres de cuentas de correo desde donde el banco envía correos				Publica número telefónico oficial (WA) desde donde el banco se comunica
	Recomienda				Recomienda
BTG PACTUAL COLOMBIA	No se encontró				

Banco	Smishing	Cambiazo	Fharming	Sim Swapping:	Whaling
BOGOTÁ	Informa				
	Recomienda				
	Publica códigos oficiales desde donde el banco envía notificaciones y SMSs				
POPULAR	Informa	Informa	Informa	Informa	
	Recomienda	Recomienda	Recomienda	Recomienda	
ITAÚ					
		Informa			
		Recomienda			
BANCOLOMBIA	Recomienda				

CITIBANK-COLOMBIA					
SUDAMERIS				Informa	
				Recomienda	
BBVA COLOMBIA	Informa	Informa			
	Recomienda	Recomienda			
OCCIDENTE					
CAJA SOCIAL	Informa				
	Recomienda				
DAVIVIENDA	Informa				
	Recomienda				
			suministra software para prevenir amenazas de fraudes a través de modalidades como Malware, Phishing y Pharming		
	Publica número para denuncias				
SCOTIABANK COLPATRIA S.A.	Informa	Informa		Informa	
	Recomienda	Recomienda		Recomienda	
	Publica número telefónico para denuncias				
	Publica correo para reporte de incidencias				
BANCO AGRARIO					
AV VILLAS	Informa	Recomienda			
	Recomienda				

	Publica códigos oficiales desde donde el banco envía notificaciones y SMSs				
CREDIFINANCIERA	Informa	Informa			
	Recomienda	Recomienda			
	Publica correo para reporte de incidencias				
BANCAMÍA	Informa	Informa			
	Recomienda	Recomienda			
	Publica correo para reporte de incidencias	Publica correo para reporte de incidencias			
W (*)	Recomienda				
	Publica códigos oficiales desde donde el banco envía notificaciones y SMSs				
COOMEVA	Recomienda				
FINANDINA	Publica códigos oficiales desde donde el banco envía notificaciones y SMSs	Recomienda			
	Recomienda				
FALABELLA	Recomienda				
PICHINCHA COLOMBIA	Informa	Informa	Informa		Informa
	Recomienda	Recomienda	Recomienda		Recomienda
COOPCENTRAL					

	Recomienda				
SANTANDER COLOMBIA	Informa				
	Recomienda				
MUNDO MUJER	Informa	Informa		Informa	
	Recomienda	Recomienda		Recomienda	
MIBANCO		Informa			
		Recomienda			
SERFINANZA	Publica códigos oficiales desde donde el banco envía notificaciones y SMSs				
	Recomienda				
J.P. MORGAN COLOMBIA					
LULO BANK					
	Recomienda				

BTG PACTUAL COLOMBIA					

Anexo E. Listado de glosas o declaraciones relacionadas con finalidades en políticas de tratamiento de datos personales de los establecimientos bancarios de Colombia

Número	Finalidad declarada	Categoría Finalidad	Banco
1	a. Promocionar, comercializar u ofrecer, de manera individual o conjunta productos y/o servicios propios u ofrecidos en alianza comercial, a través de cualquier medio o canal, o para complementar, optimizar o profundizar el portafolio de productos y/o servicios actualmente ofrecidos. Esta autorización para el Tratamiento de mis Datos Personales se hace extensiva a las entidades subordinadas del Banco, su matriz y las entidades subordinadas o vinculadas de su matriz o ante cualquier sociedad en la que éstas tengan participación accionaria directa o indirectamente (en adelante "LAS ENTIDADES AUTORIZADAS")	Mercadeo propio y de terceros autorizados	Bogotá
2	i. Actualizar bases de datos y tramitar la apertura y/o vinculación de productos y/o servicios en el Banco o en cualquiera de LAS ENTIDADES AUTORIZADAS,	Misional	Bogotá
3	ii.Evaluar riesgos derivados de la relación contractual potencial, vigente o concluida,	Perfilamiento financiero y comercial	Bogotá
4	iii. Realizar, validar, autorizar o verificar transacciones incluyendo, cuando sea requerido, la consulta y reproducción de datos sensibles tales como la huella, imagen o voz,	Prevención fraude contra la identidad	Bogotá
5	iv. Obtener conocimiento del perfil comercial o transaccional del titular, el nacimiento, modificación, celebración y/o extinción de obligaciones directas, contingentes o indirectas, el incumplimiento de las obligaciones que adquiera con El Banco o con cualquier tercero, así como cualquier novedad en relación con tales obligaciones, hábitos de pago y comportamiento crediticio con el Banco y/o terceros.	Perfilamiento financiero y comercial	Bogotá
6	v. Conocer el estado de las operaciones vigentes activas o pasivas o de cualquier naturaleza o las que en el futuro llegue a celebrar con el Banco, con otras entidades financieras o comerciales, con cualquier operador de información o administrador de bases de datos o cualquier otra entidad similar que en un futuro se establezca y que tenga por objeto cualquiera de las anteriores actividades,	Perfilamiento financiero y comercial	Bogotá
7	vi. Conocer información acerca de mi manejo de cuentas corrientes, ahorros, depósitos, tarjetas de crédito, comportamiento comercial, laboral y demás productos o servicios y, en general, del cumplimiento y manejo de mis créditos y obligaciones, cualquiera que sea su naturaleza. Esta autorización comprende información referente al manejo, estado, cumplimiento de las relaciones, contratos y servicios, hábitos de pago, incluyendo aportes al sistema de seguridad social, obligaciones y las deudas vigentes, vencidas sin cancelar, procesos, o la utilización indebida de servicios financieros.	Perfilamiento financiero y comercial	Bogotá
8	vii. Prevenir el lavado de activos, la financiación del terrorismo, así como detectar el fraude y otras actividades ilegales,	Prevención del terrorismo, lavado de activos, actividades ilegales	Bogotá
9	viii. Dar cumplimiento a sus obligaciones legales y contractuales,	Contractual	Bogotá

10	ix. Ejercer sus derechos, incluyendo los referentes a actividades de cobranza judicial y extrajudicial y las gestiones conexas para obtener el pago de las obligaciones a cargo del titular o de su empleador, si es del caso,	Misional	Bogotá
11	x. Implementación de software y servicios tecnológicos. Para efectos de lo dispuesto en el presente literal b, el Banco en lo que resulte aplicable, podrá efectuar el Tratamiento de mis Datos Personales ante entidades de consulta, que manejen o administren bases de datos para los fines legalmente definidos, domiciliadas en Colombia o en el exterior, sean personas naturales o jurídicas, colombianas o extranjeras,	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Bogotá
12	c. Realizar ventas cruzadas de productos y/o servicios ofrecidos por el Banco o por cualquiera de LAS ENTIDADES AUTORIZADAS o sus aliados comerciales, incluyendo la celebración de convenios de marca compartida,	Mercadeo propio y de terceros autorizados	Bogotá
13	d. Elaborar y reportar información estadística, encuestas de satisfacción, estudios y análisis de mercado, incluyendo la posibilidad de contactarme para dichos propósitos,	Mercadeo propio y de terceros autorizados	Bogotá
14	e. Enviar mensajes, notificaciones o alertas a través de cualquier medio para remitir extractos, divulgar información legal, de seguridad, promociones, campañas comerciales, publicitarias, de mercadeo, institucionales o de educación financiera, sorteos, eventos u otros beneficios e informar al titular acerca de las innovaciones efectuadas en sus productos y/o servicios, dar a conocer las mejoras o cambios en sus canales de atención, así como dar a conocer otros servicios y/o productos ofrecidos por el Banco; LAS ENTIDADES AUTORIZADAS o sus aliados comerciales	Comunicación cliente	Bogotá
15	f. Llevar a cabo las gestiones pertinentes, incluyendo la recolección y entrega de información ante autoridades públicas o privadas, nacionales o extranjeras con competencia sobre el Banco, LAS ENTIDADES AUTORIZADAS o sobre sus actividades, productos y/o servicios, cuando se requiera para dar cumplimiento a sus deberes legales o reglamentarios, incluyendo dentro de éstos, aquellos referentes a la prevención de la evasión fiscal, lavado de activos y financiación del terrorismo u otros propósitos similares emitidas por autoridades competentes,	Cumplimiento de deberes ante autoridades	Bogotá
16	g. validar información con las diferentes bases de datos del Banco, de LAS ENTIDADES AUTORIZADAS, de autoridades y/o entidades estatales y de terceros tales como operadores de información y demás entidades que formen parte del Sistema de Seguridad Social Integral, empresas prestadoras de servicios públicos y de telefonía móvil, entre otras, para desarrollar las actividades propias de su objeto social principal y conexo, y/o cumplir con obligaciones legales	Cumplimiento de deberes ante autoridades	Bogotá
17	, h. Para que mis Datos Personales puedan ser utilizados como medio de prueba. Los Datos Personales suministrados podrán circular y transferirse a la totalidad de las áreas del Banco incluyendo proveedores de servicios, usuarios de red, redes de distribución y personas que realicen la promoción de sus productos y servicios, incluidos callcenters, domiciliados en Colombia o en el exterior, sean personas naturales o jurídicas, colombianas o extranjeras a su fuerza comercial, equipos de telemercadeo y/o procesadores de datos que trabajen en nombre del Banco, incluyendo pero sin limitarse, contratistas, delegados, outsourcing, tercerización, red de oficinas o aliados, con el objeto de desarrollar servicios de alojamiento de sistemas, de mantenimiento, servicios de análisis, servicios de mensajería por e-mail o correo físico, servicios de entrega, gestión de transacciones de pago, cobranza, entre otros.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Bogotá

18	a. Promocionar, comercializar u ofrecer, de manera individual o conjunta productos y/o servicios propios u ofrecidos en alianza comercial, a través de cualquier medio o canal, o para complementar, optimizar o profundizar el portafolio de productos y/o servicios actualmente ofrecidos. Esta autorización para el Tratamiento de mis Datos Personales se hace extensiva a las entidades subordinadas del Banco, su matriz y las entidades subordinadas o vinculadas de su matriz o ante cualquier sociedad en la que éstas tengan participación accionaria directa o indirectamente (en adelante "LAS ENTIDADES AUTORIZADAS")	Mercadeo propio y de terceros autorizados	Occidente
19	i. Actualizar bases de datos y tramitar la apertura y/o vinculación de productos y/o servicios en el Banco o en cualquiera de LAS ENTIDADES AUTORIZADAS,	Misional	Occidente
20	ii.Evaluar riesgos derivados de la relación contractual potencial, vigente o concluida,	Perfilamiento financiero y comercial	Occidente
21	iii. Realizar, validar, autorizar o verificar transacciones incluyendo, cuando sea requerido, la consulta y reproducción de datos sensibles tales como la huella, imagen o voz,	Prevención fraude contra la identidad	Occidente
22	iv. Obtener conocimiento del perfil comercial o transaccional del titular, el nacimiento, modificación, celebración y/o extinción de obligaciones directas, contingentes o indirectas, el incumplimiento de las obligaciones que adquiera con El Banco o con cualquier tercero, así como cualquier novedad en relación con tales obligaciones, hábitos de pago y comportamiento crediticio con el Banco y/o terceros.	Perfilamiento financiero y comercial	Occidente
23	v. Conocer el estado de las operaciones vigentes activas o pasivas o de cualquier naturaleza o las que en el futuro llegue a celebrar con el Banco, con otras entidades financieras o comerciales, con cualquier operador de información o administrador de bases de datos o cualquier otra entidad similar que en un futuro se establezca y que tenga por objeto cualquiera de las anteriores actividades,	Perfilamiento financiero y comercial	Occidente
24	vi. Conocer información acerca de mi manejo de cuentas corrientes, ahorros, depósitos, tarjetas de crédito, comportamiento comercial, laboral y demás productos o servicios y, en general, del cumplimiento y manejo de mis créditos y obligaciones, cualquiera que sea su naturaleza. Esta autorización comprende información referente al manejo, estado, cumplimiento de las relaciones, contratos y servicios, hábitos de pago, incluyendo aportes al sistema de seguridad social, obligaciones y las deudas vigentes, vencidas sin cancelar, procesos, o la utilización indebida de servicios financieros.	Perfilamiento financiero y comercial	Occidente
25	vii. Prevenir el lavado de activos, la financiación del terrorismo, así como detectar el fraude y otras actividades ilegales,	Prevención del terrorismo, lavado de activos, actividades ilegales	Occidente
26	viii. Dar cumplimiento a sus obligaciones legales y contractuales,	Contractual	Occidente
27	ix. Ejercer sus derechos, incluyendo los referentes a actividades de cobranza judicial y extrajudicial y las gestiones conexas para obtener el pago de las obligaciones a cargo del titular o de su empleador, si es del caso,	Misional	Occidente
28	x. Implementación de software y servicios tecnológicos. Para efectos de lo dispuesto en el presente literal b, el Banco en lo que resulte aplicable, podrá efectuar el Tratamiento de mis Datos Personales ante entidades de consulta, que manejen o administren bases de datos para los fines legalmente definidos, domiciliadas en Colombia o en el exterior, sean personas naturales o jurídicas, colombianas o extranjeras,	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Occidente

