



Superintendencia
Financiera de Colombia



Retos importantes en seguridad y disponibilidad en el sector financiero

Francisco Espinosa Rodríguez

Superintendente Delegado para Riesgo Operacional y Ciberseguridad

**17° Congreso de seguridad, amenazas cibernéticas,
fraude y experiencia**

Cartagena de Indias, 17 de octubre de 2024



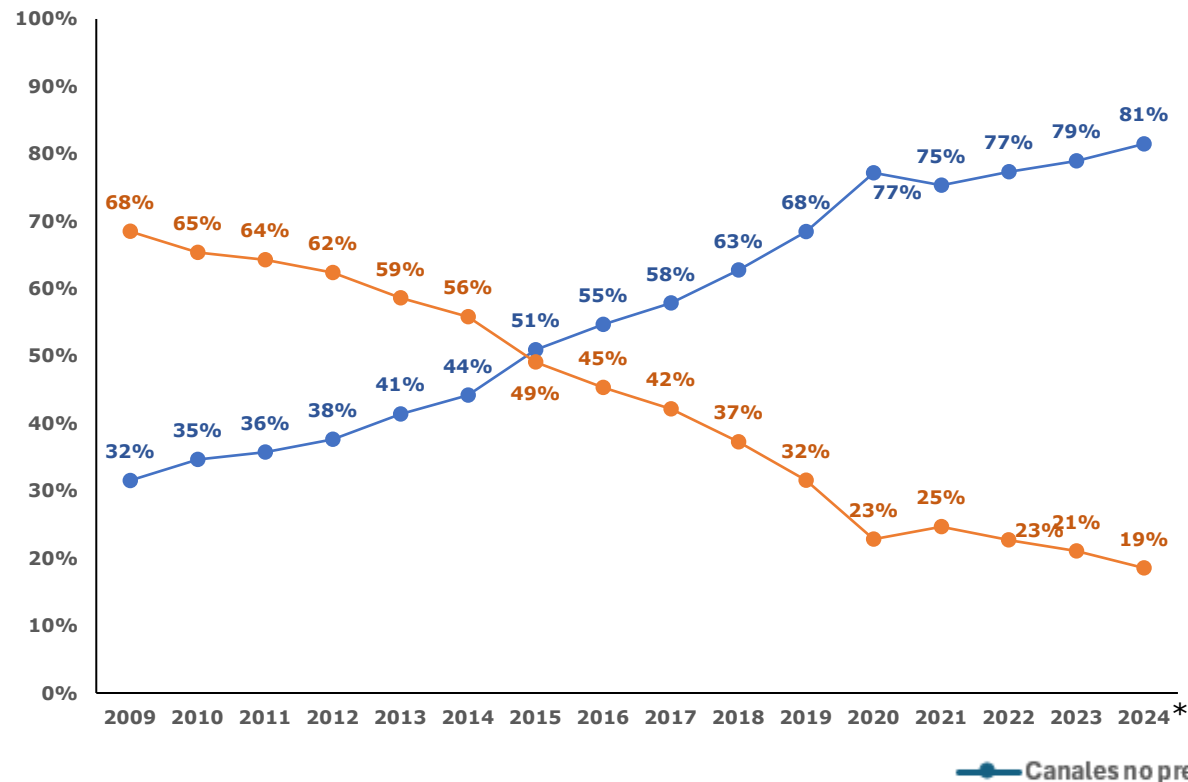
Superintendencia
Financiera de Colombia



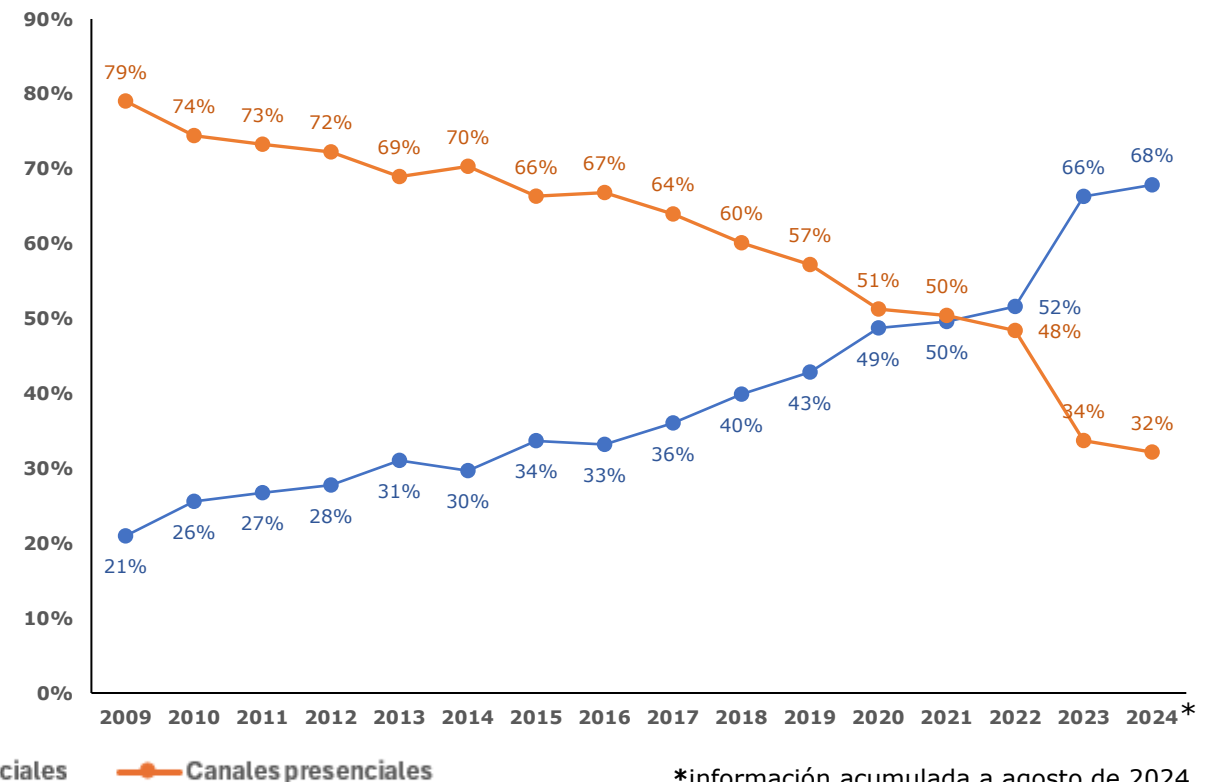
Operaciones en canales digitales

La transformación digital consolida la preferencia por los canales digitales para realizar operaciones financieras

Número de transacciones



Monto de las transacciones

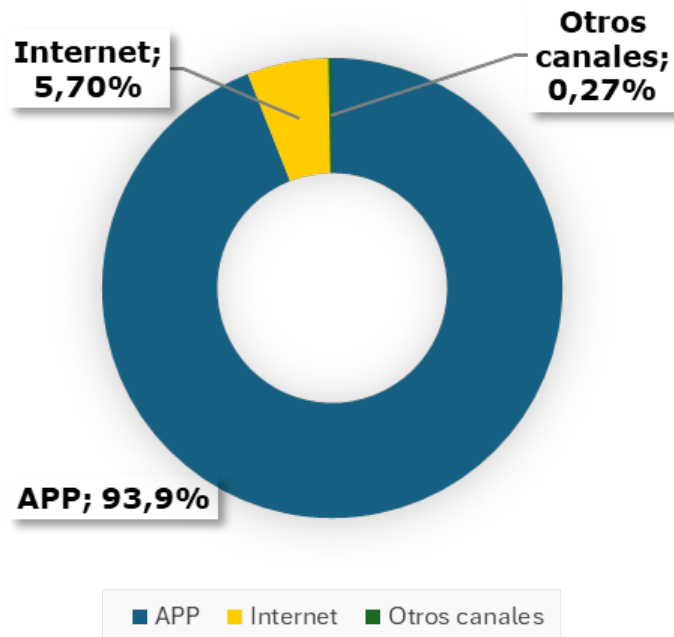


*información acumulada a agosto de 2024.

Preferencia por el uso de canales digitales en operaciones monetarias

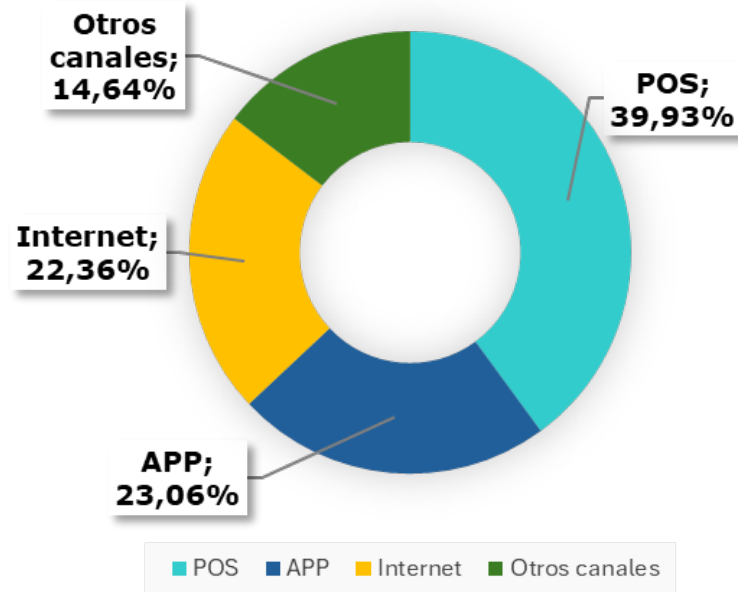
Transferencias

Las App es el canal preferido por los consumidores financieros para realizar transferencias.



