Barranquilla, octubre 27 de 2022

# **Asegurando la resiliencia operativa** ante amenazas emergentes


Jorge Castaño Gutiérrez

Superintendente Financiero de Colombia


Congreso de prevención del fraude y seguridad - Asobancaria

# El análisis prospectivo de riesgos **devela un panorama desafiante para** asegurar la confidencialidad y disponibilidad de los datos y de los sistemas

## Incremento en el uso de los canales digitales

El uso masivo de los canales digitales aumentó el apetito de los defraudadores.

Del segundo semestre de 2018 al primero de 2022 los crecimientos fueron de:

* **207%** en el canal internet
* **991%** en banca móvil

## Nuevas tipologías de ataques

- Aumento de los fraudes por **ingeniería social** (phishing, vishing, smishing, etc).
- Aparición de **nuevas modalidades** como el uso de malware, ataques de enumeración o BIN.

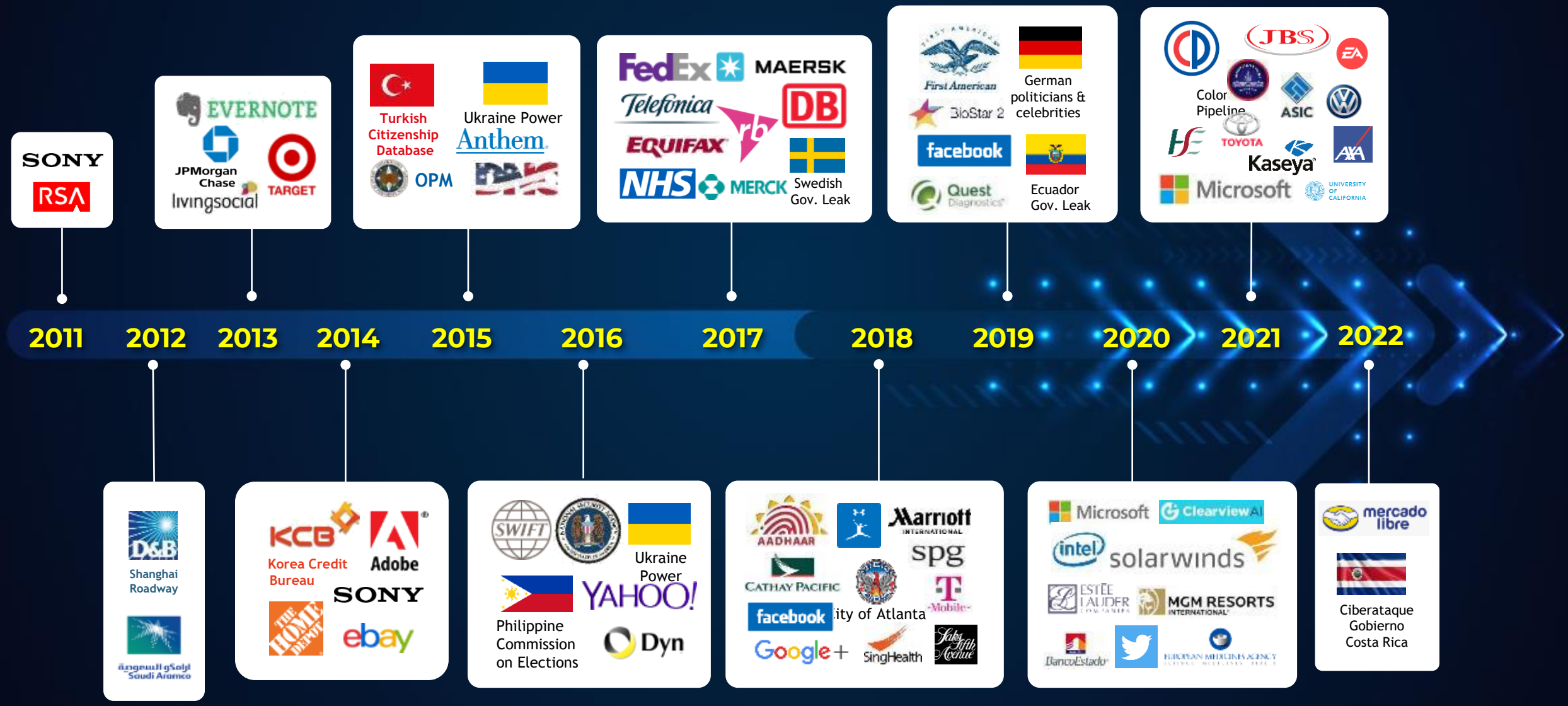
## Fallas en la concientización del usuario

El uso masivo de los canales digitales puso en evidencia las debilidades de los consumidores financieros en el cuidado de su información.