29	c. Realizar ventas cruzadas de productos y/o servicios ofrecidos por el Banco o por cualquiera de LAS ENTIDADES AUTORIZADAS o sus aliados comerciales, incluyendo la celebración de convenios de marca compartida,	Mercadeo propio y de terceros autorizados	Occidente
30	d. Elaborar y reportar información estadística, encuestas de satisfacción, estudios y análisis de mercado, incluyendo la posibilidad de contactarme para dichos propósitos,	Mercadeo propio y de terceros autorizados	Occidente
31	e. Enviar mensajes, notificaciones o alertas a través de cualquier medio para remitir extractos, divulgar información legal, de seguridad, promociones, campañas comerciales, publicitarias, de mercadeo, institucionales o de educación financiera, sorteos, eventos u otros beneficios e informar al titular acerca de las innovaciones efectuadas en sus productos y/o servicios, dar a conocer las mejoras o cambios en sus canales de atención, así como dar a conocer otros servicios y/o productos ofrecidos por el Banco; LAS ENTIDADES AUTORIZADAS o sus aliados comerciales	Comunicación cliente	Occidente
32	f. Llevar a cabo las gestiones pertinentes, incluyendo la recolección y entrega de información ante autoridades públicas o privadas, nacionales o extranjeras con competencia sobre el Banco, LAS ENTIDADES AUTORIZADAS o sobre sus actividades, productos y/o servicios, cuando se requiera para dar cumplimiento a sus deberes legales o reglamentarios, incluyendo dentro de éstos, aquellos referentes a la prevención de la evasión fiscal, lavado de activos y financiación del terrorismo u otros propósitos similares emitidas por autoridades competentes,	Cumplimiento de deberes ante autoridades	Occidente
33	g. validar información con las diferentes bases de datos del Banco, de LAS ENTIDADES AUTORIZADAS, de autoridades y/o entidades estatales y de terceros tales como operadores de información y demás entidades que formen parte del Sistema de Seguridad Social Integral, empresas prestadoras de servicios públicos y de telefonía móvil, entre otras, para desarrollar las actividades propias de su objeto social principal y conexo, y/o cumplir con obligaciones legales	Cumplimiento de deberes ante autoridades	Occidente
34	, h. Para que mis Datos Personales puedan ser utilizados como medio de prueba. Los Datos Personales suministrados podrán circular y transferirse a la totalidad de las áreas del Banco incluyendo proveedores de servicios, usuarios de red, redes de distribución y personas que realicen la promoción de sus productos y servicios, incluidos callcenters, domiciliados en Colombia o en el exterior, sean personas naturales o jurídicas, colombianas o extranjeras a su fuerza comercial, equipos de telemercadeo y/o procesadores de datos que trabajen en nombre del Banco, incluyendo pero sin limitarse, contratistas, delegados, outsourcing, tercerización, red de oficinas o aliados, con el objeto de desarrollar servicios de alojamiento de sistemas, de mantenimiento, servicios de análisis, servicios de mensajería por e-mail o correo físico, servicios de entrega, gestión de transacciones de pago, cobranza, entre otros.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Occidente
35	a. Promocionar, comercializar u ofrecer, de manera individual o conjunta productos y/o servicios propios u ofrecidos en alianza comercial, a través de cualquier medio o canal, o para complementar, optimizar o profundizar el portafolio de productos y/o servicios actualmente ofrecidos. Esta autorización para el Tratamiento de mis Datos Personales se hace extensiva a las entidades subordinadas del Banco, su matriz y las entidades subordinadas o vinculadas de su matriz o ante cualquier sociedad en la que éstas tengan participación accionaria directa o indirectamente (en adelante “LAS ENTIDADES AUTORIZADAS”)	Mercadeo propio y de terceros autorizados	Av Villas
36	i. Actualizar bases de datos y tramitar la apertura y/o vinculación de productos y/o servicios en el Banco o en cualquiera de LAS ENTIDADES AUTORIZADAS,	Misional	Av Villas
37	ii.Evaluar riesgos derivados de la relación contractual potencial, vigente o concluida,	Perfilamiento financiero y comercial	Av Villas
38	iii. Realizar, validar, autorizar o verificar transacciones incluyendo, cuando sea requerido, la consulta y reproducción de datos sensibles tales como la huella, imagen o voz,	Prevención fraude contra la identidad	Av Villas

39	iv. Obtener conocimiento del perfil comercial o transaccional del titular, el nacimiento, modificación, celebración y/o extinción de obligaciones directas, contingentes o indirectas, el incumplimiento de las obligaciones que adquiera con El Banco o con cualquier tercero, así como cualquier novedad en relación con tales obligaciones, hábitos de pago y comportamiento crediticio con el Banco y/o terceros.	Perfilamiento financiero y comercial	Av Villas
40	v. Conocer el estado de las operaciones vigentes activas o pasivas o de cualquier naturaleza o las que en el futuro llegue a celebrar con el Banco, con otras entidades financieras o comerciales, con cualquier operador de información o administrador de bases de datos o cualquier otra entidad similar que en un futuro se establezca y que tenga por objeto cualquiera de las anteriores actividades,	Perfilamiento financiero y comercial	Av Villas
41	vi. Conocer información acerca de mi manejo de cuentas corrientes, ahorros, depósitos, tarjetas de crédito, comportamiento comercial, laboral y demás productos o servicios y, en general, del cumplimiento y manejo de mis créditos y obligaciones, cualquiera que sea su naturaleza. Esta autorización comprende información referente al manejo, estado, cumplimiento de las relaciones, contratos y servicios, hábitos de pago, incluyendo aportes al sistema de seguridad social, obligaciones y las deudas vigentes, vencidas sin cancelar, procesos, o la utilización indebida de servicios financieros.	Perfilamiento financiero y comercial	Av Villas
42	vii. Prevenir el lavado de activos, la financiación del terrorismo, así como detectar el fraude y otras actividades ilegales,	Prevención del terrorismo, lavado de activos, actividades ilegales	Av Villas
43	viii. Dar cumplimiento a sus obligaciones legales y contractuales,	Contractual	Av Villas
44	ix. Ejercer sus derechos, incluyendo los referentes a actividades de cobranza judicial y extrajudicial y las gestiones conexas para obtener el pago de las obligaciones a cargo del titular o de su empleador, si es del caso,	Misional	Av Villas
45	x. Implementación de software y servicios tecnológicos. Para efectos de lo dispuesto en el presente literal b, el Banco en lo que resulte aplicable, podrá efectuar el Tratamiento de mis Datos Personales ante entidades de consulta, que manejen o administren bases de datos para los fines legalmente definidos, domiciliadas en Colombia o en el exterior, sean personas naturales o jurídicas, colombianas o extranjeras,	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Av Villas
46	c. Realizar ventas cruzadas de productos y/o servicios ofrecidos por el Banco o por cualquiera de LAS ENTIDADES AUTORIZADAS o sus aliados comerciales, incluyendo la celebración de convenios de marca compartida,	Mercadeo propio y de terceros autorizados	Av Villas
47	d. Elaborar y reportar información estadística, encuestas de satisfacción, estudios y análisis de mercado, incluyendo la posibilidad de contactarme para dichos propósitos,	Mercadeo propio y de terceros autorizados	Av Villas
48	e. Enviar mensajes, notificaciones o alertas a través de cualquier medio para remitir extractos, divulgar información legal, de seguridad, promociones, campañas comerciales, publicitarias, de mercadeo, institucionales o de educación financiera, sorteos, eventos u otros beneficios e informar al titular acerca de las innovaciones efectuadas en sus productos y/o servicios, dar a conocer las mejoras o cambios en sus canales de atención, así como dar a conocer otros servicios y/o productos ofrecidos por el Banco; LAS ENTIDADES AUTORIZADAS o sus aliados comerciales	Comunicación cliente	Av Villas

49	f. Llevar a cabo las gestiones pertinentes, incluyendo la recolección y entrega de información ante autoridades públicas o privadas, nacionales o extranjeras con competencia sobre el Banco, LAS ENTIDADES AUTORIZADAS o sobre sus actividades, productos y/o servicios, cuando se requiera para dar cumplimiento a sus deberes legales o reglamentarios, incluyendo dentro de éstos, aquellos referentes a la prevención de la evasión fiscal, lavado de activos y financiación del terrorismo u otros propósitos similares emitidas por autoridades competentes,	Cumplimiento de deberes ante autoridades	Av Villas
50	g. validar información con las diferentes bases de datos del Banco, de LAS ENTIDADES AUTORIZADAS, de autoridades y/o entidades estatales y de terceros tales como operadores de información y demás entidades que formen parte del Sistema de Seguridad Social Integral, empresas prestadoras de servicios públicos y de telefonía móvil, entre otras, para desarrollar las actividades propias de su objeto social principal y conexo, y/o cumplir con obligaciones legales	Cumplimiento de deberes ante autoridades	Av Villas
51	, h. Para que mis Datos Personales puedan ser utilizados como medio de prueba. Los Datos Personales suministrados podrán circular y transferirse a la totalidad de las áreas del Banco incluyendo proveedores de servicios, usuarios de red, redes de distribución y personas que realicen la promoción de sus productos y servicios, incluidos callcenters, domiciliados en Colombia o en el exterior, sean personas naturales o jurídicas, colombianas o extranjeras a su fuerza comercial, equipos de telemercadeo y/o procesadores de datos que trabajen en nombre del Banco, incluyendo pero sin limitarse, contratistas, delegados, outsourcing, tercerización, red de oficinas o aliados, con el objeto de desarrollar servicios de alojamiento de sistemas, de mantenimiento, servicios de análisis, servicios de mensajería por e-mail o correo físico, servicios de entrega, gestión de transacciones de pago, cobranza, entre otros.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Av Villas
52	a. Llevar a cabo todos los procesos requeridos para atender las obligaciones pactadas con EL TITULAR.	Contractual	Popular
53	b. Realizar todos los procesos necesarios para dar cumplimiento a las obligaciones legales y reglamentarias inherentes a las relaciones de índole precontractual, contractual y postcontractual con EL TITULAR, conforme a la naturaleza de la relación.	Contractual	Popular
54	c. Gestionar toda la información necesaria para el cumplimiento de las obligaciones tributarias, contables y financieras de EL BANCO.	Cumplimiento de deberes ante autoridades	Popular
55	e. Gestionar y prestar los servicios a los consumidores financieros atendiendo las necesidades particulares de cada uno.	Misional	Popular
56	f. Controlar y prevenir fraudes, lavado de activos, la financiación del terrorismo o la financiación de la proliferación de armas de destrucción masiva; o la comisión de actividades ilegales.	Prevención del terrorismo, lavado de activos, actividades ilegales	Popular
57	g. Dar cumplimiento a las obligaciones relacionadas con el Sistema de Seguridad Social Integral.	Cumplimiento de deberes ante autoridades	Popular
58	h. Elaborar estudios técnicos, estadísticos, encuestas, análisis de tendencias de mercado y en general cualquier estudio técnico o de campo relacionado con el sector o la prestación de servicios.	Mercadeo propio y de terceros autorizados	Popular
59	i. Compartir con ENTIDADES AUTORIZADAS, para el desarrollo de su objeto social o para complementar o enriquecer la oferta y/o la prestación de los productos y/o servicios de EL BANCO;	Mercadeo propio y de terceros autorizados	Popular
60	j. Dar tratamiento en medios físicos, digitales o por cualquier medio, asegurando el correcto registro y la utilización de las páginas web de EL BANCO;	Publicación	Popular
61	k. Optimizar la prestación del servicio o del producto ofrecido o adquirido por EL TITULAR con EL BANCO o con ENTIDADES AUTORIZADAS;	Mercadeo propio y de terceros autorizados	Popular

62	l. Informar a EL TITULAR acerca de las innovaciones efectuadas en sus productos y/o servicios, profundizar o ampliar su portafolio con EL BANCO, dar a conocer las mejoras o cambios en sus canales de atención, así como de servicios y/o productos ofrecidos por ENTIDADES AUTORIZADAS;	Mercadeo propio y de terceros autorizados	Popular
63	m. Obtener conocimiento del perfil comercial o transaccional de EL TITULAR;	Perfilamiento financiero y comercial	Popular
64	n. Ofrecer campañas comerciales, publicitarias, de marketing o de educación financiera, relacionadas con productos y/o servicios de EL BANCO o de ENTIDADES AUTORIZADAS.	Mercadeo propio y de terceros autorizados	Popular
65	o. Dar cumplimiento a las obligaciones legales, en especial las reglamentaciones expedidas por la Superintendencia Financiera de Colombia.	Cumplimiento de deberes ante autoridades	Popular
66	p. Las demás finalidades que determine EL BANCO en desarrollo de su objeto social que en todo caso deben ser conforme con la Ley, y en especial el cumplimiento específico en materia de protección de datos.	No determinada	Popular
67	Mantener una eficiente comunicación de la información que sea de utilidad en los vínculos contractuales en los que sea o llegare a ser parte el Titular de la Información.	Contractual	Itaú
68	Dar cumplimiento de las obligaciones contraídas por Las Sociedades con los clientes, potenciales clientes, empleados, potenciales empleados, accionistas, potenciales accionistas o proveedores o potenciales proveedores.	Contractual	Itaú
69	Informar las modificaciones que se presenten en desarrollo de los vínculos contractuales con el Titular de la Información.	Contractual	Itaú
70	Realizar estudios internos sobre los hábitos de los Titulares de la Información en su calidad de Cliente, Empleado o Proveedor.	Perfilamiento no financiero	Itaú
71	Elaboración de estudios técnicos actuariales, estadísticos, encuestas de satisfacción de clientes de los servicios prestados, análisis de tendencias de mercado, y en general de técnicas relacionadas con los servicios financieros que prestan todas Las Sociedades.	Mercadeo propio y de terceros autorizados	Itaú
72	Dar cumplimiento a requerimientos de autoridades colombianas y/o extranjeras, incluyendo, pero sin limitarse a autoridades de Estados Unidos de Norteamérica, con el fin de cumplir la normativa aplicable en las respectivas jurisdicciones en materia de prevención de lavado de activos y/o financiación del terrorismo, conocimiento del cliente y en general, disposiciones regulatorias aplicables al sistema financiero. El Grupo Itaú entregará la información que le sea requerida por las autoridades correspondientes sin que ello implique una violación al deber de reserva financiera pues dicha entrega será realizada a autoridades competentes según su jurisdicción.	Prevención del terrorismo, lavado de activos, actividades ilegales	Itaú
73	En desarrollo de los negocios jurídicos que se realicen sobre cualquier clase de productos o servicios financieros, compartan con terceros los datos personales, financieros, privados o semiprivados, con el objeto de que dichos terceros a nivel nacional o internacional procesen los datos para los fines propios de la operatividad de tales negocios. Las Sociedades y los terceros continuarán obligados por los deberes de reserva bancaria o financiera y sigilo profesional. Las Sociedades buscarán que tales deberes de reserva se extiendan a tales terceros.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Itaú