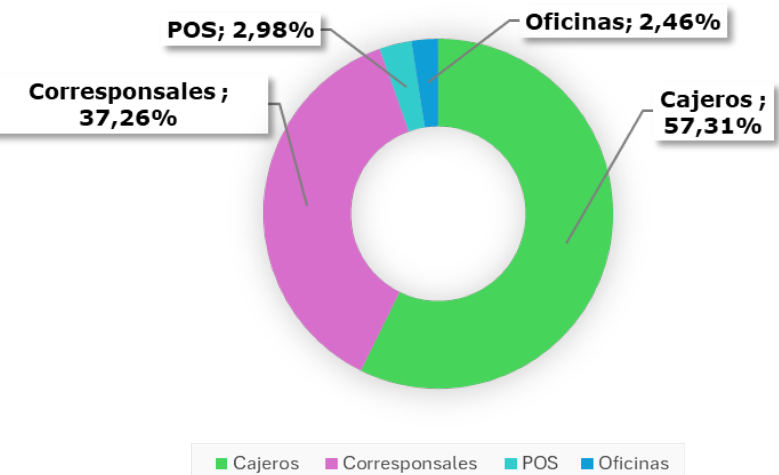
Pagos

Para realizar pagos los usuarios prefieren las POS.



Retiros

Los cajeros automáticos y los corresponsales son los canales por los que se realizan más retiros de dinero.

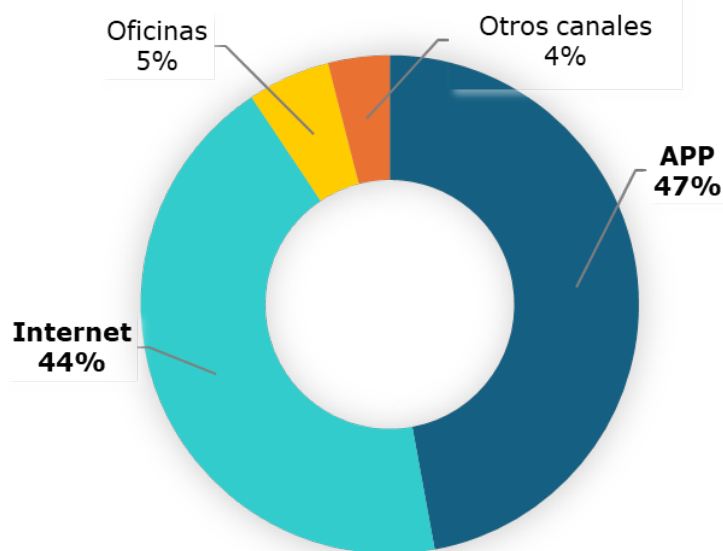




Preferencia por el uso de canales digitales en operaciones no monetarias

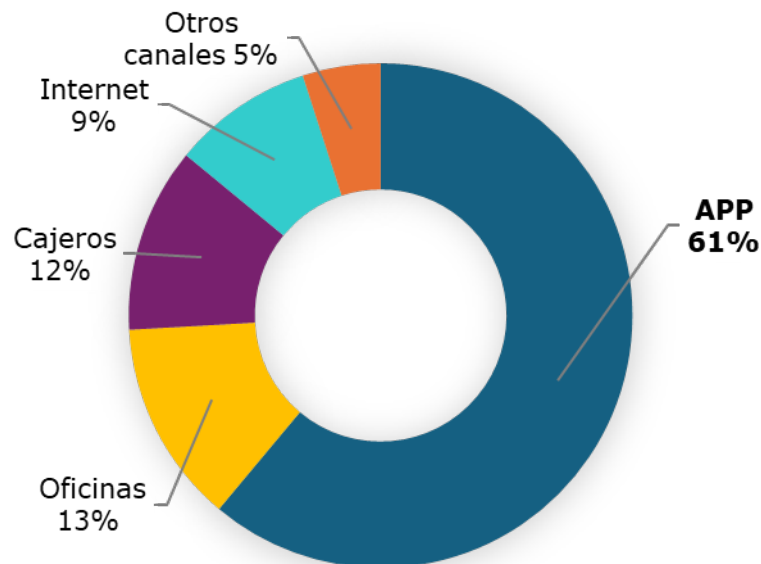
Extractos bancarios

Las App e internet son los canales preferidos por los consumidores financieros para generar sus extractos.



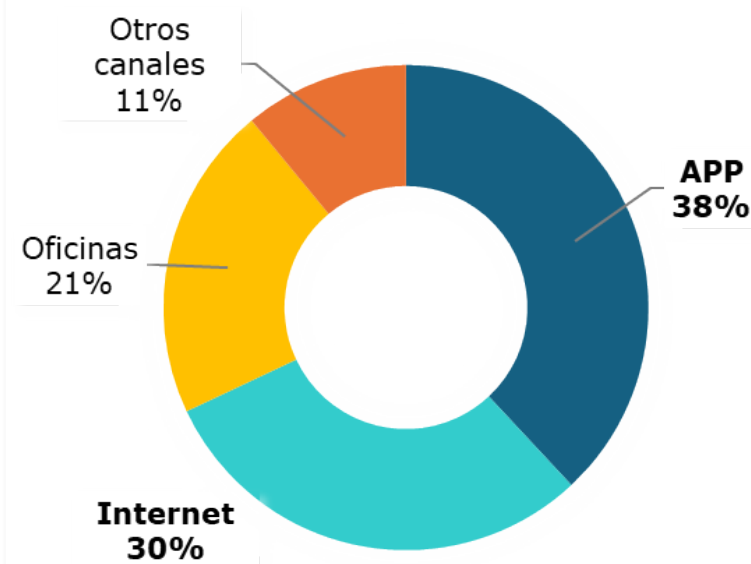
Cambio de contraseña

Para cambiar sus contraseñas los usuarios prefieren las App.



Solicitud certificados

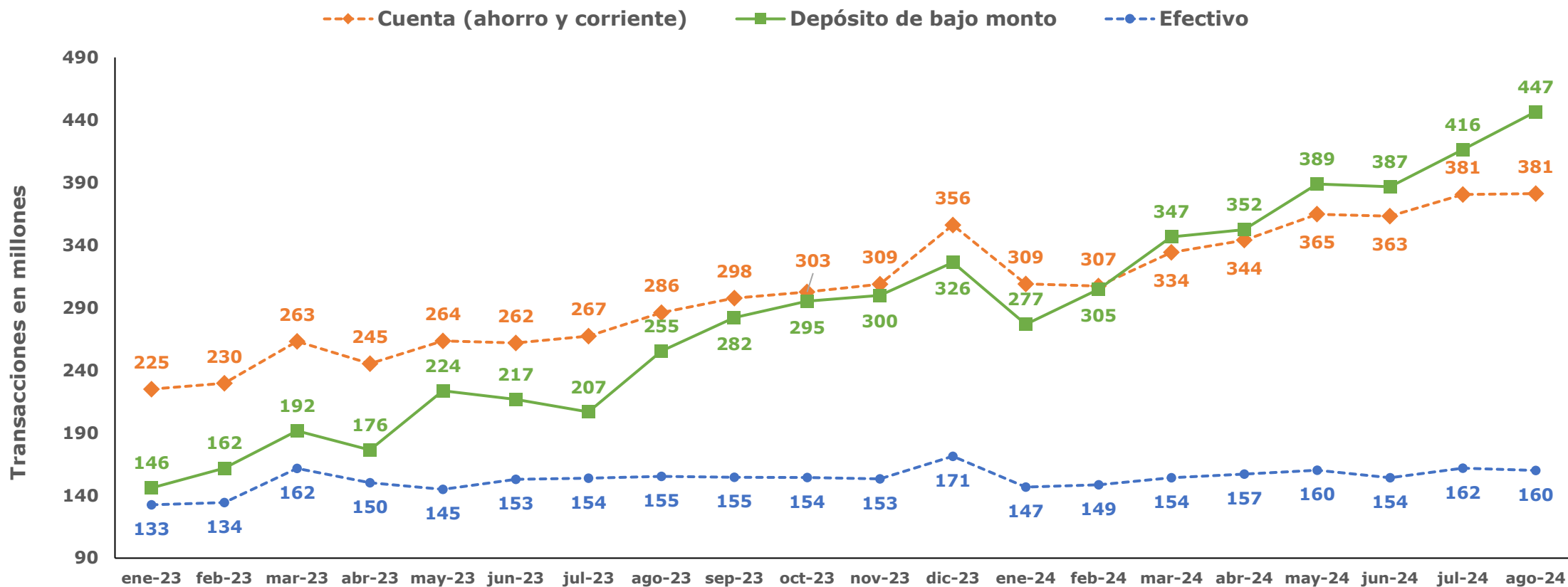
Para solicitar un certificado los consumidores financieros usan principalmente las APP e internet.