## Debilidades de las entidades

Como por ejemplo, en algunos procesos de KYC y de administración y gestión de datos de tarjetas débito y crédito.

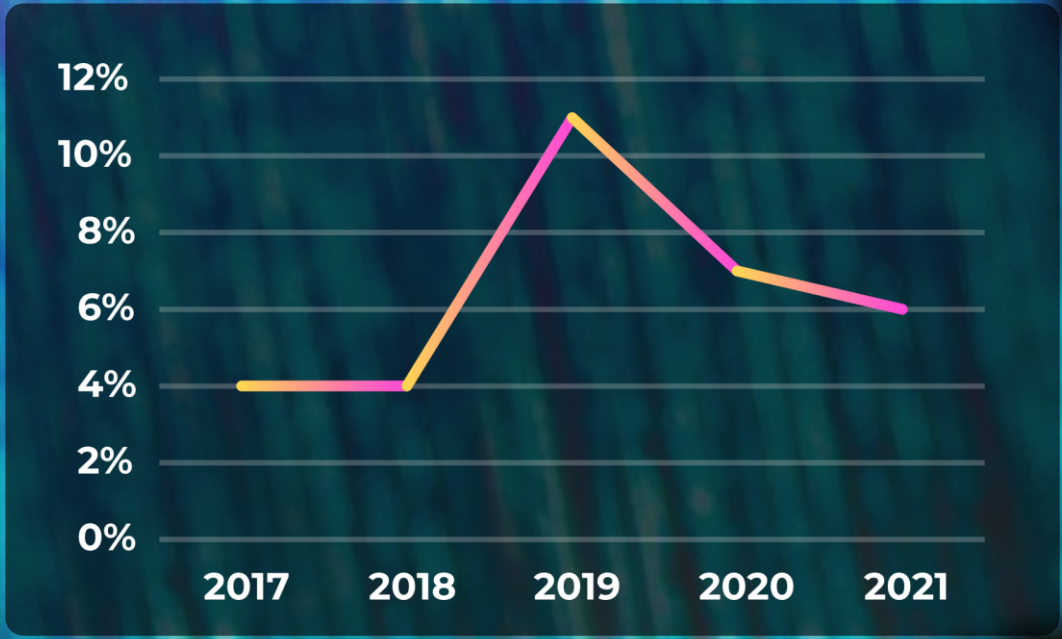
# **Las amenazas aumentan** no solo en cantidad sino en complejidad, afectando a diversos tipos de industrias