74	Reportar, compilar, ofrecer, consultar, intercambiar, transferir, mantener, procesar, solicitar o divulgar ante la ASOBANCARIA o cualquier otro Operador de Información de bases de datos o tercero que preste servicios al Banco, nacional o extranjero, nuestra información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Lo anterior para fines estadísticos, de conocimiento del cliente y protección, promoción y mantenimiento de la confianza en la actividad financiera. En consecuencia, quienes sean afiliados o tengan acceso a las bases de datos que administren todos los anteriores Operadores podrán además conocer esta información según la Ley y la jurisprudencia aplicable. La información reportada permanecerá por los tiempos establecidos en la ley y la jurisprudencia de acuerdo con la forma y momento en que se extingan las obligaciones que las soportan.	Perfilamiento financiero y comercial	Itaú
75	Envío a través de medio seguro de la información a la República de Chile o a Brasil, país de origen de la Sociedad Matriz del Grupo Itaú en Colombia y a otros países en donde por temas de contingencias se tengan “back-ups” o respaldos de la información, tales como España, Estados Unidos, México o Brasil.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Itaú
76	Transmitir ofertas de servicios financieros que puedan ser útiles o adecuadas, a título individual o mediante alianzas comerciales que contraiga Las Sociedades.	Mercadeo propio y de terceros autorizados	Itaú
77	Información acerca de las innovaciones efectuadas en los productos y servicios ofrecidos por Las Sociedades, con el fin de profundizar y/o ampliar su portafolio actual.	Mercadeo propio y de terceros autorizados	Itaú
78	Elaboración de reportes a centrales de riesgo por incumplimiento de las obligaciones financieras y/o comerciales derivadas de los contratos celebrados con Las Sociedades.	Perfilamiento financiero y comercial	Itaú
79	Control y prevención del fraude, el lavado de activos y financiación del terrorismo.	Prevención del terrorismo, lavado de activos, actividades ilegales	Itaú
80	Conocer su comportamiento financiero, comercial y crediticio y el cumplimiento de sus obligaciones legales.	Perfilamiento financiero y comercial	Bancolombia
81	Realizar todas las gestiones necesarias tendientes a confirmar y actualizar la información del cliente.	Prevención fraude contra la identidad	Bancolombia
82	Validar y verificar la identidad del cliente para el ofrecimiento y administración de productos y servicios, así mismo para compartir la información con diversos actores del mercado.	Mercadeo propio y de terceros autorizados	Bancolombia
83	Establecer una relación contractual, así como mantener y terminar una relación contractual.	Contractual	Bancolombia
84	Ofrecer y prestar productos o servicios a través de cualquier medio o canal de acuerdo con el perfil del cliente y los avances tecnológicos.	Mercadeo propio y de terceros autorizados	Bancolombia
85	Recibir información por parte del GRUPO BANCOLOMBIA respecto a campañas comerciales actuales y futuras, promoción de productos y servicios tanto propios como de terceros, y demás comunicaciones necesarias para mantener comunicado y enterado al cliente mediante: llamada telefónica, mensaje de texto, correo electrónico, Facebook, Twitter, Instagram o cualquier red social de integración o mensajería instantánea, entre otros.	Mercadeo propio y de terceros autorizados	Bancolombia

86	Recibir mensajes relacionados con la gestión de cobro y recuperación de cartera, ya sea directamente o mediante un tercero contratado para tal función.	Comunicación cliente	Bancolombia
87	Realizar una adecuada prestación y administración de los servicios financieros, incluyendo la gestión de cobranza.	Misional	Bancolombia
88	Suministrar información comercial, legal, de productos, de seguridad, de servicio o de cualquier otra índole.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Bancolombia
89	Conocer la ubicación y datos de contacto del cliente para efectos de notificaciones con fines de seguridad y ofrecimiento de beneficios y ofertas comerciales.	Comunicación cliente	Bancolombia
90	Efectuar análisis e investigaciones comerciales, estadísticas, de riesgos, de mercado, interbancaria y financiera incluyendo contactar al cliente para estos fines.	Mercadeo propio y de terceros autorizados	Bancolombia
91	Conocer el estado de las operaciones (activas, pasivas o de cualquier naturaleza) o las que en el futuro llegue a celebrar el cliente con cualquier entidad del GRUPO BANCOLOMBIA, con otras entidades financieras o comerciales, con cualquier agente o sujeto del mercado financiero, operador de información, administrador de bases de datos o cualquier otra entidad similar que en un futuro se establezca y que tenga por objeto cualquiera de las anteriores actividades.	Perfilamiento financiero y comercial	Bancolombia
92	Prevenir el lavado de activos, la financiación del terrorismo, así como detectar el fraude, corrupción, y otras actividades ilegales.	Prevención del terrorismo, lavado de activos, actividades ilegales	Bancolombia
93	Realizar, validar, autorizar o verificar transacciones, incluyendo, cuando sea requerido, la consulta y reproducción de datos sensibles tales como la huella digital, imagen o voz, entre otros.	Prevención fraude contra la identidad	Bancolombia
94	Realizar encuestas de satisfacción concerniente a los servicios prestados por el GRUPO BANCOLOMBIA.	Mercadeo propio y de terceros autorizados	Bancolombia
95	Consultar multas y sanciones ante las diferentes autoridades administrativas y judiciales o bases de datos públicas que tengan como función la administración de datos de esta naturaleza.	Perfilamiento financiero y comercial	Bancolombia
96	Desarrollar actividades propias de su objeto social y de su naturaleza jurídica como establecimiento bancario, así como las del negocio, incluyendo el análisis de capacidad crediticia, análisis de riesgo, análisis prospecto o del perfil de clientes, campañas de ventas, comerciales, de mercadeo de productos, procedimientos de cobranzas, procedimientos operativos, reportes, entre otras, lo cual puede implicar la transmisión de los datos a compañías de Citi o a terceros seleccionados por las empresas de Citi en Colombia dentro o fuera del país, quienes estarán obligados a cumplir con políticas de protección de información de Citibank, atendiendo las finalidades aquí consagradas.	Misional	Citibank
97	Enviar reportes y atender requerimientos de información exigidos por entidades de Citigroup Inc., entidades regulatorias locales o extranjeras, administrativas, gubernamentales o judiciales.	Cumplimiento de deberes ante autoridades	Citibank
98	Reportar a y obtener de, centrales de riesgo y operadores de bancos de datos de información financiera, crediticia, comercial, información sobre cumplimiento o incumplimiento de sus obligaciones y demás datos reportados a que se refiere la ley aplicable	Perfilamiento financiero y comercial	Citibank

99	. Intercambiar información con las asociaciones gremiales, para la realización de estudios y análisis correspondientes al sector.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Citibank
100	Prevenir el fraude, consultar en bases de datos de lavado de activos y financiación del terrorismo e investigaciones de seguridad.	Prevención del terrorismo, lavado de activos, actividades ilegales	Citibank
101	Proporcionar calidad en el servicio prestado, atención al cliente, realizar encuestas de satisfacción del servicio y gestionar trámites de solicitudes quejas y reclamos.	Misional	Citibank
102	Consultar información del titular en bases de datos de entidades privadas o públicas, nacionales o extranjeras, así como entidades del sector salud privado o público, historias clínicas y estado de salud del titular.	Perfilamiento no financiero	Citibank
103	Para la definición, estructuración y ejecución de transacciones estratégicas de Citi sobre su operación, mercado objetivo, servicios ofrecidos, lo cual podrá implicar la transmisión o transferencia de los datos a entidades de Citigroup Inc. o terceros.	Mercadeo propio y de terceros autorizados	Citibank
104	Para la evaluación de la capacidad incluida la financiera de los proponentes o 3 Citi y el diseño del arco es una Marca Registrada de servicios de Citigroup Inc. proveedores de servicio, así como para el cumplimiento de obligaciones, actividades y procedimientos derivados de la relación precontractual y contractual durante la vigencia de la misma y posterior a ella.	Perfilamiento financiero y comercial	Citibank
105	Con fines estadísticos, gerenciales, monitoreo, control, análisis financiero y comercial, definición de políticas y procedimientos, auditorías internas, externas y/o regulatorias.	Mercadeo propio y de terceros autorizados	Citibank
106	Contactar a terceros y/o clientes para fines relacionados con el servicio contratado, la relación comercial o en razón del estado de sus obligaciones.	Perfilamiento financiero y comercial	Citibank
107	Cualquier otra finalidad requerida para el desarrollo de su objeto social o de las entidades de Citigroup Inc.	No determinada	Citibank
108	desarrollar sus funciones, autorizaciones, operaciones o atribuciones propias en desarrollo de su objeto social o el giro ordinario de sus negocios o funciones que les otorga la ley, en sus condiciones de establecimiento bancario, sociedad fiduciaria, sociedad comisionista de bolsa y entidad administradora de sistemas de pago de bajo valor	Misional	SUDAMERIS
109	I. Efectuar las gestiones pertinentes para el desarrollo de la etapa precontractual, contractual y postcontractual, respecto de cualquiera de los productos y servicios ofrecidos por BBVA, que haya o no adquirido o respecto de cualquier relación negocial subyacente que tenga con ella, así como dar cumplimiento a la ley colombiana o extranjera y a las órdenes de autoridades judiciales o administrativas; I	Contractual	BBVA
110	I. Gestionar trámites (solicitudes, quejas, reclamos), realizar análisis de riesgo y efectuar encuestas de satisfacción respecto de los bienes y servicios de BBVA o empresas vinculadas, así como a los aliados comerciales de BBVA;	Misional	BBVA
111	III. Suministrar información de contacto y documentos pertinentes a la fuerza comercial y/o red de distribución, telemercadeo y cualquier tercero con el cual BBVA posea un vínculo contractual de cualquier índole;	Mercadeo propio y de terceros autorizados	BBVA

112	IV. Dar a conocer, transferir y/o trasmitir mis datos personales dentro y fuera del país a terceros a consecuencia de un contrato, ley o vínculo lícito que así lo requiera o para implementar servicios de computación en la nube;	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	BBVA
113	V. Suministrar a las asociaciones gremiales (ASOBANCARIA, FASECOLDA, etc.) los datos personales necesarios para la realización de estudios y en general la administración de sistemas de información del sector correspondiente;	Misional	BBVA
114	VI. Transferir o transmitir a las compañías BBVA, en calidad de encargados o a terceros en virtud de un contrato;	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	BBVA
115	VII. Crear bases de datos para los fines descritos en la presente autorización;	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	BBVA
116	VIII. Reportar datos sobre el cumplimiento o incumplimiento de las obligaciones dinerarias del titular del dato a centrales de información crediticia, entre otras CIFIN, DATACRÉDITO o a operadores de bancos de datos de información financiera, crediticia, comercial y provenientes de terceros países a que se refiere la ley 1266 de 2008 para los fines indicados en dicha ley y sus normas reglamentarias o modificatorias. BBVA también puede:	Perfilamiento financiero y comercial	BBVA
117	IX. Conocer la información del titular del dato que repose en centrales de información crediticia como, entre otros, CIFIN, DATACRÉDITO o en operadores de bancos de datos de información financiera, crediticia, comercial y provenientes de terceros países a que se refiere la ley 1266 de 2008 para los fines indicados en dicha ley y sus normas reglamentarias o modificatorias.	Perfilamiento financiero y comercial	BBVA
118	X. Acceder y consultar la información del titular del dato que repose o esté contenida en bases de datos o archivos de cualquier Entidad Privada o Pública (como entre otros, los Ministerios, los Departamentos Administrativos, la DIAN, la Fiscalía, Registraduría Nacional del Estado Civil, los Juzgados, tribunales y altas Cortes) ya sea nacional, internacional o extranjera; Página 8 de 14	Perfilamiento financiero y comercial	BBVA
119	XI. Consultar a cualquier médico, hospital, compañía de seguros, compañía de medicina prepagada o entidad promotoras de salud (EPS) para que en cualquier momento, ya sea en vida del titular o posterior a su muerte, BBVA pueda acceder a la información sobre el estado de salud del titular y a su historia clínica así como obtener copia total o parcial de la misma; en consecuencia el titular autoriza a dichas entidades para que entreguen a BBVA copia de toda la información que sea requerida por BBVA.	Perfilamiento no financiero	BBVA
120	Efectuar las gestiones pertinentes para el desarrollo del objeto social de la CORPORACIÓN en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con los Titulares de la información.	Misional	Davivienda
121	2. Desarrollar los procesos que se requieran para la adecuada prestación de los productos y/o servicios contratados;	Misional	Davivienda

122	3. Como elemento de análisis en etapas precontractuales, contractuales y postcontractuales para establecer y/o mantener cualquier relación contractual, incluyendo, como parte de ello, los siguientes propósitos. Actualizar bases de datos y tramitar la apertura y/o vinculación de productos y/o servicios en la CORPORACIÓN,	Perfilamiento financiero y comercial	Davivienda
123	ii. Evaluar riesgos derivados de la relación contractual potencial, vigente o concluida,	Perfilamiento financiero y comercial	Davivienda
124	iii. Realizar, validar, autorizar o verificar transacciones incluyendo, cuando sea requerido, y la consulta y reproducción de datos sensibles tales como la huella, imagen o voz.	Prevención fraude contra la identidad	Davivienda
125	iv. Obtener conocimiento del perfil comercial o transaccional de los Titulares, el nacimiento, modificación, celebración y/o extinción de obligaciones directas, contingentes o indirectas, el incumplimiento de las obligaciones que adquiera con la CORPORACIÓN o con cualquier tercero, así como cualquier novedad en relación con tales obligaciones, hábitos de pago y comportamiento crediticio con CORPORACIÓN y/o terceros.	Perfilamiento financiero y comercial	Davivienda
126	v. Conocer el estado de las operaciones vigentes activas o pasivas o de cualquier naturaleza o las que en el futuro llegue a celebrar con la CORPORACIÓN, con otras entidades financieras o comerciales, con cualquier operador de información o administrador de bases de datos o cualquier otra entidad similar que en un futuro se establezca y que tenga por objeto cualquiera de las anteriores actividades	Perfilamiento financiero y comercial	Davivienda
127	4. Actualizar los datos suministrados con la información que se encuentre disponible en los Operadores de Información o cualquier otra persona, entidad u organización que maneje o administre bases de datos con los fines legalmente definidos para este tipo de entidades;	Perfilamiento financiero y comercial	Davivienda
128	5. Desarrollar e implementar herramientas de prevención de fraudes;	Prevención fraude contra la identidad	Davivienda
129	6. Compartir los datos relativos a la información financiera, lo cual incluye el uso y la actualización de los datos de contacto, con firmas especializadas en labores de cobranzas para que adelanten la gestión de cobro y recaudo de las obligaciones por contraídas, y demás servicios que se consideren necesarios o complementarios. Así como, el manejo de la cartera vencida, utilizando para ello tanto los mecanismos judiciales como también las vías extraprocesales permitidas por el ordenamiento jurídico.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Davivienda
130	7. Para el desarrollo de actividades de conocimiento del perfil comercial de los Titulares, campañas comerciales, publicitarias, y de marketing, relacionadas con productos y servicios del Grupo Bolívar y con aliados comerciales que puedan complementar o enriquecer la oferta de dichos productos y servicios, los cuales serán dados a conocer de manera oportuna a los Titulares. En dichos fines se encuentran 7.1 Hacer estudios estadísticos o de comportamiento sobre mis gustos y preferencias respecto de los productos y/o servicios contratados;7.2 Realizar prospección comercial, con el fin de identificar las necesidades y gustos a satisfacer con los productos y/o servicios a ser ofrecidos, y 7.3 Suministrar información sobre eventos, novedades, promociones, publicidad y programas de fidelidad, mediante el uso de correo electrónico, correo postal, teléfono fijo, celular, fax, SMS, MSM, redes sociales o medios similares; 7.4 Medir el nivel de satisfacción respecto de los productos y/o servicios contratados; 7.5 Compartir la información con entidades del Grupo Empresarial Bolívar cuya matriz es GRUPO BOLÍVAR S.A., ubicadas dentro o fuera del territorio de la República de Colombia, las cuales aparecen listadas en el link: https://www.sociedadesbolivar.com.co/wps/portal/web/nuestrascompanias, en el que se informa el tipo de actividad que cada una de ellas desarrolla, a efecto de que me sean ofrecidos sus productos o	Mercadeo propio y de terceros autorizados	Davivienda