El número de transacciones en los depósitos de bajo monto va en aumento

Número de transacciones





Tendencias y retos en la gestión de la ciberseguridad



Principales riesgos emergentes WEF

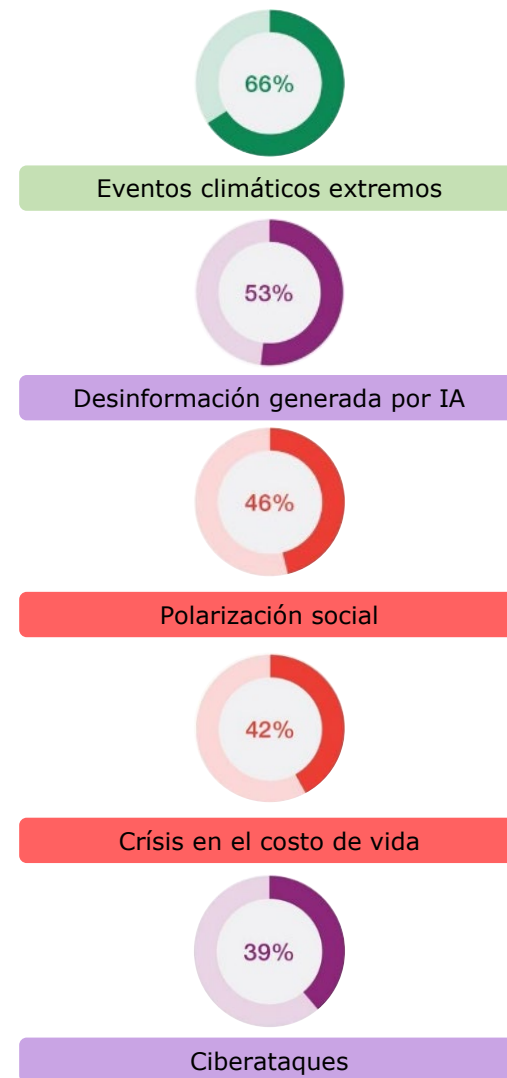
Informe 2024

Riesgos con mayor probabilidad
de presentarse en 2024

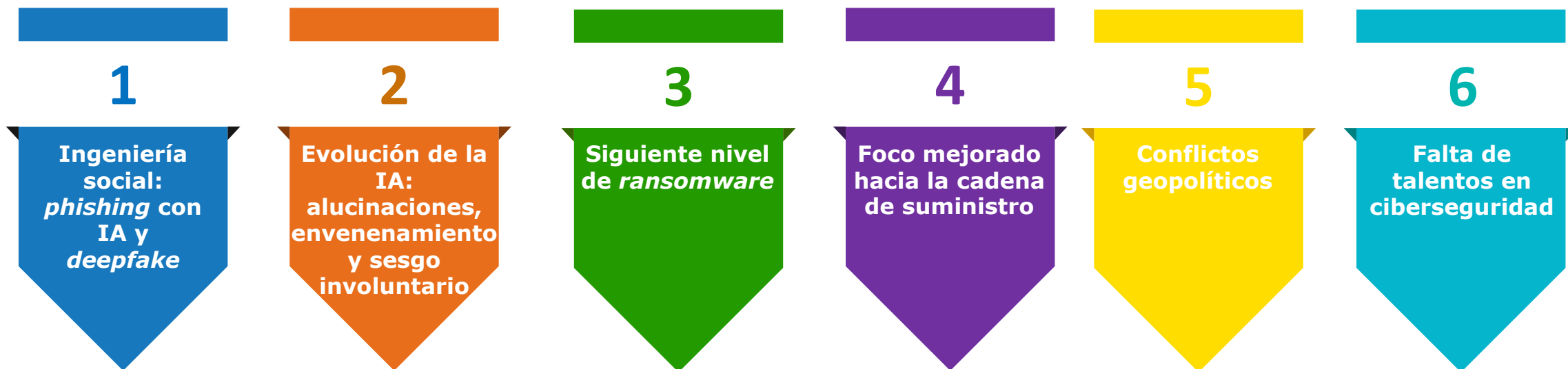
Proyección a 2 años

1°	Desinformación
2°	Eventos climáticos externos
3°	Polarización social
4°	Inseguridad cibernética
5°	Conflicto armado interestatal
6°	Falta de oportunidades económicas
7°	Inflación
8°	Migración involuntaria
9°	Caída económica
10°	Contaminación

- Tecnología
- Ambiental
- Social
- Geopolítico
- Económico



Perspectivas globales de la ciberseguridad en 2024



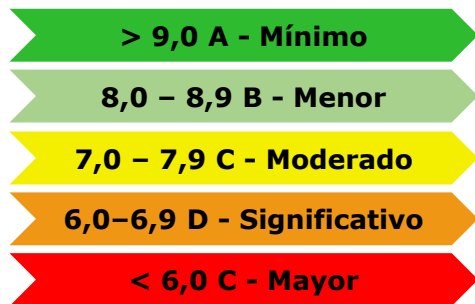


Seguir apostando por una postura de ciberseguridad adecuada para el consumidor financiero

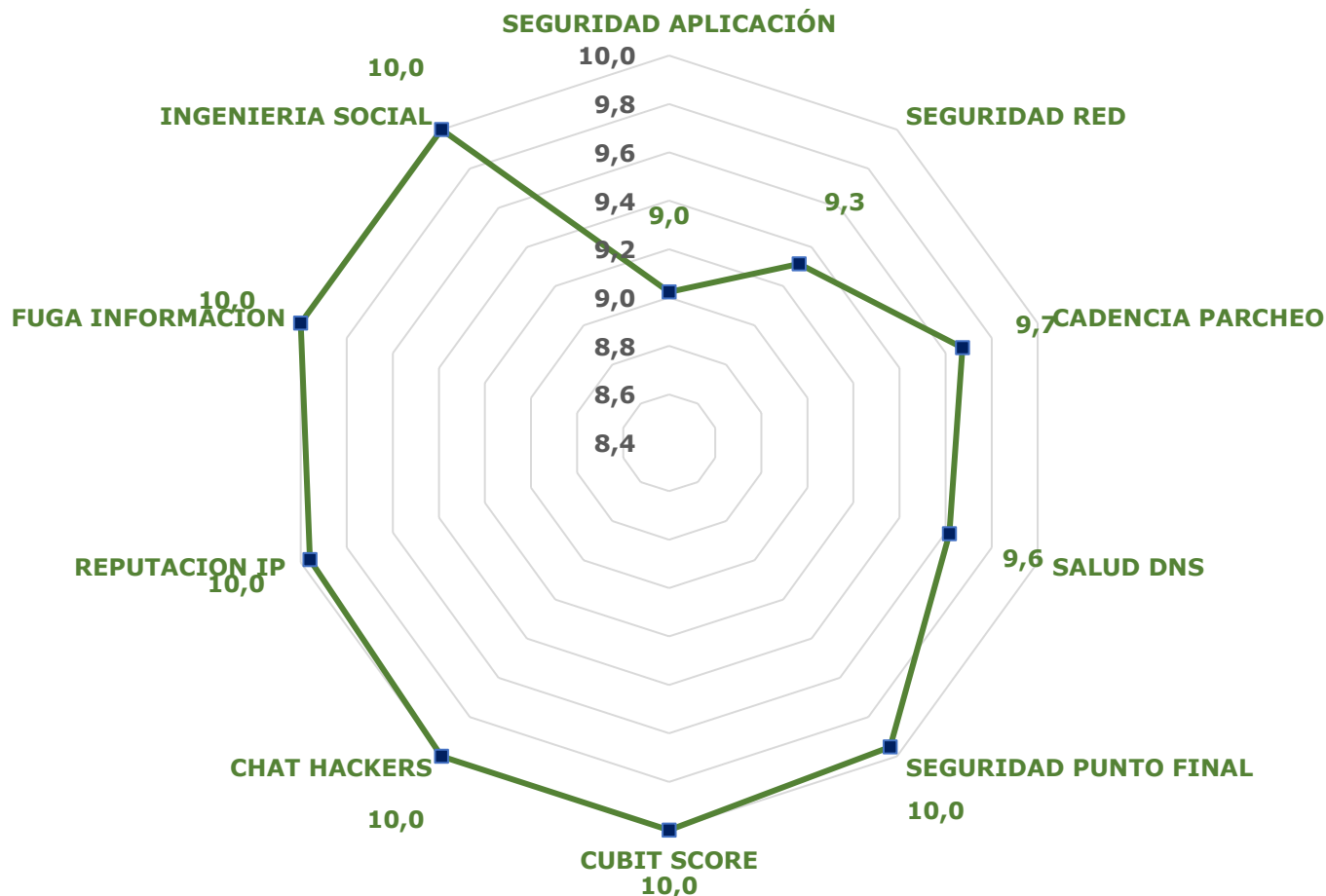
Metodología para la supervisión

Evaluar la postura de ciberseguridad de las entidades financieras mediante la evaluación de señales de inteligencia de amenazas cibernéticas.

- ✓ 11 dominios.
- ✓ Resultado:
 - Análisis y definición de planes de trabajo de la entidad sobre los hallazgos.
 - Seguimientos a planes de acción
- ✓ Promedio simple.
- ✓ Escala de calificación de 0 a 100.
- ✓ Evaluación 2 veces al año, visitas.
- ✓ Evaluación por entidad e industria.



Postura de ciberseguridad EB – septiembre 30/2024

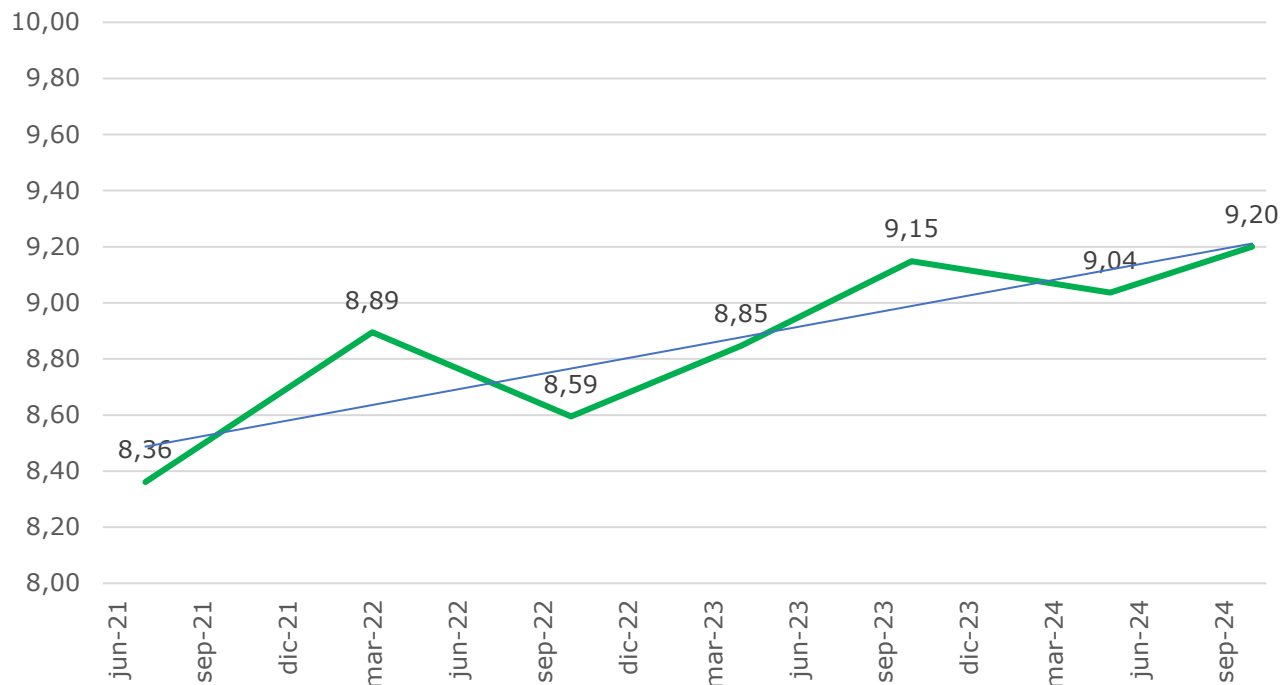


Seguir apostando por una postura de ciberseguridad adecuada para el consumidor financiero