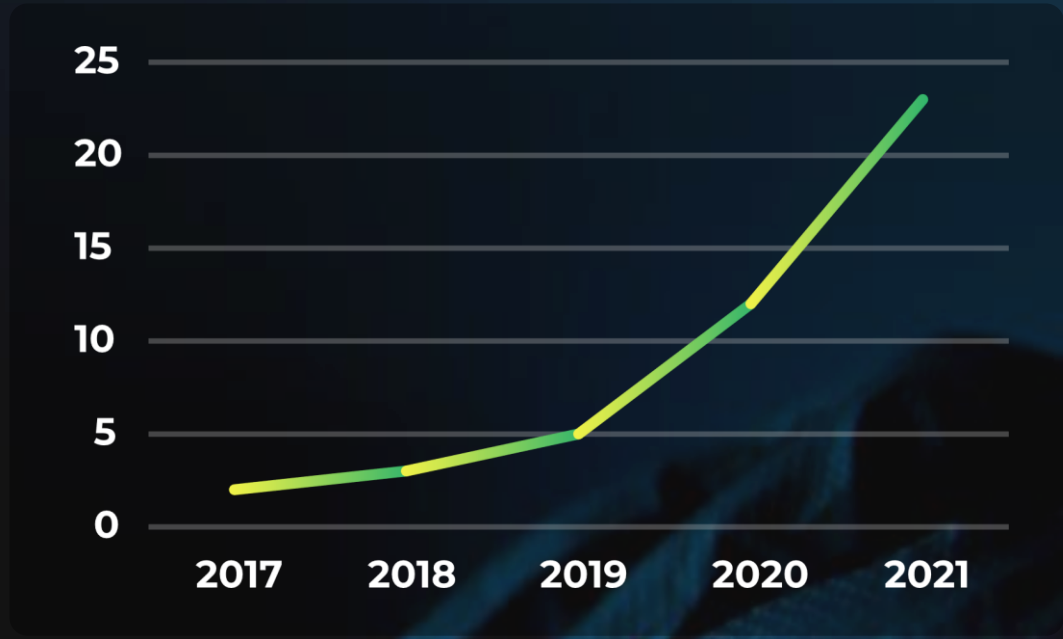

Fuente: Reportes de prensa

# Los factores determinantes en muchos incidentes están **sobrediagnosticados:**

## ¿Cómo nos preparamos?, ¿cómo los enfrentamos?




El **13%** de los incidentes se debe a **mala configuración** de ambientes *on premise* y en especial en la nube.




En América Latina una de cada **23 empresas** experimentó incidentes de **ransomware** en 2021.

**82%** de los incidentes de seguridad involucró el factor humano (uso de credenciales robadas, phishing, indebida asignación de privilegios, etc). Por esta razón es importante fortalecer la concientización de los consumidores financieros en el manejo de sus datos y la revisión periódica de los procesos en los que intervienen los funcionarios, con el fin de optimizarlos.

Fuente: Data Breach Investigations Report 2022 - Verizon

# De igual forma, la acción articulada ha permitido identificar diferentes modalidades de fraude, que han representado **pérdidas económicas y reputacionales**

**Ingeniería Social**

Phishing

Vishing

Smishing

Ataque CEO

**Suplantación de Identidad**

Uso no consentido de información

SIM Swapping

Fraude Amigo

**Datos de Tarjetas**

Skimming

Ataque BIN

**Ciberseguridad**

Malware

Keylogger

Enumeración

Pharming

En los primeros **siete meses de 2022** los bancos recibieron más de **221.000 quejas** por fraude, reconociendo **$243 mil millones,** de los cuales, **$72 mil millones** fueron asumidos por incidentes cibernéticos que sufrieron **sus clientes.**

Fuente: Datos SFC – Enero a Julio 2022

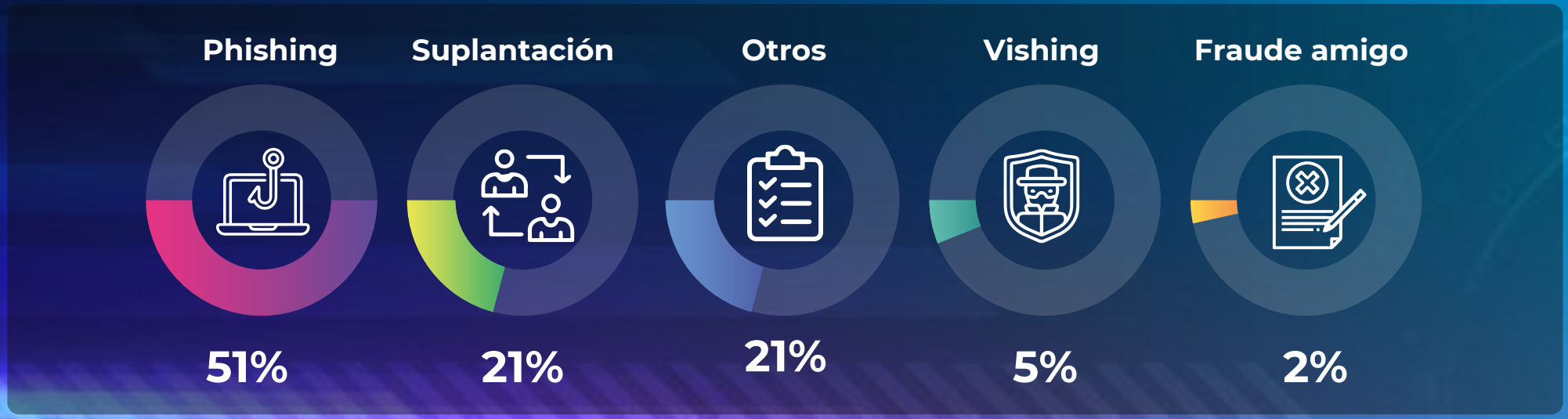
**Necesitamos proteger la confianza:**
cerca del 30% de los consumidores colombianos de diferentes sectores dijo **haber sido víctima de fraude digital**

## Tendencias de fraude
(Noviembre 2021 - marzo de 2022)


**10.391**
consumidores encuestados

Fuente: Tendencias de Fraude- Análisis Trimestral – Transunion.