	servicios comerciales mediante el uso de correo electrónico, correo postal, teléfono fijo, celular, fax, SMS, MSM, redes sociales o medios similares, así como para desarrollar actividades de conocimiento del cliente, campañas comerciales, publicitarias, y marketing.		
131	A. Conocer, almacenar y procesar toda la información suministrada por EL TITULAR en una o varias bases de datos, en el formato que estime más conveniente.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Scotiabank
132	B. Conocer, almacenar, grabar, procesar y monitorear toda la información suministrada por EL TITULAR de manera verbal o escrita por cualquier canal establecido por EL RESPONSABLE lo cual podrá ser utilizado, inclusive, como prueba en cualquier queja, reclamación, conciliación o demanda.	Misional	Scotiabank
133	C. Ordenar, catalogar, clasificar, dividir o separar la información suministrada por el(los) Titular(es).	Misional	Scotiabank
134	D. Verificar, corroborar, comprobar, validar, monitorear, investigar o comparar la información suministrada por el(los) Titular(es), con cualquier información de que disponga legítimamente, incluyendo aquella conocida por su matriz, las filiales o subsidiarias de ésta, las filiales, subsidiarias y/o afiliadas de EL RESPONSABLE o cualquier compañía Scotiabank.	Prevención fraude contra la identidad	Scotiabank
135	E. Acceder, consultar, comparar, monitorear, actualizar y evaluar toda la información que sobre EL TITULAR se encuentre almacenada en las bases de datos de cualquier central de antecedentes judiciales o de seguridad, de naturaleza estatal o privada, nacional o extranjera, o cualquier base de datos comercial o de servicios o aquella que sea suministrada por cualquier persona que haya sido indicada por EL TITULAR a EL RESPONSABLE como referencia de cualquier tipo (por ejemplo laboral, financiera o personal) o aquella que sea suministrada por la(s) persona(s) que se encuentre(n) disponible(s) ante cualquier contacto realizado por EL RESPONSABLE, en uso de los datos que han sido informados a EL RESPONSABLE, que permita identificar el(los) Titular(es), actualizar la información o datos de contacto u otros datos personales requeridos para la ejecución del contrato o el cumplimiento de otras obligaciones legales.	Perfilamiento financiero y comercial	Scotiabank
136	F. Analizar, procesar, evaluar, tratar o comparar la información suministrada por EL TITULAR o recolectada por EL RESPONSABLE a través de la interacción en plataformas digitales relacionadas con EL RESPONSABLE por parte del(los) Titular(es). A los datos resultantes de análisis, procesamientos, evaluaciones, tratamientos y comparaciones, les serán aplicables las mismas autorizaciones que EL TITULAR otorgó).	Prevención fraude contra la identidad	Scotiabank

137	G. Estudiar, analizar, personalizar y utilizar la información y la documentación suministrada por EL TITULAR para el seguimiento, desarrollo y/o mejoramiento, tanto individual como general, de condiciones de servicio, administración, seguridad o atención, así como para la implementación de planes de mercadeo, campañas, beneficios especiales y promociones de productos y servicios financieros y comerciales asociados que puedan ser de interés o que impliquen un beneficio EL TITULAR EL RESPONSABLE podrá compartir con su matriz, con el grupo Scotiabank, o con los aliados de negocios que se sometan a las condiciones del presente Reglamento los resultados de los mencionados estudios, análisis, personalizaciones y usos, así como toda la información, documentos y datos personales suministrados por el(los) Titular(es).	Mercadeo propio y de terceros autorizados	Scotiabank
138	H. Reportar, comunicar o permitir el acceso a la información suministrada por EL TITULAR o aquella que se disponga sobre el mismo a: a. A las centrales de riesgo crediticio, financiero, comercial o de servicios legítimamente constituidas, o a otras entidades financieras, de acuerdo con las normas aplicables.	Perfilamiento financiero y comercial	Scotiabank
139	b. Reportar, comunicar o permitir el acceso a la información suministrada por EL TITULAR o aquella que se disponga sobre el mismo a: A los terceros que, en calidad de proveedores nacionales o extranjeros, en el país o en el exterior, de servicios tecnológicos, logísticos, de cobranza, de seguridad o de apoyo general puedan tener acceso a la información suministrada por EL TITULAR.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Scotiabank
140	c. Reportar, comunicar o permitir el acceso a la información suministrada por EL TITULAR o aquella que se disponga sobre el mismo a: A las autoridades públicas que en ejercicio de su competencia y con autorización legal lo soliciten, o ante las cuales se encuentre procedente formular denuncia, demanda, convocatoria a arbitraje, queja o reclamación.	Cumplimiento de deberes ante autoridades	Scotiabank
141	d. Reportar, comunicar o permitir el acceso a la información suministrada por EL TITULAR o aquella que se disponga sobre el mismo a: A toda otra persona natural o jurídica a quien EL TITULAR autorice expresamente.	No determinada	Scotiabank
142	Registrarlo en la base de datos como prospecto comercial y cliente.	Mercadeo propio y de terceros autorizados	Credifinanciera
143	b. Verificar, validar, confirmar y actualizar la información e identidad del prospecto comercial y cliente.	Mercadeo propio y de terceros autorizados	Credifinanciera
144	c. Conocer el comportamiento financiero, comercial, crediticio, y nivel de endeudamiento del prospecto comercial y cliente.	Perfilamiento financiero y comercial	Credifinanciera
145	d. Establecer, mantener, actualizar y terminar una relación contractual, para la cual se utilizarán sus datos para generar comunicaciones efectivas.	Contractual	Credifinanciera
146	e. Efectuar una adecuada prestación de los servicios financieros de colocación, captación y gestión de cobro. La gestión de cobro y recuperación de cartera se podrá efectuar directamente por la entidad o a través de un tercero contratado para tal función, razón por la cual, el cliente aprueba que su información personal sea compartida con el mencionado tercero.	Misional	Credifinanciera
147	f. Establecer un canal de comunicación efectiva con el prospecto comercial y cliente, cuyo contacto puede efectuarse a través de llamada telefónica, mensaje de texto, correo electrónico, redes sociales, aplicaciones de mensajería instantánea (WhatsApp, entre otras), correspondencia física, entre otros.	Mercadeo propio y de terceros autorizados	Credifinanciera
148	g. Grabar llamadas telefónicas, guardar las comunicaciones y, en general, dejar constancia de los mensajes que se intercambien en desarrollo del contrato.	Misional	Credifinanciera
149	h. Efectuar estudios estadístico y análisis de mercado.	Mercadeo propio y de terceros autorizados	Credifinanciera

150	i. Destruir los documentos entregados en caso de que la solicitud de financiación sea negada o en caso de que sea aprobada y no aceptada.	Misional	Credifinanciera
151	j. Informar sobre el estado de los servicios contratados, modificaciones, novedades y realización de encuestas de satisfacción del servicio.	Comunicación cliente	Credifinanciera
152	k. Responder a solicitudes o requerimientos de información de nuestros productos y servicios.	Comunicación cliente	Credifinanciera
153	l. Realizar análisis estadísticos de tendencias, hábitos de consumo y comportamientos del consumidor.	Mercadeo propio y de terceros autorizados	Credifinanciera
154	m. Gestionar actividades de servicio al cliente y postventa.	Misional	Credifinanciera
155	n. Ofrecer los productos o servicios de la entidad, así como los servicios y productos de las entidades con las cuales cuenten con una alianza vigente, a través de cualquier medio conocido o por conocerse, ya sea directamente o a través de un tercero encargado para tal efecto.	Mercadeo propio y de terceros autorizados	Credifinanciera
156	o. Informar sobre cambios sustanciales en la Política de Tratamiento de Datos Personales.	Comunicación cliente	Credifinanciera
157	p. Responder a las peticiones, consultas, reclamos y/o quejas que realicen los titulares de información de tipo personal a través de cualquiera de los canales habilitados que el responsable para dicho efecto.	Misional	Credifinanciera
158	q. Transferir o transmitir la información personal a terceros, cuya gestión garantice el correcto funcionamiento de la operación del responsable, ya sea por una prestación de servicios como agencias de transporte, servicios de tecnología e infraestructura, abogados, entre otros, así se encuentren en países diferentes a Colombia sin importar si cumplen o no los requisitos mínimos adecuados sobre protección de datos personales establecidos por la ley colombiana para su tratamiento.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Credifinanciera
159	a) Los datos personales podrán ser tratados por Bancamía con el fin de administrar la relación comercial con sus consumidores financieros; contactarlos para evaluaciones de servicio, encuestas de satisfacción; invitarlos a la experimentación de nuevos productos y servicios;	Mercadeo propio y de terceros autorizados	Bancamía
160	efectuar gestiones de cobranza;	Misional	Bancamía
161	tratar los datos personales registrados en el Portal Transaccional o Banca móvil, a través de los cuales es posible que conozcan el número de ID del dispositivo móvil utilizado, información de red, información sobre las acciones adelantadas en la aplicación, la fecha y hora de tales acciones, así como la dirección IP y/o las coordenadas de geolocalización /GPS asignadas a al dispositivo móvil por el tercero proveedor de acceso a internet, a fin de conocer la localización, detectar y/o prevenir fraudes, funciones de grabación de voz, acceso a la galería de imágenes del dispositivo, información de app instaladas, conocer el consumo de datos, tipo de teléfono, incluyendo aquellos que puedan llegar a ser clasificados como sensibles (datos biométricos que se requieran para el uso de la aplicación como por ejemplo la huella dactilar o voz), correo electrónico, firma digital, número de móvil, datos económicos y financieros recolectados, uso de cookies, entre otros. Todo lo anterior, dentro del marco de la configuración de seguridad y privacidad que cada usuario le asigne a la plataforma y/o al dispositivo móvil según sea el caso.	Perfilamiento no financiero	Bancamía
162	Así mismo Bancamía podrá contactar a sus consumidores financieros a través de correo físico o electrónico, SMS, llamadas telefónicas, mensajes PUSH, redes sociales como Facebook, Twitter, Instagram o similares, servicios de mensajería instantánea como WhatsApp y Facebook Messenger o cualquier otro medio de comunicación electrónica equivalente, con los fines descritos anteriormente, lo que incluye entre otros: el ofrecimiento de productos y servicios, actualización de datos personales, efectuar gestión de cobro, establecer acuerdos de pago ya sea directamente o a través de un tercero, realizar encuestas de satisfacción y recibir información del trámite de PQR.	Comunicación cliente	Bancamía

163	b) La finalidad del tratamiento incluye tomar huellas digitales (dato sensible) y administrarla con el fin de facilitar la vinculación a Bancamía; el manejo de los productos; y en especial validar la identidad de sus consumidores financieros en la realización de transacciones. En todo caso, la huella digital no podrá ser vendida, transferida o cedida a terceros, salvo que medie orden de autoridad competente en ese sentido.	Prevención fraude contra la identidad	Bancamía
164	c) BANCAMÍA podrá entregar datos personales recolectados a entidades radicadas en Colombia o en el exterior, sean públicas o privadas, siempre y cuando: Sean empresas MP-AGI-DATOSPERSONAL POLÍTICA PROTECCIÓN DE DATOS PERSONALES o entidades con las que BANCAMÍA se relacione por vínculos de participación accionaria, o sean su matriz o subsidiaria, aliados estratégicos;	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Bancamía
165	o la entrega de los datos personales tengan como finalidad la estructuración o implementación de ofertas de productos o servicios,	Mercadeo propio y de terceros autorizados	Bancamía
166	la prevención de conductas delictivas,	Prevención del terrorismo, lavado de activos, actividades ilegales	Bancamía
167	o en general propuestas de valor adicionales a las que el Banco está en capacidad de ofrecerme de manera autónoma, a través de programas gubernamentales o de carácter privado;	Mercadeo propio y de terceros autorizados	Bancamía
168	o tenga como finalidad facilitar el desarrollo del objeto social de BANCAMÍA mediante la tercerización de sus procesos, tales como archivo, almacenamiento de datos digitales, funcionamiento de Banca móvil o Portal Transaccional, cobranza, gestión de riesgos, desarrollo de software, contacto de consumidores financieros, investigación de mercados, elaboración de análisis estadísticos, análisis de riesgos, elaboración de estrategias comerciales, de profundización de mercados, mercadeo, promociones, estudios de impacto social, establecimiento de nuevos canales de atención, y demás fines relacionados y conexos.	Misional	Bancamía
169	Finalidades varias - Fidelización de clientes	Mercadeo propio y de terceros autorizados	W
170	Gestión administrativa	Misional	W
171	Gestión de clientes	Misional	W
172	Gestión de cobros y pagos	Misional	W
173	Gestión de facturación	Misional	W
174	Gestión económica y contable	Misional	W
175	Gestión fiscal	Misional	W
176	Históricos de relaciones comerciales	Misional	W
177	Marketing	Mercadeo propio y de terceros autorizados	W
178	Prospección comercial	Mercadeo propio y de terceros autorizados	W
179	Publicidad propia	Mercadeo propio y de terceros autorizados	W
180	Segmentación de mercados	Mercadeo propio y de terceros autorizados	W
181	Venta a distancia	Mercadeo propio y de terceros autorizados	W