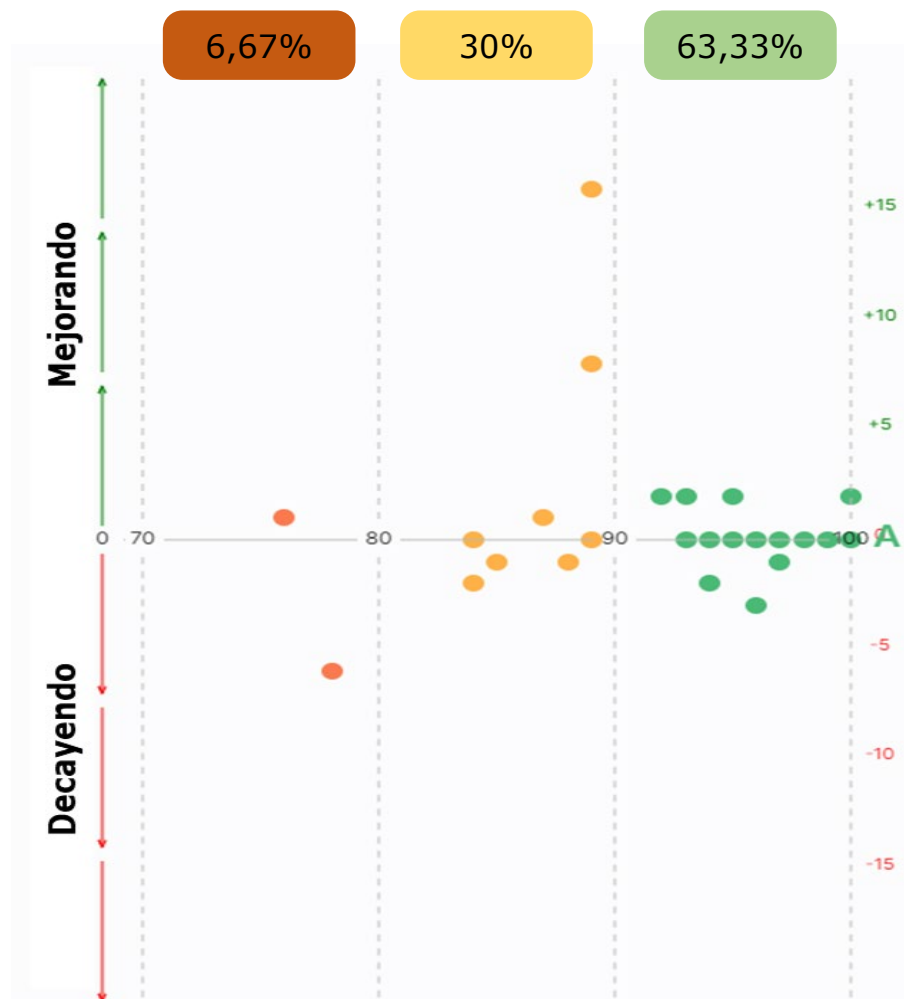
**Postura CS
Establecimientos Bancarios**