# La mejor **experiencia del cliente** no solo radica en la prestación del servicio sino en el **cuidado y protección de su información**





Fuente: Datos SFC

# No podemos retroceder en materia de digitalización por el fenómeno de fraude. Las demandas por este concepto **continúan en aumento**


**2.921**
**Demandas admitidas**

**33%** Del total de las tramitadas por la Delegatura de Funciones Jurisdiccionales

**95,4%** De mínima cuantía

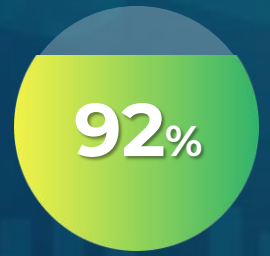
**+51,9%** Incremento 2020 vs. 2021

Fuente: SFC

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

**Tendencia al alza de litigiosidad**

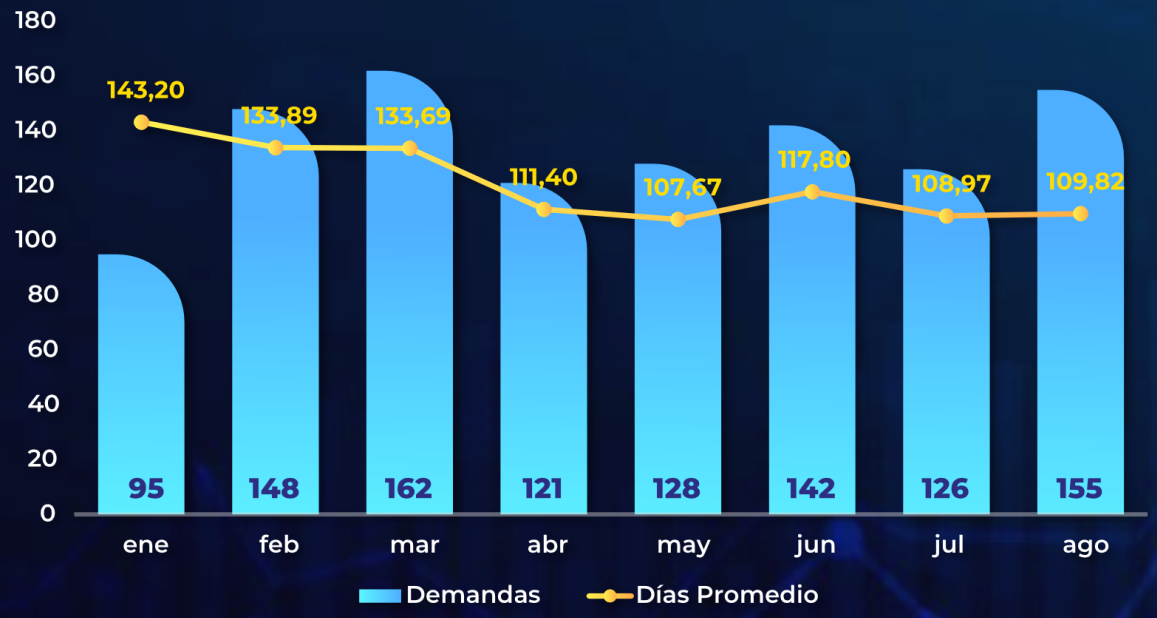
**120,54**
días en promedio




**Tipo de decisión:**
**A favor**

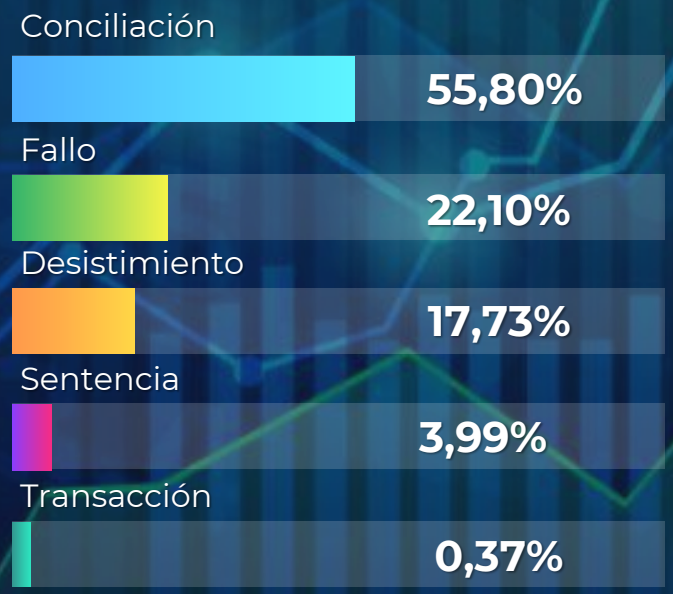