182	tramitar la vinculación del Titular a cualquiera de las Empresas del GECC, en calidad de asociado, cliente o usuario, según corresponda y transferir de manera total o parcial la información registrada en cualquier formulario de vinculación, de actualización de datos, soportes y los resultados de los análisis de SARLAFT efectuados por cualquier Empresa del GECC, con cualquiera de las Empresas del GECC, y transmitir a entidades aseguradoras en Colombia	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Coomeva
183	permitir el ofrecimiento y venta de servicios y productos derivados del objeto social de cada una de las Empresas del GECC, efectuar labores de mercadeo, realizar muestreos, encuestas e investigaciones comerciales y de servicio, de riesgos y de mercado, realizar pruebas, generar estadísticas, utilizar modelos matemáticos, identificar, recolectar y asociar información sobre intereses y hábitos de utilización de los productos o servicios y derivar conclusiones o determinar tendencias que podrán ser compartidas entre las Empresas del GECC acá definidas como responsables, permitiendo que la información del Titular se pueda o no anonimizar para los fines previstos en este numeral y cuyos resultados podrán ser utilizados por las Empresas del GECC y aliados comerciales del GECC para los fines previstos en la presente finalidad;	Mercadeo propio y de terceros autorizados	Coomeva
184	comunicar, publicitar u ofrecer servicios de las empresas o entidades filiales, subsidiarias, vinculadas o partes relacionadas, actuales y futuras, de la Cooperativa Médica del Valle y de Profesionales de Colombia COOMEVA, para generar contacto comercial con el Titular y darle a conocer los beneficios de dichas empresas o entidades, cualquiera de las Empresas del GECC podrá trasferir información personal del Titular para estos efectos	Mercadeo propio y de terceros autorizados	Coomeva
185	implementar programas de fidelización, acumulación y redención de puntos por la compra y utilización de servicios o transacciones sobre productos de cualquiera de las Empresas del GECC acá definidas, permitiendo el uso de dichos datos comerciales, financieros o crediticios del Titular para procesos comerciales, de mercadeo, redención y acumulación de premios contenidos en los reglamentos y demás campañas promocionales;	Mercadeo propio y de terceros autorizados	Coomeva
186	manejar cualquier información personal, financiera, crediticia, comercial, sensible, privada y semiprivada del Titular en una o varias bases de datos para ser transmitida o transferida a cualquiera de las Empresas del GECC, hacer perfilamientos o segmentaciones a partir de la utilización de productos o servicios, incluyendo la georreferenciación o ubicación generada por cualquier dispositivo del Titular al momento de utilización de un canal virtual para propósitos de profundizar, optimizar y completar el portafolio de productos y servicios ofrecidos y tomados por el Titular con las Empresas del GECC;	Perfilamiento financiero y comercial	Coomeva
187	suministrar al Titular información comercial sobre los productos y servicios ofrecidos por las Empresas del GECC, así como recomendaciones de seguridad, y en general cualquier información que se considere necesaria y apropiada para la utilización de los productos o la prestación de los servicios;	Comunicación cliente	Coomeva
188	realizar el análisis de riesgos integral del Titular, incluyendo el cumplimiento de la normativa sobre “conocimiento del cliente”, prevención de fraudes, prevención de lavado de activos y la financiación del terrorismo,	Perfilamiento financiero y comercial	Coomeva
189	así como realizar informes de seguridad sobre las transacciones validando registros físicos, auditivos, electrónicos y fílmicos con el propósito de elevar los niveles de eficiencia,	Seguridad	Coomeva
190	evaluar y generar estadísticas para efectos de control y supervisión por las Empresas del GECC.	Misional	Coomeva
191	En caso de que sea requerido o en cumplimiento de los deberes legales y reporte a reguladores, organismos de autorregulación y autoridades competentes, el Titular autoriza compartir los resultados de dichos análisis y de los informes a cualquiera de las Empresas del GECC en desarrollo de las finalidades acá establecidas;	Cumplimiento de deberes ante autoridades	Coomeva

192	cumplir con los deberes legales impuestos para cada una de las Empresas del GECC individualmente consideradas, así como los deberes legales que debe cumplir como Grupo Económico y como Conglomerado Financiero;	Cumplimiento de deberes ante autoridades	Coomeva
193	realizar gestiones de cobranza, bien sea directamente por alguna Empresa del GECC o a través de casas de cobranza o abogados externos autorizados por éstas, quienes actuarán como encargados, así como la localización e investigación de bienes del Titular;	Misional	Coomeva
194	transmitir, transferir, enviar, procesar, almacenar o enviar a proveedores de cualquier Empresa del GECC que presten servicios logísticos, oferta de seguros, administrativos, tecnológicos, de distribución, marketing, contact center, ubicados dentro o fuera del territorio nacional que actuarán como encargados del tratamiento;	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Coomeva
195	transmitir o transferir a la empresa o entidad ubicada dentro o fuera del territorio nacional que a futuro adquiera o administre a cualquiera de las Empresas del GECC, o alguna unidad de negocio o de sus activos, total o parcialmente;	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Coomeva
196	enriquecer cualquiera de las bases de datos de las Empresas del GECC utilizando datos de otras bases de estas mismas entidades, así como el cruce de información reportada y existente en las bases de datos de la Registraduría Nacional del Estado Civil, de los operadores de información financiera, comercial, de seguridad social y parafiscales, de empresas de servicios públicos o telefonía móvil, y de terceros que tengan autorización para el efecto; y	Prevención fraude contra la identidad	Coomeva
197	establecer, mantener, cumplir o terminar la relación contractual entre el Titular y cualquier Empresa del GECC y permitir que la información del Titular sea utilizada como medio de prueba.	Contractual	Coomeva
198	Realizar ofrecimientos comerciales de productos y servicios que ofrezca el Banco separadamente o de forma conjunta con terceros o a nombre de terceros.	Mercadeo propio y de terceros autorizados	Finandina
199	La venta, promoción, publicidad, mercadeo, seguimiento, estudios, atención al cliente, mejoramiento del servicio	Mercadeo propio y de terceros autorizados	Finandina
200	Trasladar información a los aliados comerciales del Banco que derive en el ofrecimiento comercial de nuevos productos y/o servicios que mejoren la oferta de valor con que cuentan.	Mercadeo propio y de terceros autorizados	Finandina
201	Notificación de cambios o emisión de comunicados, registros contables y estadísticos, encuestas, facturación, gestión de cobranza, análisis de crédito, análisis de riesgo, consultas y reportes a entidades y/o centrales de riesgo	Misional	Finandina
202	Validación de información, confirmación de referencias, respuesta de consultas, requerimientos, PQR´s y/o solución de casos de soporte,	Misional	Finandina
203	consulta en bases de datos de referencias personales, comerciales y/o de prevención de actividades ilícitas (SARLAFT) entre otras	Prevención del terrorismo, lavado de activos, actividades ilegales	

204	Incluir información de los titulares en bases de datos compartidas con otros responsables que persigan las mismas finalidades que las determinadas en el presente documento	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Finandina
205	Compartir los datos personales con las entidades que hagan parte del grupo económico y empresarial del Banco.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Finandina
206	Las demás finalidades que autorice el cliente o se permitan de acuerdo con la Ley 1581 de 2012, sus decretos reglamentarios, y demás normas que la regulen, o modifiquen.	No determinada	Finandina
207	Prestar sus servicios de acuerdo con las necesidades particulares de los clientes de BANCO FALABELLA, y con las actividades realizadas por BANCO FALABELLA conforme a su naturaleza jurídica de establecimiento de crédito, con el fin de cumplir los contratos celebrados.	Contractual	Falabella
208	Gestionar toda la información necesaria para el cumplimiento de las obligaciones tributarias y de registros comerciales, corporativos y contables de BANCO FALABELLA.	Cumplimiento de deberes ante autoridades	Falabella
209	Cumplir las obligaciones de facturación y obligaciones regulatorias aplicables a la relación contractual entre BANCO FALABELLA y el titular del dato.	Contractual	Falabella
210	Dar cumplimiento a obligaciones regulatorias a cargo de BANCO FALABELLA en relación con sus negocios y operación.	Cumplimiento de deberes ante autoridades	Falabella
211	Poner en práctica las políticas corporativas de BANCO FALABELLA.	Misional	Falabella
212	Cumplir con las obligaciones contractuales adquiridas por BANCO FALABELLA con sus clientes.	Contractual	Falabella
213	Desarrollar actividades comerciales y de mercadeo, tales como análisis de consumo, perfilamiento de clientes, trazabilidad de marca, envío de beneficios, promociones, ofertas, novedades, descuentos, programas de fidelización de clientes, investigación de mercado, diseño y divulgación de campañas y eventos de marcas propias, de aliados o de empresas vinculadas a EL BANCO.	Mercadeo propio y de terceros autorizados	Falabella
214	Enviar publicidad comercial, propia, de aliados y de Entidades Vinculadas.	Mercadeo propio y de terceros autorizados	Falabella
215	Realizar campañas de actualización de datos personales.	Misional	Falabella
216	Garantizar el cumplimiento de protocolos de seguridad de la información y de los establecimientos de BANCO FALABELLA.	Seguridad	Falabella
217	Elaborar estudios estadísticos, encuestas (comerciales, académicas, actuariales, etc.), análisis de mercado y de consumo, o para la creación de bases de datos de acuerdo con las características y perfil financiero y/o comercial de los clientes.	Perfilamiento financiero y comercial	Falabella
218	Atender requerimientos de auditoría externa y de autoridades competentes.	Cumplimiento de deberes ante autoridades	Falabella
219	Adelantar el control y prevención de fraudes, lavado de activos y/o financiación del terrorismo.	Prevención del terrorismo, lavado de activos, actividades ilegales	Falabella

220	Realizar labores de videovigilancia.	Misional	Falabella
221	Realizar consultas y Reportes a Centrales de Riesgo.	Perfilamiento financiero y comercial	Falabella
222	enviar información financiera de sujetos de tributación en los Estados Unidos al Internal Revenue Service (IRS) o a otras autoridades de Estados Unidos u otros países, en los términos del Foreign Account Tax Compliance Act (FATCA) o de normas de similar naturaleza de terceros países o en virtud de tratados internacionales y la prevención y control del lavado de activos y la financiación del terrorismo	Prevención del terrorismo, lavado de activos, actividades ilegales	Falabella
223	Realizar actividades de mercadeo de los productos y servicios del Banco, así como de los productos y servicios de sus filiales y/o aliados estratégicos.	Mercadeo propio y de terceros autorizados	Pichincha
224	Realizar las labores propias para que se avalen, afiancen y/o garanticen la(s) operación(es) de crédito a cargo de los clientes.	Misional	Pichincha
225	Realizar labores de venta y/o comercialización de productos y/o servicios propios y/o de aliados estratégicos.	Mercadeo propio y de terceros autorizados	Pichincha
226	Realizar gestiones de apoyo en las labores propias del Banco	Misional	Pichincha
227	Ofrecer al cliente la información y posibilidad de obtener más productos y servicios dentro del portafolio del Banco, filiales y/o subsidiarias, que puedan suplir sus necesidades y expectativas financieras	Mercadeo propio y de terceros autorizados	Pichincha
228	Informar sobre nuevos productos o servicios que estén relacionados con el o los contratos adquiridos	Mercadeo propio y de terceros autorizados	Pichincha
229	Informar sobre cambios en los productos y/o servicios del Banco, filiales y/o subsidiarias.	Comunicación cliente	Pichincha
230	Informar sobre las ventajas y beneficios a los que pueden acceder los clientes del Banco, como resultado de los acuerdos, convenios o marcas compartidas que tiene y puede llegar a tener con otras entidades de cualquier naturaleza.	Mercadeo propio y de terceros autorizados	Pichincha
231	Realizar análisis internos sobre hábitos de consumo.	Perfilamiento financiero y comercial	Pichincha
232	Entre Otros.	No determinada	Pichincha
233	sus datos se utilizan para prestarle un mejor servicio como enviarle mensajes de alertamiento de transacciones a los celulares que usted ha registrado, mensajes de generación de facturación de productos o recordatorios de pagos entre otros, los cuales adicionalmente pueden ser enviados a su correo electrónico y para cuyo mejor funcionamiento, en ocasiones encargamos a terceros, caso en el cual procuramos estándares de seguridad que garanticen la entrega de información en condiciones de total reserva y únicamente para los fines de garantizarle su información y manejo de sus productos de forma adecuada.	Comunicación cliente	COOPCENTRAL
234	Igualmente, sus datos pueden ser utilizados para remitirle informaciones, invitaciones, notificaciones, campañas educativas, de mercadeo, de cobranza y promocionales las cuales procuramos hacer en forma directa, en caso de realizarlas con un tercero igualmente procuramos el cumplimiento de procedimientos específicos de seguridad de la información.	Mercadeo propio y de terceros autorizados	COOPCENTRAL

235	Realizar consultas, solicitudes y reportes de toda la información de comportamiento crediticio ante cualquiera de los operadores de información financiera, en razón de las obligaciones contraídas o que se lleguen a contraer entre el Titular y el Banco. Así mismo, el Banco queda autorizado para obtener información sobre relaciones comerciales del Titular de la información con otras entidades y consultar sus reportes ante las centrales de información; para ello se autoriza de manera expresa, previa e irrevocable al Banco a realizar ante cualquier operador de centrales de información, entre ellos Cifín o Data crédito, cualquier operación o tratamiento efectuado sobre la información y los datos entregados, tanto del Titular de la información, como de sus representantes o directivos, incluyendo la consulta, solicitud, suministro, reporte, procesamiento y divulgación de toda la información relacionada con el comportamiento crediticio del Titular de la información, el origen de las obligaciones a su cargo, cualquier novedad, modificación, extinción, cumplimiento o incumplimiento de obligaciones. El Banco queda autorizado para verificar el comportamiento del Titular de la Información en las relaciones establecidas con cualquier otra entidad, bien directamente ante tal entidad o bien a través de un operador de la información	Perfilamiento financiero y comercial	Santander
236	Recolectar, obtener, compilar, ofrecer, vender, intercambiar, enviar, divulgar, modificar, emplear, almacenar, procesar, transferir a cualquier título, y, en general, administrar información proveniente de: el Titular de la Información, del titular de los datos o sus legítimos representantes; de las fuentes de información con las que Banco celebre convenios o contratos para el efecto; de los registros, documentos o publicaciones a los cuales haya tenido acceso Banco; de otros bancos de datos o archivos de información cuyo objeto sea o no similar al de Banco; de autoridades públicas, nacionales o internacionales, que administren o lleven registros del cumplimiento e incumplimiento de obligaciones fiscales, parafiscales, relacionadas con la prevención del blanqueo o lavado de activos o de la financiación del terrorismo y cualquier otra información de carácter público; de bases de información pública y, en general, de cualquier otra permitida por la normatividad aplicable;	Prevención del terrorismo, lavado de activos, actividades ilegales	Santander
237	El Banco debidamente autorizado por el Titular de la Información, podrá suministrar la información que reposa en sus bases de datos a las siguientes personas: a los titulares, a las personas debidamente autorizadas por éstos y a sus causahabientes; a los usuarios de la información, dentro de los parámetros de la ley, de los contratos o convenios suscritos por Banco; a cualquier autoridad judicial o administrativa, previa orden judicial o administrativa; a las entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información corresponda directamente al cumplimiento de alguna de sus funciones; a los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación en curso; a operadores de datos, de acuerdo con la normatividad vigente, y, en general a las demás personas autorizadas por la ley;	Cumplimiento de deberes ante autoridades	Santander
238	Para efectos de soportes operativos, de procesamiento de información o tecnológicos, Banco queda expresamente autorizado, para compartir la información con empresas dedicadas a labores de “outsourcing” o prestación de servicios soportes para entidades financieras, dentro o fuera de Colombia, autorizando el Titular de la Información la divulgación, suministro y cesión de la información, para cuyo efectos Banco podrá recolectar, obtener, compilar, ofrecer, vender, intercambiar, enviar, divulgar, modificar, emplear, almacenar, procesar, transferir a cualquier título y, en general, hacer todo lo que implica la administración de información para terceros, dentro o fuera de Colombia. Cuando se haga entrega o cesión de información a otros países se realizará con observancia de la Constitución Política de Colombia, la ley, la jurisprudencia y las instrucciones de las autoridades colombianas en la materia.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Santander