A 9,2

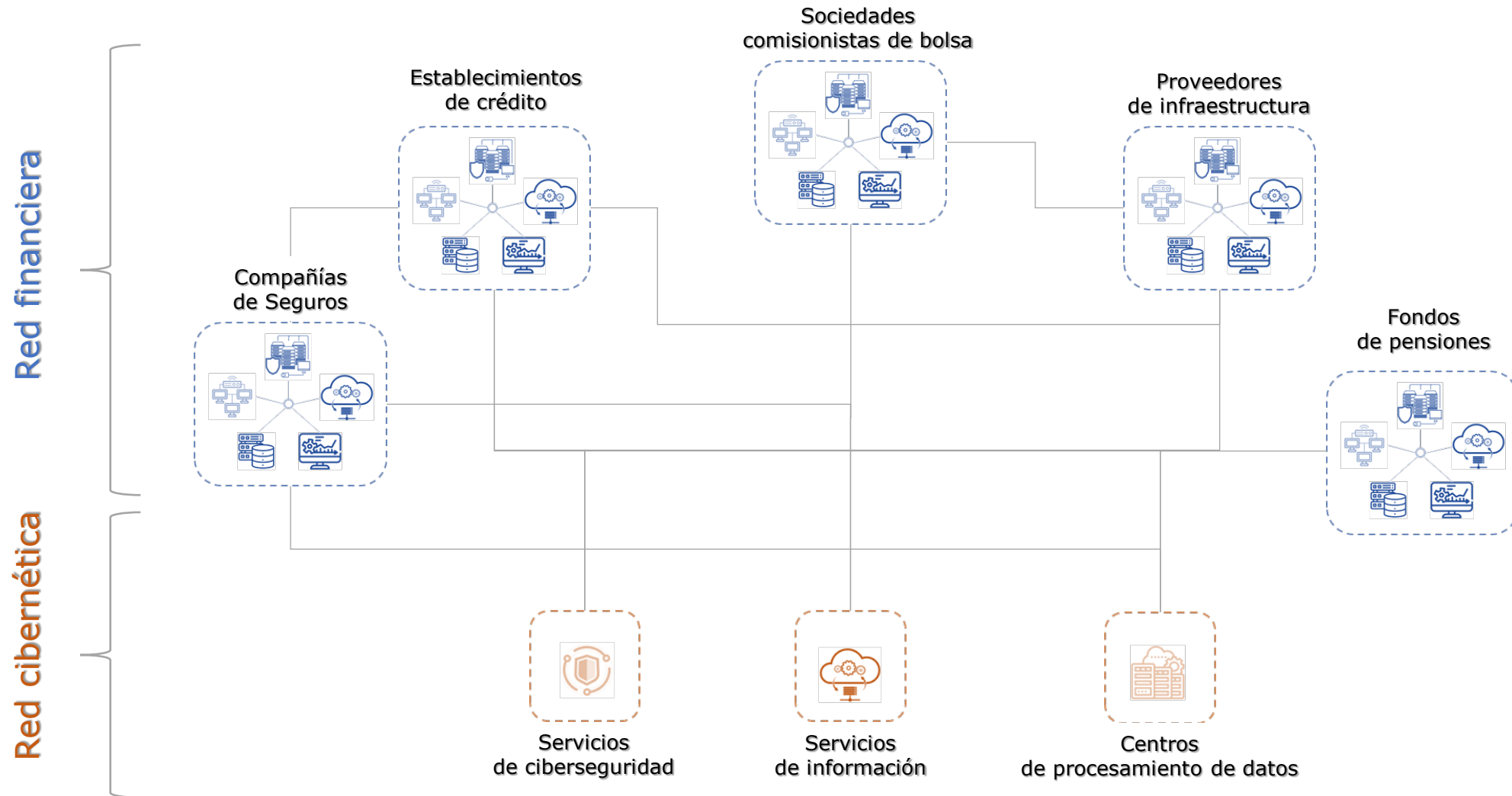
**Variación de la postura
2021 - 2024**



Distribución de la industria

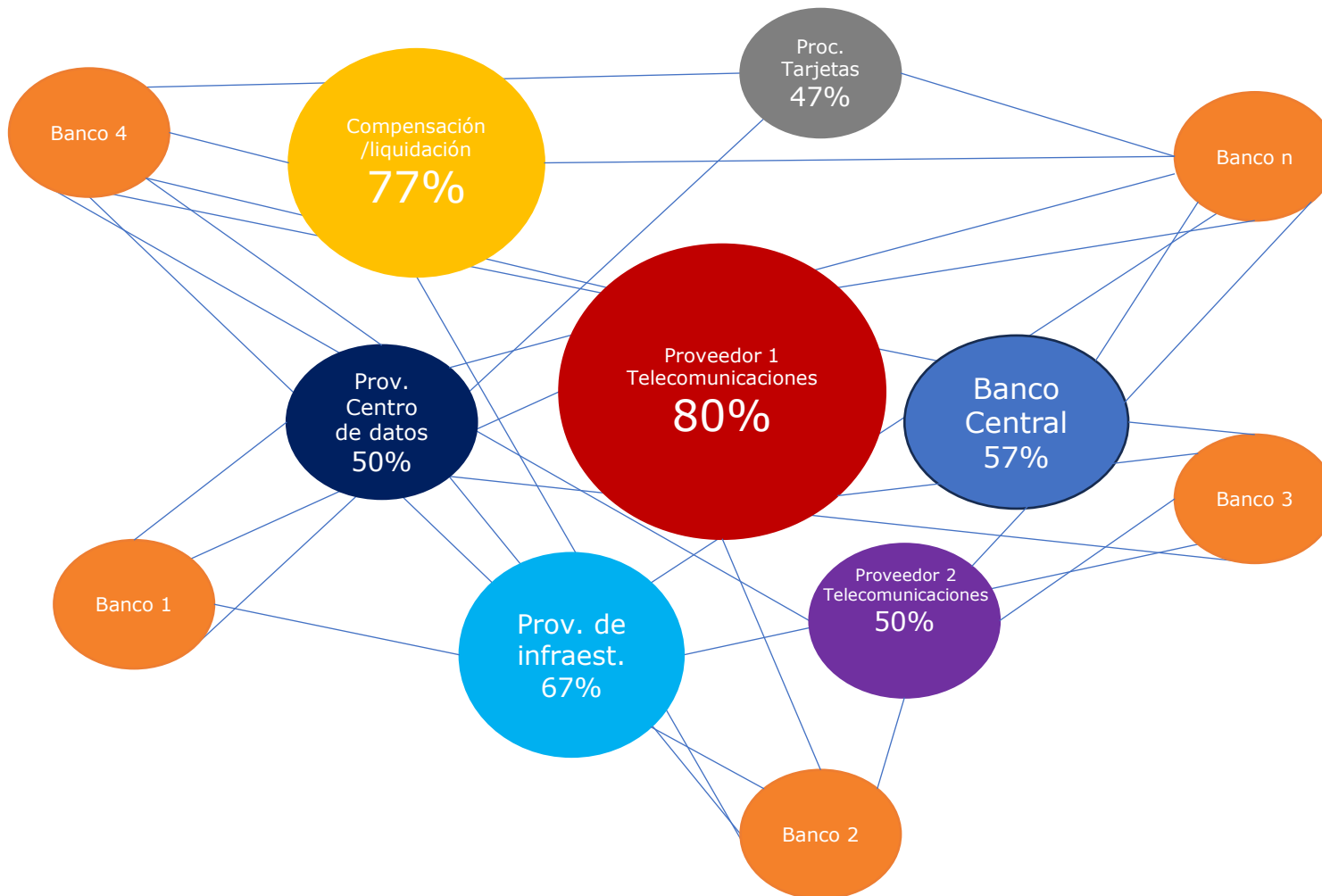


La SFC se encuentra en el camino para identificar el riesgo de concentración de proveedores críticos de tecnología a través del mapa cibernético (*cybermapping*)





Para los establecimientos bancarios se destacan los siguientes servicios que prestan los proveedores críticos de TIC con mayor concentración



Riesgos de las *API* y *web services* y medidas para su mitigación

Exposición de datos sensibles

API abuse
(uso indebido de *API*)

Falta de autenticación y autorización adecuadas

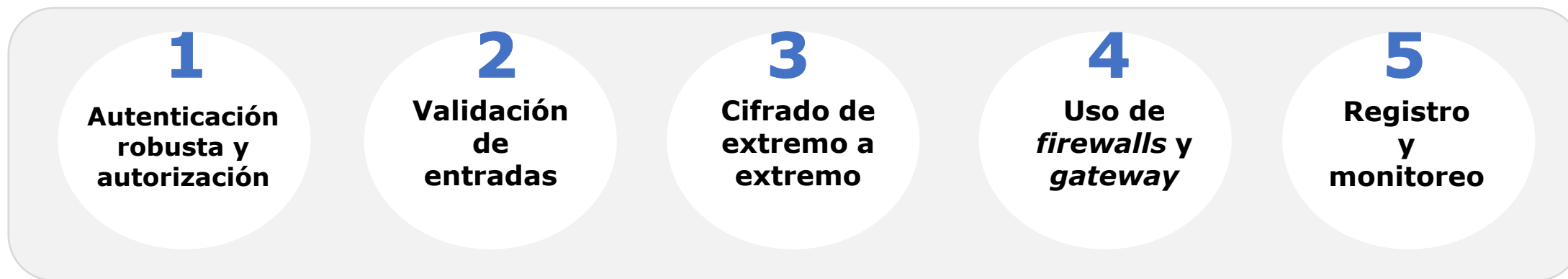
Falta de cifrado en las comunicaciones

Falta de monitoreo y registro de actividades (*logging*)

Ataques de inyección (*injection attacks*)

Errores en la implementación de CORS (*cross-origin resource sharing*)

Medidas para su mitigación



Las entidades deben ir preparando el camino para enfrentar los riesgos derivados de la computación cuántica

Si “x”+“y” se acerca a “z”
¡actúe ahora!

El tiempo para amenaza
de la QC (“z” años)



Tiempo para
migración (“y”
años)

Tiempo en que
la data necesita
estar segura
(“x” años)

Riesgos


- ✓ Procesos de cifrado actuales ineficaces.
- ✓ Tecnología actual obsoleta.

En una encuesta realizada en 2023 a entidades sistémicas de diferentes industrias, se observó que la investigación y los proyectos frente a la computación cuántica se adelantan de manera incipiente


Es necesario implementar el concepto de confianza cero (*zero trust*)

La confianza cero

La confianza cero es un conjunto de principios y estrategias que buscan reducir al mínimo la incertidumbre, al implementar decisiones de acceso estrictas basadas en solicitudes con privilegios mínimos. Esto se aplica a sistemas y servicios de información en un entorno donde la red se asume como comprometida.



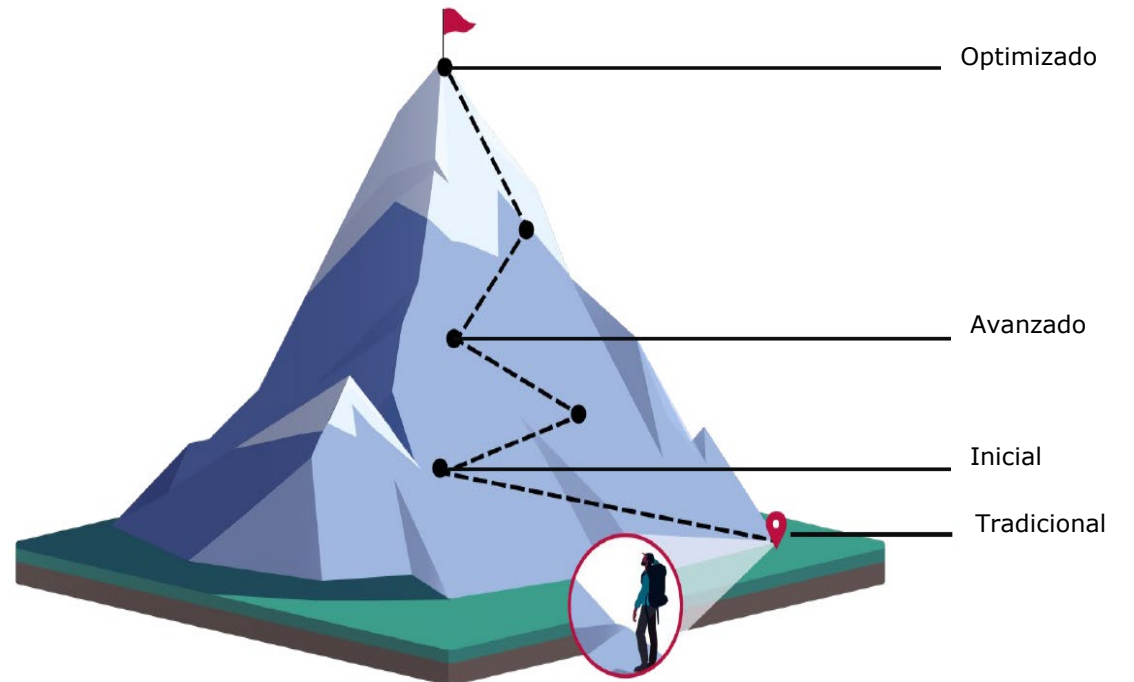
Principales retos

- Sistemas heredados (*legacy*).
 - Infraestructura tecnológica actual.
 - Compromiso de las partes interesadas.
- 

La ruta hacia la confianza cero es un proceso incremental que puede tomar muchos años en la implementación.



Se requiere medir la implementación de confianza cero a través del modelo de madurez



Cálculo de indicadores de SI y CS de los establecimientos bancarios 2023 - 2024



15.989
millones
Ataques
cibernéticos

Es el intento que hace el **ciberdelincuente** para acceder sin autorización a los servicios, recursos o información del sistema, así como para comprometer la seguridad de la información o interrumpir, denegar o degradar los recursos del sistema de información (CE 033/20). **Incremento del 23%** con respecto al primer semestre de 2023.



502.000
millones COP

Invirtieron los establecimientos bancarios en 2024 para gestionar la SI y CS con una **variación del 14%** con respecto a 2023.



9,2 / 10
Postura de
ciberseguridad

Monitoreo y gestión de la CS del ecosistema digital de la entidad con el que se mide el nivel de exposición, se identifican vulnerabilidades y amenazas potenciales, la evaluación al **30 de septiembre de 2023 registró un aumento de 1.10%** respecto de septiembre de 2023 cuando se ubicó en 9,1/10,0. La escala de evaluación va entre 0,0 y 10,0.



La SFC se encuentra revisando la normatividad en temas de ciberseguridad para fortalecerla. Sin embargo, las entidades deben:

- 1** Realizar el intercambio de información en el sector financiero acerca de inteligencia de amenazas.
- 2** Realizar el reporte de incidentes cibernéticos al ColcERT (o quien haga sus veces) a través del CSIRT sectorial.
- 3** Contratar o implementar el servicio de un *SOC (Security Operation Center)*.
- 4** Realizar pruebas individuales y sectoriales de simulación de incidentes cibernéticos.