Participación del total

## Finalizadas y tiempo promedio




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

## Tipo de terminación

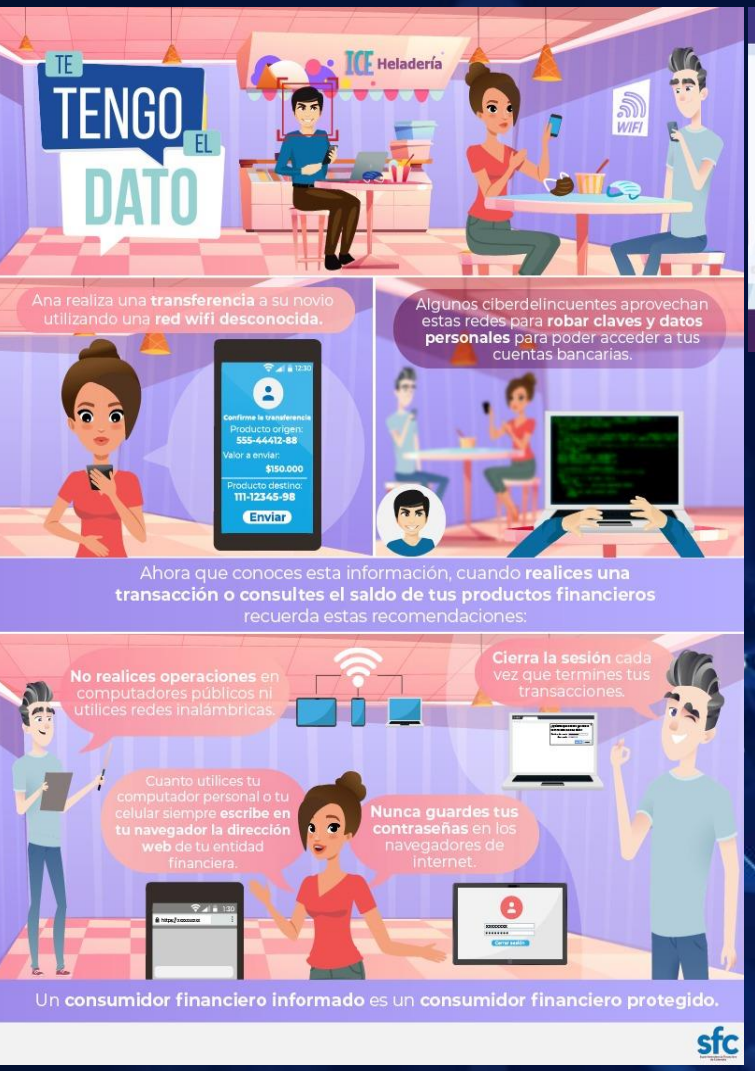



**Pretensiones**
**$11.8 mil millones**

**Decisión**
**$5.7 mil millones**

Fuente: Delegatura para Funciones Jurisdiccionales SFC / Enero – Septiembre 2022

# No podemos abandonar el propósito de concientizar a los consumidores en el **uso y protección de su información**










La SFC ha requerido a las entidades para que refuercen sus campañas de sensibilización, con el fin de que los clientes hagan un mejor uso de la información.

# Sumado a lo anterior, el trabajo y las inversiones realizadas en materia de ciberseguridad **han logrado contener los ataques**