239	Con la finalidad de ser ofrecidos al Titular de la Información otros productos o servicios financieros, comerciales o para realizar gestiones de mercadeo, tanto por Banco como por cualquier otra entidad filial de Banco o vinculada con Banco, nacional o internacionalmente, se autoriza a compartir la información entregada tanto de la entidad como de sus administradores o apoderados.	Mercadeo propio y de terceros autorizados	Santander
240	Con la finalidad que Banco realice el procesamiento o la producción de sistemas, se autoriza compartir tal información con entidades vinculadas al denominado Grupo Santander que se dediquen a la prestación de esa clase de servicios, tales como Ingeniería de Software Bancario, S.L., Isban Chile S.A. (www.isban.com), Produban Servicios Informáticos, S.L. (www.inteqsoft.com.mx) o, Geoban, S.A. (www.geoban.com).	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Santander
241	Prevenir el fraude o mi suplantación.	Prevención fraude contra la identidad	Mundo Mujer
242	Ser utilizados como medio de prueba.	Prevención fraude contra la identidad	Mundo Mujer
243	Verificar mi identidad (incluso mediante biometría).	Prevención fraude contra la identidad	Mundo Mujer
244	Realizar procesos de actualización de mi información.	Misional	Mundo Mujer
245	Dar cumplimiento a las obligaciones que hemos pactado.	Contractual	Mundo Mujer
246	Dar atención oportuna a sus peticiones, quejas y/o reclamos.	Misional	Mundo Mujer
247	Realizar análisis de perfil de riesgos y calificación de cartera.	Perfilamiento financiero y comercial	Mundo Mujer
248	Realizar estudios mediante encuestas para conocer la calidad y el nivel de satisfacción de los productos o servicios que ha adquirido.	Misional	Mundo Mujer
249	Gestionar, mediante actividades de cobranza jurídica o prejurídica, el cobro y el recaudo de las obligaciones crediticias que ha contraído.	Misional	Mundo Mujer
250	Desarrollar los procesos que se requieran para la adecuada prestación de los productos y/o servicios que ha contraído.	Misional	Mundo Mujer
251	Consultar, reportar y actualizar la información y los datos relacionados con su comportamiento financiero y comercial (cumplimiento de sus obligaciones contractuales).	Perfilamiento financiero y comercial	Mundo Mujer
252	Ofrecerle y suministrarle, mediante llamada telefónica, mensaje de texto (SMS y/o MMS), mensaje de datos y/u otra mensajería ajustada a la Ley 527/99, correo electrónico, Facebook, Twitter, Instagram o cualquier red social de integración o mensajería instantánea; información comercial, publicitaria o promocional sobre los productos y/o servicios, eventos y/o promociones de tipo comercial que ofrece el Banco.	Mercadeo propio y de terceros autorizados	Mundo Mujer
253	Generar y/o enviar y/o entregar mediante llamada telefónica, mensaje de texto (SMS y/o MMS), mensaje de datos y/u otra mensajería ajustada a la Ley 527/99, correo electrónico, Facebook, Twitter, Instagram o cualquier red social de integración o mensajería instantánea; correspondencia, mensajes y/o notificaciones mediante el uso de correo electrónico, correo postal, teléfono fijo, celular, SMS, MSM, redes sociales o medios similares.	Comunicación cliente	Mundo Mujer
254	Realizar análisis de fraude, corrupción y otras actividades ilegales, así como de lavado de activos y financiación del terrorismo.	Prevención del terrorismo, lavado de activos, actividades ilegales	Mundo Mujer

255	Realizar transacciones, tales como retiros, compras, pagos, o similares, a través de medios presenciales o no presenciales, ya sea en Colombia o en el exterior.	Misional	Mundo Mujer
256	Ejercer su derecho de conocer de manera suficiente al usuario con quien se propone entablar relaciones, prestar servicios, y valorar el riesgo presente o futuro de las mismas relaciones y servicios.	Perfilamiento financiero y comercial	Mibanco
257	Efectuar las gestiones pertinentes para el desarrollo de la etapa precontractual, contractual y postcontractual con MIBANCO S.A., respecto de cualquiera de los productos o servicios ofrecidos por MIBANCO S.A., que haya o no adquirido o respecto de cualquier relación negocial subyacente que tenga con ella, así como dar cumplimiento a la ley colombiana o extranjera y a las órdenes de autoridades judiciales o administrativas;	Misional	Mibanco
258	Realizar actividades de mercadeo, ventas y promocionales, telemarketing (mercadeo telefónico), servicio al cliente, actividades de activación de marca, premios y promociones, directamente o a través de terceros derivados de alianzas comerciales o de cualquier vínculo.	Mercadeo propio y de terceros autorizados	Mibanco
259	Implementar estrategias de relacionamiento con clientes, proveedores, accionistas y otros terceros con los cuales la Empresa tenga relaciones contractuales o legales.	Comunicación cliente	Mibanco
260	Realizar invitaciones a eventos, mejorar productos y servicios u ofertar nuevos productos, y todas aquellas actividades asociadas a la relación comercial o vínculo existente con MIBANCO S.A., o aquel que llegare a tener.	Mercadeo propio y de terceros autorizados	Mibanco
261	Gestionar trámites (solicitudes, quejas, reclamos), efectuar encuestas de satisfacción respecto de los bienes y servicios de MIBANCO S.A. o empresas vinculadas y los aliados comerciales de MIBANCO S.A.	Misional	Mibanco
262	Dar a conocer, transferir y/o trasmitir datos personales dentro y fuera del país a sus accionistas, compañías matrices, filiales o subsidiarias de MIBANCO S.A. o a terceros a consecuencia de un contrato, ley o vínculo lícito que así lo requiera o para implementar servicios de computación en la nube.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Mibanco
263	Ordenar, catalogar, clasificar, dividir o separar la información suministrada por los titulares de datos.	Misional	Mibanco
264	Verificar, corroborar, comprobar, validar, investigar o comparar la información suministrada por los titulares de datos, con cualquier información de que disponga legítimamente, como relaciones comerciales.	Perfilamiento financiero y comercial	Mibanco
265	Acceder, consultar, comparar y evaluar toda la información que sobre el Titular se encuentre almacenada en las bases de datos de cualquier central de riesgo crediticio, financiero, de antecedentes judiciales o de seguridad, de naturaleza estatal o privada, nacional o extranjera, o cualquier base de datos comercial o de servicios, que permita establecer de manera integral e histórica completa, el comportamiento que como deudor, usuario, cliente, garante, endosante, afiliado, beneficiario, suscriptor, contribuyente y/o como titular de servicios financieros, comerciales o de cualquier otra índole.	Perfilamiento financiero y comercial	Mibanco

266	Para fines de seguridad de las personas, los bienes e instalaciones de MIBANCO S.A. y podrán ser utilizados como prueba en cualquier tipo de proceso, respecto de los datos (i) recolectados directamente en los puntos de seguridad, (ii) tomados de los documentos que suministran las personas al personal de seguridad y (iii) obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de MIBANCO S.A., éstos se utilizarán para fines de seguridad de las personas, los bienes e instalaciones de MIBANCO S.A. y podrán ser utilizados como prueba en cualquier tipo de proceso	Seguridad	Mibanco
267	Conocer, almacenar y procesar toda la información suministrada por los titulares de datos en una o varias bases de datos, en el formato que estime más conveniente.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Mibanco
268	Realizar todas las gestiones de orden tributario, contable, fiscal y de facturación necesaria para el desarrollo del objeto social de MIBANCO S.A.	Misional	Mibanco
269	Para cumplir con las obligaciones derivadas de los contratos comerciales y demás negocios jurídicos que celebra SERFINANZA en desarrollo de su actividad principal.	Contractual	Serfinanza
270	Para el cumplimiento de las obligaciones y/o compromisos derivados de las relaciones, contractuales o no, existentes con sus grupos de interés.	Contractual	Serfinanza
271	Para el cumplimiento de las obligaciones legales que involucren datos personales de sus grupos de interés.	Contractual	Serfinanza
272	Para el cumplimiento de órdenes de autoridades judiciales o administrativas.	Cumplimiento de deberes ante autoridades	Serfinanza
273	Para la gestión comercial, venta cruzada y relacionamiento con sus grupos de interés.	Mercadeo propio y de terceros autorizados	Serfinanza
274	Para la gestión de cartera y cobranza en el marco del régimen de habeas data financiero.	Misional	Serfinanza
275	Para comunicar a sus grupos de interés información sobre sus bienes, servicios, publicaciones, eventos de capacitación, actividades comerciales y publicidad asociada a su actividad empresarial, sea que se realice de manera directa o no.	Mercadeo propio y de terceros autorizados	Serfinanza
276	Para determinar con base en la información del cliente, sus gustos y preferencias, así como su capacidad de endeudamiento, perfilamiento y segmentación en el tipo de crédito al cual puede acceder con la entidad.	Perfilamiento financiero y comercial	Serfinanza
277	Para desplegar hacia sus grupos de interés actividades de responsabilidad social empresarial.	Perfilamiento no financiero	Serfinanza
278	Para gestionar la seguridad de las personas, bienes y activos de información en custodia de la organización.	Seguridad	Serfinanza
279	Para la adopción de medidas tendientes a la prevención de actividades ilícitas.	Prevención del terrorismo, lavado de activos, actividades ilegales	Serfinanza
280	El tratamiento tendrá como fin la gestión administrativa de los datos personales de directores, empleados, contratistas, proveedores y clientes. Incluyendo dentro de esta gestión administrativa, la vinculación, gestión de nómina y de beneficios prestacionales, prestación de servicios, pagos, trámites de facturación, retiro o terminación,	Misional	J.P. MORGAN COLOMBIA

	reporte a autoridades administrativas y judiciales cuando así sea requerido, y en general, el proceso de gestión		
281	- Para validar tu identidad	Prevención fraude contra la identidad	Lulo Bank
282	Para cumplirte nuestras obligaciones.	Contractual	Lulo Bank
283	Para validar tus referencias.	Prevención fraude contra la identidad	Lulo Bank
284	- Para contactarte en el desarrollo de tu relación con Lulo Bank, y para responder consultas, reclamos o quejas, y demás peticiones.	Comunicación cliente	Lulo Bank
285	Para informarte cambios en nuestros procesos administrativos.	Comunicación cliente	Lulo Bank
286	Para administrar el riesgo de fraude, de robo, de hurto, de lavado de activos, de financiación del terrorismo, reputacional, de crédito u otros riesgos que deba administrar Lulo Bank, según aplique.	Prevención del terrorismo, lavado de activos, actividades ilegales	Lulo Bank
287	Para cumplir nuestras obligaciones con las autoridades, judiciales o administrativas.	Cumplimiento de deberes ante autoridades	Lulo Bank
288	- Para obtener y presentar pruebas ante terceros	Prevención fraude contra la identidad	Lulo Bank
289	- Para colaborar con la justicia y con las demás autoridades administrativas.	Cumplimiento de deberes ante autoridades	Lulo Bank
290	Para cumplir las normas sobre conflictos de interés.	Cumplimiento de deberes ante autoridades	Lulo Bank
291	Para brindar seguridad a las personas y bienes en las instalaciones de Lulo Bank, en caso de visita.	Seguridad	Lulo Bank
292	- Para identificar y controlar enfermedades altamente contagiosas, o que deban ser manejadas con procedimientos específicos en las instalaciones de Lulo Bank, solamente en caso de visita, y específicamente para proteger a los demás visitantes.	Bioseguridad	Lulo Bank
293	Consultar, actualizar, procesar, reportar y suprimir mis Datos Personales en centrales de riesgo y administradoras de bases de datos de bureau crediticio, así como en listas de control y/o bases de datos asociadas al Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.	Prevención del terrorismo, lavado de activos, actividades ilegales	BTG Pactual Colombia
294	Contactar telefónicamente, por vía electrónica, escrita o personalmente, con el fin de: i) informar sobre los productos y servicios que ofrece BTG Pactual; ii) Suministrar información relacionada con el portafolio de productos que tenga con BTG PACTUAL y todo lo relacionada con el desarrollo del contrato suscrito con BTG Pactual; iii) Actualizar la información que anualmente por su naturaleza pueda variar o que por disposición legal deba ser actualizada; iv) Enviar o suministrar información de los programas publicitarios de BTG Pactual; v) Evaluar la calidad de nuestros productos y servicios	Comunicación cliente	BTG Pactual Colombia