Superintendencia
Financiera de Colombia

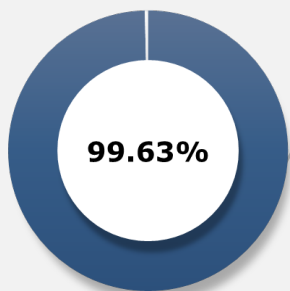


Disponibilidad de canales digitales

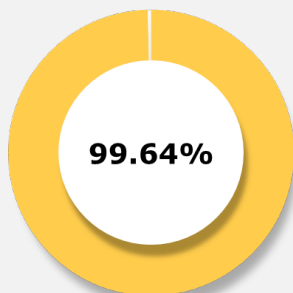


Disponibilidad de los canales banca móvil e internet. Establecimientos bancarios

Primer semestre de 2023

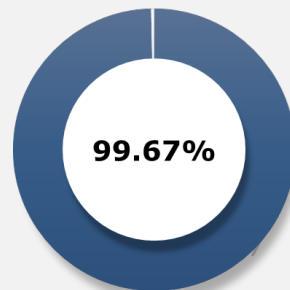


Indisponibilidad de **2 horas, 40 minutos y 50 segundos** en el mes

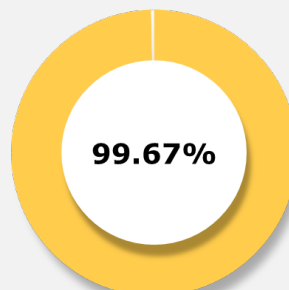


Indisponibilidad de **2 horas, 36 minutos y 29 segundos** en el mes

Primer semestre de 2024



Indisponibilidad de **2 horas, 23 minutos y 27 segundos** en el mes



Indisponibilidad de **2 horas, 23 minutos y 27 segundos** en el mes

Para tener en cuenta:

Cada entidad define la metodología y las variables internas y externas para medir la disponibilidad de los canales digitales. (aplicación, infraestructura, métricas, periodicidad, tipo de canal (app, monedero, internet), período de tiempo de las ventanas de mantenimiento, entre otros).

El Ministerio de Hacienda y Crédito Público propone en el proyecto de decreto, en relación con los ajustes normativos al ecosistema de pagos de bajo valor, que las entidades emisoras aseguren la disponibilidad de los canales digitales en el **99.95%**, es decir, una indisponibilidad permitida **mensual** de **21 minutos y 44 segundos**.

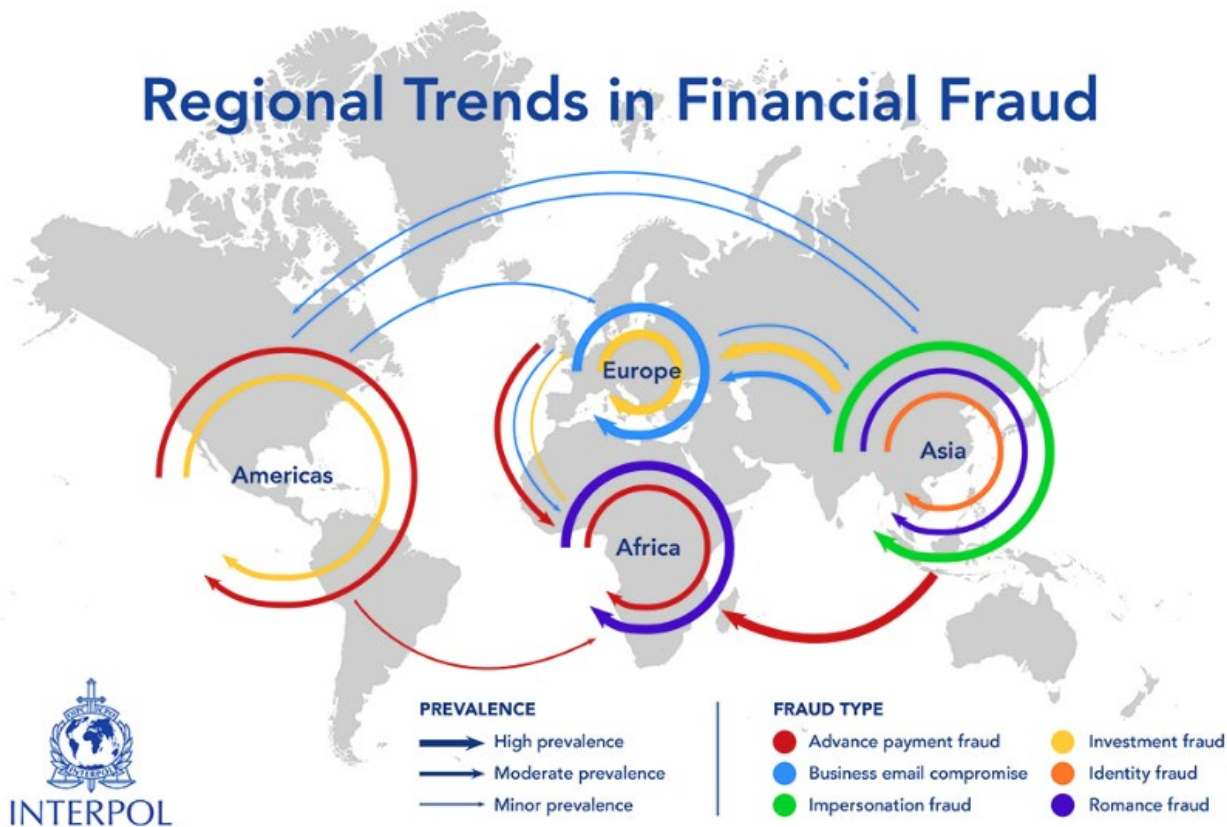


Gestión del fraude



Tendencias regionales del fraude financiero

Regional Trends in Financial Fraud



- Las tendencias mundiales más frecuentes son las estafas de inversión, las de pago por adelantado, las sentimentales por Internet y las estafas a empresas por **e-mail mediante suplantación de identidad**.
- Con el uso de la inteligencia artificial, ahora los grandes modelos lingüísticos y las criptomonedas, combinados con modelos de negocio (como el *phishing* y el *ransomware* como servicio), se pueden llevar a cabo unas estafas más sofisticadas y profesionales sin necesidad de tener habilidades técnicas avanzadas y a un coste relativamente bajo.

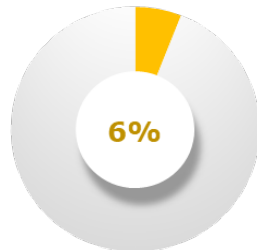
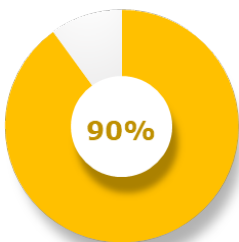


Crecimiento de la variación del fraude digital sospechoso comparado con las transacciones digitales a nivel global

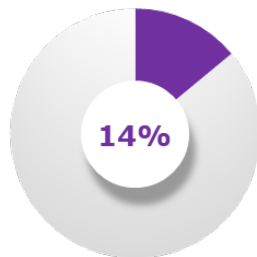
2019-2023

2022-2023

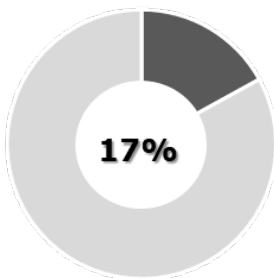
Crecimiento de transacciones digitales



Crecimiento del fraude digital sospechoso



El crecimiento del fraude digital sospechoso supera el crecimiento de las transacciones




Tipos de principales fraudes y su crecimiento



	% de fraude digital 2023	Variación 2022 - 2023	Variación 2019 - 2023
Apropiación de cuentas	7%	18%	113%
Tarjeta de crédito	7%	14%	102%
Fraude de identidad real	7%	18%	113%
ACH / tarjeta débito	6%	14%	153%
Identidad sintética	6%	21%	184%



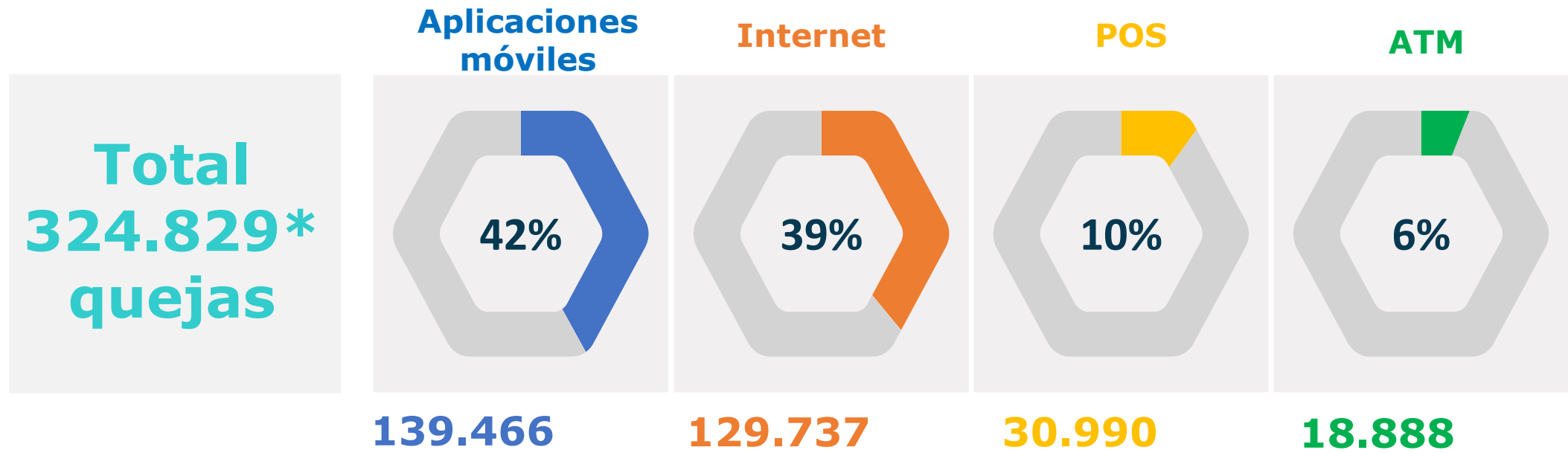
Modalidades de fraude



 En el primer semestre de 2024 los bancos recibieron más de **242.000** quejas por fraude. Reconocieron alrededor de **\$290 mil millones COP.**


 La **ingeniería social (27%)** y la **suplantación de identidad (18%)** fueron las modalidades de fraude más reportadas.