**$424 mil millones**
Presupuesto para seguridad de la información y ciberseguridad en **2022.**

**+1.327 millones**
Número de ataques que dieron origen a **dos** incidentes cibernéticos.

**$72 mil millones**
Costo de los incidentes cibernéticos sufridos por los **clientes** asumidos por las entidades.

A **septiembre** de **2022**

**4.42 días**
Tiempo promedio de gestión de los incidentes cibernéticos.

**7%**
Promedio de obsolescencia tecnológica.

# En este contexto, **hemos priorizado nuestra estrategia de supervisión** preventiva sobre tres pilares

## Un ambiente seguro que consolida la trasformación digital y la inclusión

**1** **Seguridad de la información**

**2** **Disponibilidad y planeación de la capacidad**

**3** **Calidad del software**

### Acciones de supervisión

**1. Fortalecer** el KYC .

**2. A**plicación de mecanismos fuertes de autenticación.

**3. Guía** de gestión de incidentes en terceros

**4**. **Incentivar** la modernización de los controles de ciberseguridad.

**5. Incrementar las campañas** sobre protección de datos a consumidores financieros .

**1.** Contar con **procesos de monitoreo.**

**2. Contar con r**ecursos para procesar tres veces el pico histórico de operaciones.

**3.** Generar **pruebas de capacidad** operativa de sus canales.

**4.** Los canales digitales : **disponibilidad mínima** de 99:9% (máx. 8 horas off al año. Hoy es de 98.5% - 131 horas/año).

**1. Adopción de mejores técnicas de desarrollo** (modulares, flexibles y modernas).

**2. Incentivar** el uso de lenguajes de programación modernos.

**3. Capacitar** a los programadores en técnicas de desarrollo seguro.

**4. Fomentar** la realización de pruebas de calidad automáticas.

# La importancia de la resiliencia operacional se refleja en la intensidad de los procesos de **supervisión adelantados**

## Temas objeto de supervisión

- Madurez de la tecnología, continuidad del negocio y gestión de la ciberseguridad.
- Seguridad en operaciones digitales.
- Capacidad de las plataformas.
- Obsolescencia tecnológica.
- Calidad de los sistemas de información.
- Tercerización.
- Incidentes cibernéticos y fraude.
- Gestión de riesgos.

| Modalidad | 2021 | 2022 | 2023 |
|---|---|---|---|
| Entidades visitadas | 28 | 23 | 24 |
| Entidades con extra situ - transversales | 145 | 119 | 110 |

# Una gestión de riesgo robusta **nos permite enfrentar amenazas incipientes** derivadas de: la sofisticación del delito y de los nuevos modelos de negocio, actores, tecnologías y necesidades

## Ciberseguridad

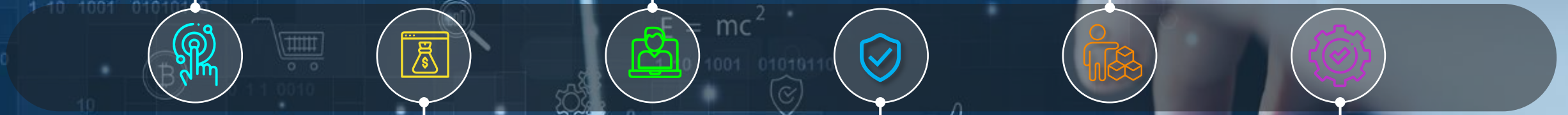
- Ransomware
- Phishing
- Ataques a la cadena de suministro
- Talento humano

## Open finance

- **Iniciadores** de pago
- **APIs**
- **Ecosistemas** digitales
- **Comercialización** de tecnología e infraestructura

## Terceros

- **Gestión** de seguridad de la información y ciberseguridad
- **Incidentes** cibernéticos



## Gestión de riesgos de tecnologías emergentes

- **Nube** (Errores en configuración)
- **Blockchain**
- **Robots**
- **Computación cuántica** (retos criptográficos)

## Operaciones monetarias más seguras

- **Biometría Comportamental**
- **3D Secure**
- **Tokenización**

## Resiliencia de TI

- **Gestión de obsolescencias**
- **Simulación de incidentes**

# El Supervisor no es ajeno a estos desafíos, por eso nos preparamos para enfrentarlos de **manera articulada** con otras autoridades y con el sector privado

**Simulación** periódica de incidentes cibernéticos sectoriales con la participación de **la industria y autoridades nacionales** de seguridad digital.

Fomentar el intercambio **automatizado** de información de amenazas e incidentes cibernéticos.

**Consolidación** de equipos de trabajo especializados en fraude, ciberseguridad, resiliencia operacional, analítica de datos para **fortalecer** la supervisión y aplicación de mejores prácticas internacionales.

Actualizar la CE 007 de 2018 con respuesta al **ransomware** (gestión, pago de rescate, compilación de llaves) y la actualización de NIST.

Publicación de la guía de gestión de incidentes cibernéticos de terceros para **fortalecer su gestión** de la seguridad de la información.

# Descárguela en su dispositivo

@SFCsupervisor

Superintendencia Financiera de Colombia

superfinanciera

Superintendencia Financiera de Colombia

superfinanciera


**super@superfinanciera.gov.co**

**www.superfinanciera.gov.co**