295	Realizar análisis estadísticos con los Datos Personales de los Clientes;	Mercadeo propio y de terceros autorizados	BTG Pactual Colombia
296	Atender adecuadamente peticiones, solicitudes, quejas o reclamos formuladas por autoridades judiciales y administrativas;	Misional	BTG Pactual Colombia
297	Compartir la información con entidades del Grupo BTG Pactual en el exterior, incluyendo, pero sin limitarse a Banco BTG Pactual S.A. (Brasil), BTG Pactual Cayman Branch, BTG Pactual Chile S.A. para llevar a cabo actividades que apoyan el desarrollo y monitoreo de las operaciones realizas por BTG Pactual dentro del cumplimiento de las políticas y procedimientos de los Sistemas de Administración de Riesgos y del Sistema de Control Interno.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	BTG Pactual Colombia
298	Compartir la información con las demás entidades de BTG Pactual, incluyendo, pero sin limitarse a BTG Pactual Sociedad Fiduciaria S.A., BTG Pactual Sociedad Comisionista de Bolsa S.A., sus subordinadas, matrices y subordinadas de sus matrices. para el ofrecimiento de productos y servicios propios de dichas entidades.	Mercadeo propio y de terceros autorizados	BTG Pactual Colombia
299	Compartir la información con terceros para el desarrollo de las labores relacionadas con las actividades del objeto social, tales como como depósitos de valores, bolsas de valores, sistemas de negociación, cámaras centrales de riesgos, cámaras de riesgos de divisas, compañías de mensajería, contrapartes, emisores, proveedores de infraestructura, entre otras.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	BTG Pactual Colombia
300	Suministrar la información al Revisor Fiscal para el desarrollo de sus labores, conforme la normativa vigente	Misional	BTG Pactual Colombia
301	Compartir la información con terceros con quien BTG Pactual tenga relaciones contractuales necesarias para el desarrollo de su objeto social, y que conlleven la Transmisión o Transferencia de Datos.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	BTG Pactual Colombia
302	Enviar la información a autoridades administrativas como la DIAN, Superintendencias, entre otras, con el fin de dar cumplimiento a disposiciones legales aplicables.	Cumplimiento de deberes ante autoridades	BTG Pactual Colombia
303	Enviar información al Cliente mediante: llamada telefónica, mensaje de texto, correo electrónico, Facebook, Twitter, Instagram o cualquier red social utilizada por BTG Pactual.	Comunicación cliente	BTG Pactual Colombia
304	Tratar mis datos biométricos tales como reconocimiento facial o dactilar con el fin de desarrollar una efectiva verificación de la identidad y prevenir el fraude. Entendiendo que estos son considerados Datos Sensibles y que no estoy obligado a autorizar su tratamiento.	Prevención fraude contra la identidad	BTG Pactual Colombia
305	Almacenarlos por el tiempo definido en la regulación vigente aplicable.	Misional	BTG Pactual Colombia
306	Las demás que surjan en el desarrollo de la relación contractual.	No determinada	BTG Pactual Colombia
307	Estudiar y atender las solicitudes de servicios y productos solicitados en los que participe como deudor, codeudor, avalista, fiador, o en cualquier otro carácter	Misional	Agrario
308	Para realizar el proceso de conocimiento del cliente y obtener mayor seguridad en el desarrollo de las diferentes transacciones que se realicen a través de los canales con los que desarrollo de las diferentes transacciones que se realicen a través de los canales con los que cuenta el Banco.	Perfilamiento financiero y comercial	Agrario

309	Realizar la consulta en las centrales de información	Perfilamiento financiero y comercial	Agrario
310	Desarrollar las gestiones necesarias para dar adecuado cumplimiento a las obligaciones que se deriven de los contratos celebrados con el Banco.	Contractual	Agrario
311	Llevar a cabo el seguimiento de las obligaciones y adelantar la gestión de cobranza de las mismas.	Misional	Agrario
312	Consolidar la información personal, para efectos de realizar análisis, estudios de mercadeo, actividades de suministro de información, así como la promoción y comercialización de los distintos productos y servicios ofrecidos por el Banco.	Mercadeo propio y de terceros autorizados	Agrario
313	Ofrecer conjunta o separadamente con terceros, servicios financieros y comerciales.	Mercadeo propio y de terceros autorizados	Agrario
314	Realizar el seguimiento, control, desarrollo y/o mejoramiento de las condiciones de procesos, productos, servicios y canales del Banco.	Misional	Agrario
315	Implementar planes de mercadeo, campañas, beneficios especiales y promociones.	Mercadeo propio y de terceros autorizados	Agrario
316	Ejecutar actividades, controles y seguimiento a los procesos de evaluación y calificación de cartera.	Misional	Agrario
317	Ejecutar actividades y controles en el proceso de solicitud, análisis, otorgamiento y seguimiento de operaciones de crédito.	Misional	Agrario
318	Ejecución y control de actividades y trámites contables y de procesos de administración tributaria.	Misional	Agrario
319	Realizar análisis de riesgo, estadísticas, supervisión, encuestas, pruebas de mercadeo, comercialización de productos y de actualización y verificación de información.	Perfilamiento financiero y comercial	Agrario
320	Desarrollar e implementar herramientas de prevención de fraudes	Prevención fraude contra la identidad	Agrario
321	Usar, recolectar, almacenar transmitir y transferir los datos sensibles obtenidos con ocasión de cualquier operación y/o gestión que realice con el Banco	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Agrario
322	Para hacer la lectura y utilización de mi huella dactilar con el fin de validar mi identidad con dicho organismo, para el proceso en curso y garantizar mayor seguridad en la prevención del fraude y la suplantación	Prevención fraude contra la identidad	Caja Social
323	Para que mi huella digital y registro fotográfico se recolecten, almacenen, usen, circulen, supriman y, en general, se traten en procesos de identificación para garantizar mi seguridad y prevenir el fraude o la suplantación.	Prevención fraude contra la identidad	Caja Social
324	Para solicitarme información relacionada con mi comportamiento financiero, comercial y crediticio, así como el cumplimiento de mis obligaciones crediticias y los provenientes de terceros países, incluyendo los aportes al Sistema de Seguridad Social. Esto implica	Perfilamiento financiero y comercial	Caja Social

	consultarla, confirmarla, reportarla, analizarla, actualizarla, conservarla y retirarla		
325	Para cumplir con los derechos y exigir las obligaciones de la relación contractual y su objeto social directamente o a través de terceros contratados por el Banco (encargados) por ejemplo, extractos, notificaciones, actividades de cobranza, entrega de correspondencia, procesos operativos o de riesgos, proveedores de tecnología, entre otros, e implementar medidas de seguridad para proteger la identidad del titula	Misional	Caja Social
326	Para transferirla a autoridades nacionales o internacionales, en cumplimiento de las normas sobre prevención de actividades ilícitas y el intercambio de datos para efectos tributarios	Cumplimiento de deberes ante autoridades	Caja Social
327	Para compartirla con las cámaras de riesgo central de la contraparte, Deceval S.A. o cualquier otro depósito centralizado de valores o entidad de certificación, con el propósito de que la administre y se la deje disponible a los depositantes directos que acceden a sus sistemas	Perfilamiento financiero y comercial	Caja Social
328	Para compartir mis datos personales con entidades establecidas para apoyar el desarrollo empresarial productivo y/o bancos de segundo piso, fondos de garantías, agremiaciones, entre otros	Perfilamiento financiero y comercial	Caja Social
329	Para actualizar, conservar, procesar, recopilar y utilizar mi información personal o la documentación entregada en virtud de la relación contractual.	Procesamiento, circulación y transferencia a través de sus redes operativas nacionales y/o en el exterior	Caja Social
330	Para que me brinden asesoría o asistencia en la administración de los productos y servicios de la entidad	Misional	Caja Social
331	Para enviarme a la dirección de correo electrónico y demás datos de contacto que registre, las comunicaciones y reportes de tipo legal y comercial que el Banco requiera remitirme.	Comunicación cliente	Caja Social
332	Para compartir mis datos de contacto y de titularidad de productos financieros con las entidades que son parte del Conglomerado Financiero al que el Banco Caja Social pertenece y con entidades de la Organización de la que éste hace parte, para ofrecerme productos y servicios complementarios a los ofrecidos por el Banco. Los nombres de las entidades referidas se encuentran publicados en el aviso de privacidad que se puede consultar en el sitio web de la entidad	Mercadeo propio y de terceros autorizados	Caja Social
333	Para el ofrecimiento de bienes, productos y servicios que puedan ser de mi interés, mediante la realización de campañas comerciales o el desarrollo de convenios de marca compartida	Mercadeo propio y de terceros autorizados	Caja Social
334	Para hacer estudios sobre mis gustos, hábitos e intereses:	Perfilamiento financiero y comercial	Caja Social
335	Para que terceros me ofrezcan bienes, productos o servicios financieros complementarios a los adquiridos con el Banco:	Mercadeo propio y de terceros autorizados	Caja Social

Anexo F. Listado tipos de banca y mecanismos de autenticación implementados por los establecimientos bancarios de Colombia

Mecanismo Autenticación	Factor	Mecanismo	Encontrado	Entidad
Clave único uso (One Time Password - OTP)	Segundo	SMS		Av Villas
Usuario y Clave/contraseña	Primer			Av Villas
Banca Móvil			Si	Av Villas
Biometría en banca móvil			No lo dice	Av Villas
Token físico	Segundo	Dispositivo		Av Villas
Usuario y Clave/contraseña	Primer			Bancamía
Banca Móvil			Si	Banco Agrario
Biometría en banca móvil			No lo dice	Banco Agrario
Registro direcciones Ips /Móvil	Segundo			Banco Agrario
Token por software	Segundo	SMS		Banco Agrario
Usuario y Clave/contraseña	Primer			Banco Agrario
Imagen /pregunta/ frase de seguridad	Segundo			Banco Agrario
banca telefónica			Si	Banco w
Clave telefónica	Primer			Banco w
Banca Móvil			No lo dice	Banco w
Biometría en banca móvil			No lo dice	Banco w
Clave único uso (One Time Password - OTP)	Segundo			Banco w
Token físico	Segundo			Banco w
Token por software	Segundo	App		Bancolombia
Usuario y Clave/contraseña	Primer			Bancolombia
Banca Móvil			Si	Bancolombia
Biometría en banca móvil	Segundo	Huella/ Reconocimiento facial	SI	Bancolombia
Clave único uso (One Time Password - OTP)	Segundo			Bancolombia
Banca Móvil			Si	BANCOOMEVA
Usuario y Clave/contraseña	Primer			BANCOOMEVA
Imagen /pregunta/ frase de seguridad	Segundo			BANCOOMEVA
Token físico	Segundo	Dispositivo		BANCOOMEVA
Clave único uso (One Time Password - OTP)	Segundo	SMS		BANCOOMEVA

Biometría en banca móvil	Segundo	Huella	Si	BANCOOMEVA
Usuario y Clave/contraseña	Primer			BBVA
Clave único uso (One Time Password - OTP)	Segundo	SMS		BBVA
Token por software	Segundo			BBVA
Banca Móvil			Si	BBVA
Biometría en banca móvil	Segundo	huella, reconocimiento facial	SI	BBVA
Usuario y Clave/contraseña	Primer			Bogotá
Token por software	Segundo	App		Bogotá
Biometría en banca móvil	Segundo	Reconocimiento facial y prueba de vida	SI	Bogotá
Banca Móvil			Si	Bogotá
Clave único uso (One Time Password - OTP)	Segundo	SMS		Bogotá
Usuario y Clave/contraseña	Primer			Btg Pactual
Usuario y Clave/contraseña	Primer			CAJA SOCIAL
Token físico	Segundo	Dispositivo		CAJA SOCIAL
Imagen /pregunta/ frase de seguridad	Segundo			CAJA SOCIAL
Banca Móvil			Si	CAJA SOCIAL
Biometría en banca móvil			No lo dice	CAJA SOCIAL
Registro direcciones Ips /Móvil	Segundo			CAJA SOCIAL
Clave único uso (One Time Password - OTP)	Segundo			CAJA SOCIAL
Banca Móvil			Si	Citibank
Biometría en banca móvil	Segundo		SI	Citibank
Token por software	Segundo	App		Citibank
Usuario y Clave/contraseña	Primer			Citibank
Usuario y Clave/contraseña	Primer			Coopcentral
Token físico	Segundo	Dispositivo		Coopcentral
Clave único uso (One Time Password - OTP)	Segundo	SMS		Coopcentral
Banca Móvil			Si	Coopcentral
Biometría en banca móvil			No lo dice	Coopcentral
Usuario y Clave/contraseña	Primer			Credifinanciera
Registro direcciones Ips /Móvil	Segundo			Credifinanciera
Banca Móvil			No lo dice	Credifinanciera
Biometría en banca móvil			No lo dice	Credifinanciera
Token por software	Segundo			Credifinanciera

Token físico	Segundo	App		Davivienda
Usuario y Clave/contraseña	Primer			Davivienda
Clave único uso (One Time Password - OTP)	Segundo	SMS		Davivienda
Banca Móvil			Si	Davivienda
Biometría en banca móvil			No lo dice	Davivienda
Banca Móvil			Si	Falabella
Biometría en banca móvil			No lo dice	Falabella
Token por software	Segundo			Falabella
Usuario y Clave/contraseña	Primer			Falabella
Banca Móvil			Si	Finandina
Biometría en banca móvil			No lo dice	Finandina
Usuario y Clave/contraseña	Primer			Finandina
Token por software	Segundo	App		Finandina
Token físico	Segundo	Dispositivo		Finandina
Token físico	Segundo	Dispositivo		Itaú
Imagen /pregunta/ frase de seguridad	Segundo			Itaú
Registro direcciones Ips /Móvil	Segundo			Itaú
Usuario y Clave/contraseña	Primer			Itaú
Clave único uso (One Time Password - OTP)	Primer			Itaú
Usuario y Clave/contraseña	Primer			J.P. MORGAN COLOMBIA
Banca Móvil			Si	J.P. MORGAN COLOMBIA
Biometría en banca móvil	Segundo		SI	J.P. MORGAN COLOMBIA
Token físico	Segundo			J.P. MORGAN COLOMBIA
Token por software	Segundo			J.P. MORGAN COLOMBIA
Usuario y Clave/contraseña	Primer			Lulo Bank
Clave único uso (One Time Password - OTP)	Segundo	SMS		Lulo Bank
Banca Móvil			Si	Lulo Bank
Biometría en banca móvil	Segundo	Reconocimiento facial	SI	Lulo Bank
Token físico			No lo dice	Mibanco
Clave único uso (One Time Password - OTP)			No lo dice	Mibanco
Banca Móvil			No lo dice	Mibanco
Biometría en banca móvil			No lo dice	Mibanco