En los canales no presenciales se concentró la mayoría de las quejas por fraude en el primer semestre de 2024



El **monto reclamado** por fraude corresponde al **0,01023%** del valor total que se tranzó durante el primer semestre de 2024.

Por cada **16.420 operaciones** monetarias se presentó **una queja** por fraude.

* Bancos (billeteras), Compañías de financiamiento, cooperativas y SEDPE.
Fuente: información remitida por las entidades y consolidada por la SFC.



Las entidades tendrán que enfrentar retos cada vez mayores

7

Lucha colaborativa contra el fraude

6

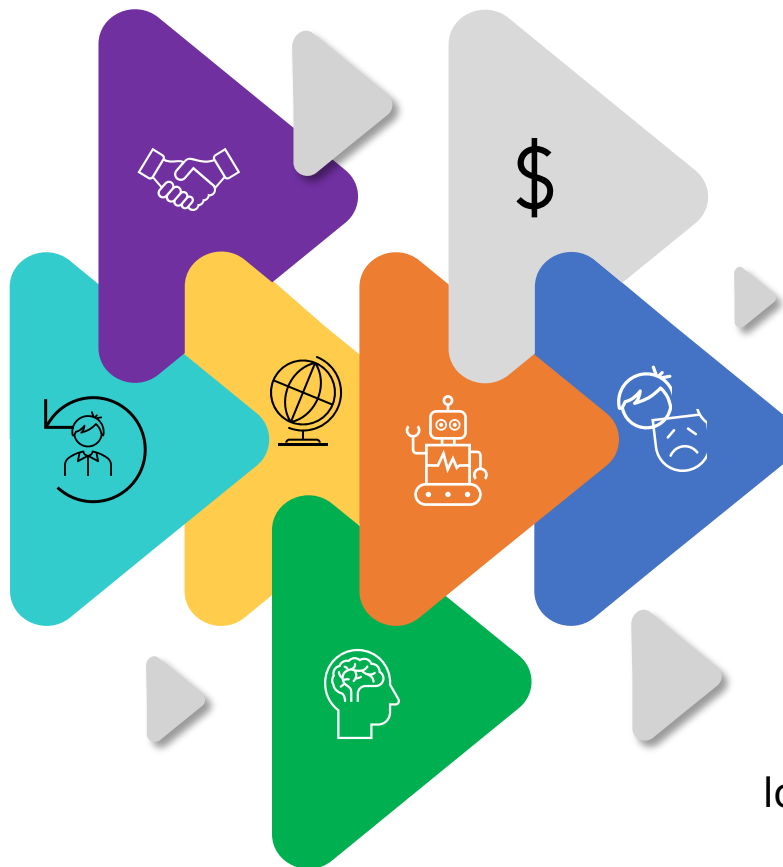
Adoptar una vista de 360° del cliente será imperativo para mejorar la evaluación del riesgo.

5

El fraude cada vez más coordinado a través de las fronteras internacionales.

4

La mayor utilización de inteligencia de comportamiento para enfrentar el fraude complejo.



1

La presión regulatoria adicional, que probablemente impactará los costos de la gestión del riesgo.

2

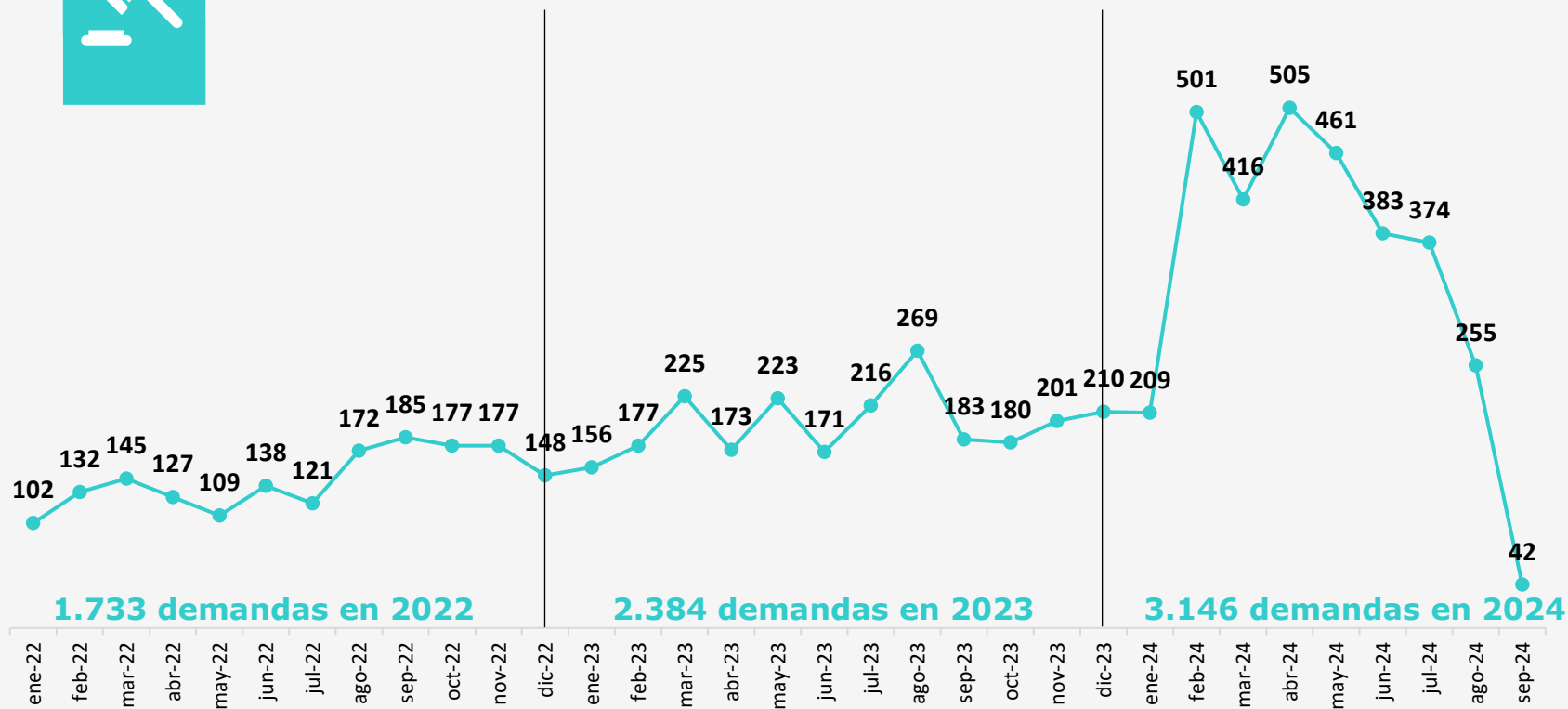
El crecimiento explosivo del uso de identidades sintéticas.

3

El incremento en el uso de inteligencia artificial, por parte de los delincuentes, exigirá nuevas tácticas de mitigación del riesgo.



Las demandas por fraude continúan en aumento



7.263

Demandas admitidas

43%

Del total de las tramitadas por la Delegatura de Funciones Jurisdiccionales

96.5%

De mínima cuantía

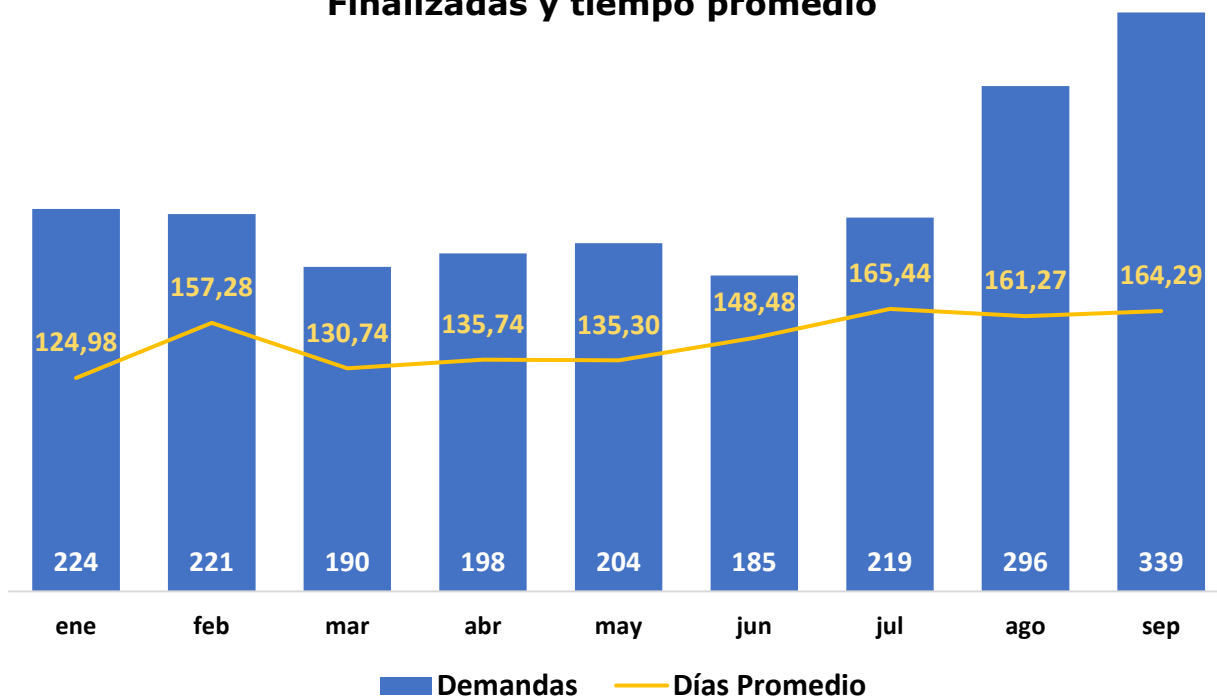
37.6%

Incremento 2022-2023



El sentido de los fallos muestra la necesidad de consolidar la confianza del consumidor

Finalizadas y tiempo promedio



Tendencia al alza de litigiosidad

148,94
días en promedio

Tipo de decisión

85% a favor

Participación del total

Tipo de terminación

Sentencia

36,42%

Conciliación

33,48%

Desistimiento

18,59%

Fallo

11,22%

Transacción

0,29%

La conciliación no puede ser la **salida rápida** para el consumidor.