Usuario y Clave/contraseña	Primer			Mibanco
Clave único uso (One Time Password - OTP)	Segundo	SMS		Mundo Mujer
Banca Móvil			Si	Mundo Mujer
Biometría en banca móvil			No lo dice	Mundo Mujer
Usuario y Clave/contraseña	Primer			Mundo Mujer
Imagen /pregunta/ frase de seguridad	Segundo			Mundo Mujer
Token físico	Segundo	Dispositivo		Occidente
Token por software	Segundo	App		Occidente
Clave único uso (One Time Password - OTP)	Segundo	SMS		Occidente
Usuario y Clave/contraseña	Primer			Occidente
Banca Móvil			Si	Occidente
Biometría en banca móvil	Segundo	huella	SI	Occidente
Banca Móvil			Si	Pichincha
Biometría en banca móvil			No lo dice	Pichincha
Usuario y Clave/contraseña	Primer			Pichincha
Clave único uso (One Time Password - OTP)	Segundo	SMS		Pichincha
Token por software	Segundo	App		Pichincha
Biometría en banca móvil			No lo dice	Popular
Banca Móvil			Si	Popular
Clave único uso (One Time Password - OTP)	Segundo	SMS		Popular
Usuario y Clave/contraseña	Primer			Popular
Token físico	Segundo	Dispositivo		Santander
Usuario y Clave/contraseña	Primer			Santander
Clave único uso (One Time Password - OTP)	Segundo	App		Santander
Banca Móvil			No lo dice	Santander
Biometría en banca móvil			No lo dice	Santander
Banca Móvil			Si	SCOTIABANK COLPATRIA
Biometría en banca móvil			No lo dice	SCOTIABANK COLPATRIA
Clave único uso (One Time Password - OTP)	Segundo	SMS		SCOTIABANK COLPATRIA
Usuario y Clave/contraseña	Primer			SCOTIABANK COLPATRIA
Token físico	Segundo	Dispositivo		Serfinanza
Usuario y Clave/contraseña	Primer			Serfinanza
Clave único uso (One Time Password - OTP)	Segundo	SMS		Serfinanza

Banca Móvil			Si	Serfinanza
Biometría en banca móvil	Segundo	huella	SI	Serfinanza
Registro direcciones Ips /Móvil	Segundo			Serfinanza
Imagen /pregunta/ frase de seguridad	Segundo			Serfinanza
Token por software	Segundo	App		Sudameris
Usuario y Clave/contraseña	Primer			Sudameris
Banca Móvil			Si	Sudameris
Biometría en banca móvil			No lo dice	Sudameris

Anexo G. Resumen Analítico Especializado

Fecha de Realización:	20/06/2023
Programa:	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Línea de Investigación:	INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD EN REDES
Título:	CIBERSEGURIDAD DE LA IDENTIDAD DIGITAL EN LAS TRANSACCIONES ELECTRÓNICAS BANCARIAS EN COLOMBIA
Autor(es):	SÁNCHEZ PEÑA DIEGO ANDRÉS
Palabras Claves:	Identidad digital, gestión de la identidad digital, suplantación de identidad, protección de datos.
Descripción:	El análisis de los aspectos relevantes a la ciberseguridad de la identidad digital en las transacciones electrónicas bancarias en Colombia ante la amenaza de suplantación de la identidad es un trabajo de grado en modalidad de monografía que presenta el estado de las características o rasgos importantes a dicha gestión en operaciones bancarias virtuales disponibles a usuarios a través de teléfonos inteligentes e internet. El trabajo se realiza mediante una revisión sistemática de literatura dentro de los diferentes entornos jurídicos, de gobernanza y tecnológico en tiempos de incremento del uso intensivo de medios electrónicos y redes sociales, y en particular en presencia del aumento de servicios ofrecidos por el sector bancario. El enfoque del presente trabajo revisa la información presentada por los bancos en las secciones de seguridad de sus sitios web, relacionada con las amenazas, riesgos y vulnerabilidades de la identidad digital por ellos identificados, igualmente revisa y analiza las características de ciberseguridad, particularmente los mecanismos de cara al usuario como factores de autenticación de la identidad digital dentro del contexto de transacciones electrónicas con la banca. De la misma manera, se revisan y analizan las finalidades o usos de los datos de los usuarios

	de los servicios bancarios, declaradas por los mismos en sus políticas de tratamiento de datos, sobre el entendido que del adecuado manejo que se realice de la información personal suministrada o recaudada por los bancos, se pueden derivar implicaciones relacionadas, entre otras, con la protección de la privacidad, la confianza entre los actores de transacciones bancarias y los costos económicos asociados al fraude por suplantación de la persona.

Fuentes bibliográficas destacadas:

ASOBANCARIA. [En línea]. Impacto económico y social del phishing y el smishing en Colombia y el mundo. [Consultado el 6 de febrero de 2022]. Disponible en: https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf

BANCO AGRARIO. [En línea]. Tips de seguridad. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.bancoagrario.gov.co/canales/Seguridad/Paginas/default.aspx

BANCO AGRARIO DE COLOMBIA. [En línea]. Política Protección de Datos Personales Banco Agrario de Colombia. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.bancoagrario.gov.co/SAC/Documents/DocTratamientoDatosPersonales.pdf

BANCO AV VILLAS. [En línea]. Centro de Entrenamiento - Antifraude AV Villas. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.avvillas.com.co/avvillas/seccionseguridad/index.html

BANCO AV VILLAS. [En línea]. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: https://www.avvillas.com.co/wps/wcm/connect/avvillas/b3326505-307e-403c-8c5c-f3e46681eec8/Politica-Proteccion-Datos-Personales-def.pdf?MOD=AJPERES&CVID=m8L62VU#:~:text=El%20Banco%20AV%20Villas%20garantiza,autorizados%20conforme%20a%20la%20ley.

BANCO BANCOLOMBIA. [En línea]. Política para el tratamiento de datos personales de BANCOLOMBIA S.A. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/personas/documentos-legales/proteccion-datos/bancolombia-sa#:~:text=Principios%20Rectores%20del%20Tratamiento%20De%20Datos%20Personales&text=Principio%20de%20libertad%3A%20BANCOLOMBIA%20S.A.,de%20mandato%20legal%20o%20judicial.

BANCO BANCOLOMBIA. [En línea]. Seguridad informática - Protección frente a ataques cibernéticos. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/educacion-financiera/seguridad-bancaria

BANCO BANCOLOMBIA. [En línea]. ¿Cómo activo el ingreso con huella a App Bancolombia? [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancolombia.com/centro-de-ayuda/preguntas-frecuentes/ingreso-con-huella-app-personas
BANCO BANCOLOMBIA. [En línea]. Uso de redes sociales en pandemia: la transformación hacia lo digital. [Consultado el 10 de diciembre de 2021]. Disponible en https://www.bancolombia.com/wps/portal/negocios/actualizate/tendencias/uso-redes-sociales-pandemia-transformacion-digital
BANCO BBVA COLOMBIA. [En línea]. Política de tratamiento de datos personales. [Consultado el 3 de mayo de 2022]. Disponible en: DO-01-Politica-tratamiento-datos-personales.pdf (bbva.com.co)
BANCO BBVA. [En línea]. Recomendaciones de seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bbva.com.co/personas/recomendaciones-de-seguridad.html
BANCO CAJA SOCIAL. [En línea]. Medidas de Seguridad en el Canal de Internet. [Consultado el 12 de mayo de 2022].Disponible en: https://www.bancocajasocial.com/portalserver/medidas-de-seguridad-en-el-canal-de-internet#:~:text=REVISE%20que%2C%20al%20ingresar%20a,computador%20personal%20actualizado%20con%20antivirus
BANCO CAJA SOCIAL. [En línea]. AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: AUTORIZACION-TRATAMIENTO-DATOS-PERSONALES.pdf (bancocajasocial.com)
BANCO DAVIVIENDA. [En línea]. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES. [Consultado el 3 de mayo de 2022]. Disponible en: Política de Protección de Datos Personales (corporacionfinancieradavivienda.com)
BANCO DAVIVIENDA. [En línea]. Seguridad. [Consultado el 12 de mayo de 2022].Disponible en: https://www.davivienda.com/wps/portal/empresas/nuevo/seguridad/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zijS0CTfy8nIx8TQy8zA0cQz0DHEN8vIy9_Yz1w8EKDHAARwP9KGL041EQhd_4cP0oVCucHb2NDBxdXQOCvJ2CjJy8jKEK8JhRkBsaYZDpqAgAbB8RKA!!/dz/d5/L2dBISEvZ0FBIS9nQSEh/
BANCO DE BOGOTÁ. [En línea]. Seguridad. [Consultado el 12 de mayo de 2022]. Disponible en: https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/atencion-al-cliente/seguridad-bancaria
BANCO DE BOGOTÁ. [En línea]. Términos y Condiciones Política de Tratamiento de Datos. [Consultado el 3 de mayo de 2022].Disponible en: https://www.bancodebogota.com/wps/themes/html/banco-de-bogota/pdf/atencion-al-cliente/terminos-y-condiciones-politica-tratamiento-datos.pdf
BANCO INTERAMERICANO DE DESARROLLO. [En línea]. Regulación de blockchain e identidad digital en América Latina | El futuro de la identidad digital.

[Consultado:12 de mayo de 2022].Disponible en: https://publications.iadb.org/publications/spanish/document/Regulacion-de-blockchain-e-identidad-digital-en-America-Latina-El-futuro-de-la-identidad-digital.pdf
CONGRESO DE LA REPÚBLICA DE COLOMBIA. [En línea].LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. [Consultado el 10 de diciembre de 2021].Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
CSIRT FINANCIERO. [En línea]. Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. [Consultado: 6 de febrero de 2022].Disponible en: https://csirtasobancaria.com/sala-de-prensa/201cdesafios-del-riesgo-cibernetico-en-el-sector-financiero-para-colombia-y-america-latina201d-publicacion-conjunta-entre-asobancaria-y-la-organizacion-de-estados-americanos-oea
INTER -AMERICAN DEVELOPMENT BANK. [En línea]. IDENTIDAD DIGITAL AUTOGESTIONADA El futuro de la identidad digital: autogestión, billeteras digitales y blockchain. [Consultado: 10 de diciembre de 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf
ISO. [En línea]. ISISO/IEC 24760-1:2019(en) IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en
ISO. [En línea].ISO/IEC 24760-2:2015(en) Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-2:ed-1:v1:en
ISO. [En línea].ISO/IEC 24760-3:2016(en) Information technology — Security techniques — A framework for identity management — Part 3: Practice. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-3:ed-1:v1:en
ITU. [En línea]. X.1251: Marco para el control por el usuario de la identidad digital. [Consultado el 10 de diciembre de 2021].Disponible en: https://www.itu.int/rec/T-REC-X.1251/es
ITU. [En línea]. X.1253: Directrices de seguridad para los sistemas de gestión de identidades. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itu.int/rec/T-REC-X.1253-201109-I/es
ITU. [En línea]. X.1254: Marco de garantía de autenticación de entidad. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.itu.int/rec/T-REC-X.1254/es
NIST. [En línea]. Digital Identity Guidelines. [Consultado el 10 de diciembre de 2021]. Disponible en: https://pages.nist.gov/800-63-3/

OKTA. [En línea]. What is Decentralized Identity? [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.okta.com/blog/2021/01/what-is-decentralized-identity/
ORGANIZACIÓN DE ESTADOS AMERICANOS. [En línea]. Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. [Consultado: 10 de diciembre de 2021]. Disponible en: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf
SUPERINTENDENCIA FINANCIERA DE COLOMBA. [En línea]. Circulares Externas. [Consultado el 10 de diciembre de 2021].Disponible en: https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/circulares-externas--10082461
SUPERINTENDENCIA FINANCIERA DE COLOMBA. [En línea]. Circulares Externas. [Consultado el 10 de diciembre de 2021]. Disponible en: https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circulares-externas-cartas-circulares-y-resoluciones-desde-el-ano-/circulares-externas/circulares-externas--10082461

Contenido del documento:

Conceptos adquiridos:	El desarrollo de esta monografía permitió adquirir conocimientos relacionados con la identidad digital, su gestión y las actuales tendencias hacia un manejo auto soberano por parte de las personas. Igualmente, permitió establecer que la gestión de la identidad digital opera dentro de un marco jurídico que protege los derechos a la intimidad, la privacidad y la protección de datos personales. Finalmente, permitió afianzar los conocimientos relacionados con las amenazas, vulnerabilidades y riesgos de la identidad digital, los mecanismos de autenticación fuerte o multifactorial y su aplicación en transacciones electrónicas bancarias en Colombia.
Conclusiones:	Las principales amenazas contra la identidad digital en transacciones electrónicas bancarias son las identificadas como *Phishing, Smishing y Vishing* en asocio de técnicas de ingeniería social. Las vulnerabilidades más importantes se encuentran en el desconocimiento, falta de previsión e impericia de los usuarios de las transacciones electrónicas bancarias. El mayor esfuerzo comunicacional de los bancos para contrarrestar el fraude por las amenazas identificadas se concentra en la publicación de información y recomendaciones generarles. Hay muy poco despliegue comunicativo de acciones particulares dentro del contexto propio de cada banco para facilitar a su cliente evitar la ocurrencia de incidentes asociados al *Phishing, Vishing y Smishing* y/o dar apoyo una vez ocurridos estos incidentes, si fuera el caso. En relación con el uso de datos personales por parte de los bancos, el “Mercadeo propio y de terceros autorizados” es la finalidad de mayor énfasis, lo que permitiría suponer que los datos personales de los usuarios bancarios pudieran caracterizarse por un grado de exposición importante que implicaría un eventual compromiso de la privacidad. El mecanismo “Usuario y Clave/contraseña” se constituye como el primer factor de autenticación usado por

	la banca. La autenticación fuerte en las transacciones electrónicas bancarias se realiza principalmente a través de mensajes tipo SMS que contienen claves temporales de único uso u OTPs y Tokens generados por software. El teléfono celular es el dispositivo sobre el cual reposa la autenticación fuerte de la identidad digital de los usuarios de transacciones electrónicas bancarias, elemento muy vulnerable a daños, pérdidas y clonación, entre otros. El uso de la biometría, mecanismo de muy alta percepción de confiabilidad, es incipiente, y solo se ofrece en modalidad de banca móvil. Los esquemas multifactoriales de autenticación de la identidad digital de usuarios en transacciones electrónicas bancarias en Colombia basados en certificados digitales e interacción on-line con entidades de confianza no están documentados. La posibilidad de fraude por suplantación presunta de persona es mayor en uso de productos bancarios asociados a transacciones electrónicas con implicaciones importantes en el relacionamiento banco – cliente. En las actuales condiciones y características de la ciberseguridad de las transacciones electrónicas bancarías en Colombia, el actor más importante y a la vez más débil, sigue siendo el usuario, ya que, del conocimiento de las modalidades de fraude, de su comportamiento y del aprovisionamiento de los elementos tecnológicos idóneos dependerá, no solo la protección de activos dinerarios, sino también su buen nombre, su tranquilidad y en últimas su calidad de vida financiera.