Educación al consumidor financiero

Estrategia de educación financiera SFC



La estrategia tiene como objetivo crear conocimientos y competencias financieras que permitan a los ciudadanos transformar positivamente su relacionamiento con el sistema financiero y la administración de su dinero.



Curso virtual de educación financiera

Contenidos didácticos, interactivos, ejemplos y otras actividades de aprendizaje autónomo sobre temas relacionados con el sistema financiero, por ejemplo, el mercado de valores, negocios fiduciarios, pensiones y seguros, además de ofrecer herramientas de utilidad para no dejarse engañar por diversas modalidades de **fraude financiero**.

Educación financiera para todos



Espacios de educación para niños, jóvenes y ciudadanía en general en los que, a través de actividades didácticas, se comparten conocimientos y se fortalecen competencias financieras con la intención de transformar positivamente el relacionamiento de las personas con el sistema financiero y la administración de su dinero.

Piezas publicitarias enfocadas en la prevención del fraude

Instagram



Superintendencia Financiera de Colombia

Las entidades vigiladas
NO te contactan por videollamada o chat para pedir información personal.



Denuncia cualquier mensaje sospechoso ante el **CAI virtual** www.caivirtual.policia.gov.co o comunícate con tu entidad financiera.

X (@SFCsupervisor)



Superfinanciera @SFCsupervisor

#MisTransaccionesSeguras | ¡Cuidado con las estafas por chat!

Los ciberdelincuentes utilizan la función de compartir pantalla para vaciar cuentas bancarias. Mantente alerta y protege tu información.



6:25 p. m. · 10 jun. 2024 · 1.171 Reproducciones

Ver las interacciones de post

Facebook



Superintendencia Financiera de Colombia

Publicado por Brandwatch

· 19 de agosto a las 8:33 a.m. ·

#MisTransaccionesSeguras | ¡Atención usuarios!

La estafa de compartir pantalla pone en riesgo tus datos financieros. Aprende a protegerte.



5

3 comentarios 2 veces compartido

Me gusta Comentar Enviar Compartir

https://www.instagram.com/p/C--Ud10Kwb8/?utm_source=ig_web_copy_link&igsh=MzRIODBiNWFIZA==

<https://x.com/SFCsupervisor/status/1800308258445410486>

<https://www.facebook.com/photo?fbid=917224410436849&set=pcb.917224450436845>



Proyectos estratégicos



La digitalización también hace parte de los proyectos estratégicos de la SFC

Supervisión digital

- Transformar el esquema actual de supervisión.
- Reducir costos de reportería.
- **Contar con datos en línea.**
- Principio de interoperabilidad.
- Desarrollar analítica predictiva y prescriptiva.
- Desarrollar supervisión a través de colegios bilaterales con otras autoridades.

Finanzas Abiertas

- **Reglas para la adopción de estándares tecnológicos y seguridad.**
- Simetría de información.
- Promover la competencia en los mercados.
- Productos financieros a la medida.
- Empoderar al consumidor financiero.

Modernización de la SFC

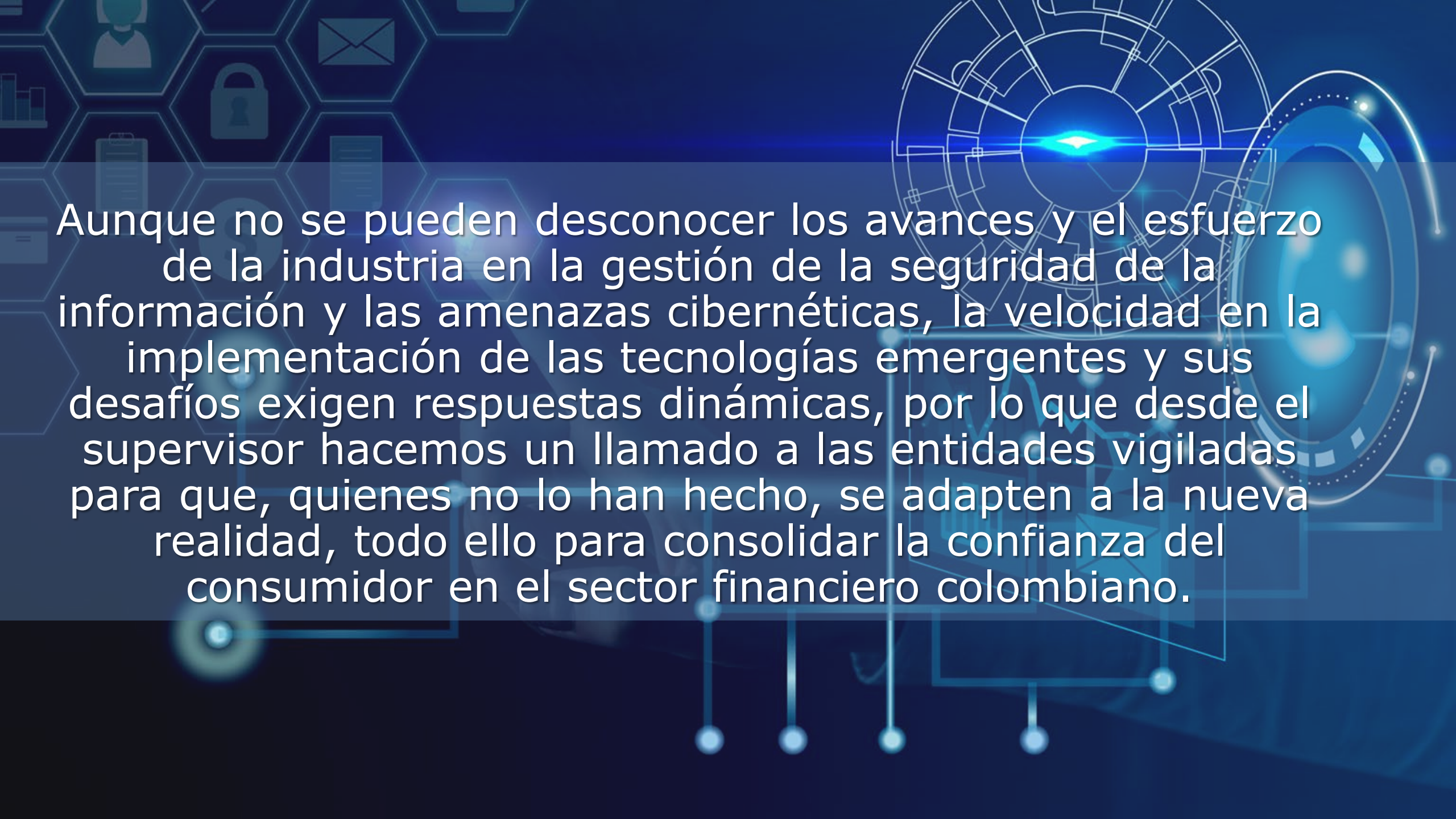
- Reducción costos funciones de autorización y supervisión
- Autorización y tramites más ágiles.
- Mejora de la estrategia, estructuras y tecnología.
- Supervisión integral por cada industria o mercado.
- Mejora gobernanza y transparencia.
- Visión holística en los supervisores **basada en análisis de datos.**

Actualización matriz de riesgos

- Metodología de **supervisión digital basada en datos.**
- Modelos econométricos.
- Integrar los Riesgos ASCG.
- Métricas para identificar riesgos inherentes.
- Modelo del Indicador de Riesgos Compuesto (IRC).

Optimización normativa

- **Apoyo de nuevas tecnologías para el proceso.**
- Ajustar duplicidad y obsolescencia normativa.
- Asegurar estabilidad y confianza de los mercados.
- Ajustar la regulación para facilitar comprensión y cumplimiento.
- Ajustar cargas o limitaciones para los agentes de mercado.




Aunque no se pueden desconocer los avances y el esfuerzo de la industria en la gestión de la seguridad de la información y las amenazas cibernéticas, la velocidad en la implementación de las tecnologías emergentes y sus desafíos exigen respuestas dinámicas, por lo que desde el supervisor hacemos un llamado a las entidades vigiladas para que, quienes no lo han hecho, se adapten a la nueva realidad, todo ello para consolidar la confianza del consumidor en el sector financiero colombiano.


Descárguela
en su dispositivo


Gracias


 @SFCsupervisor

 Superintendencia
Financiera de Colombia

 superfinanciera

 Superintendencia
Financiera de Colombia

 SuperfinancieraSFC

 superfinanciera



www.superfinanciera.gov.co



super@superfinanciera.gov.co