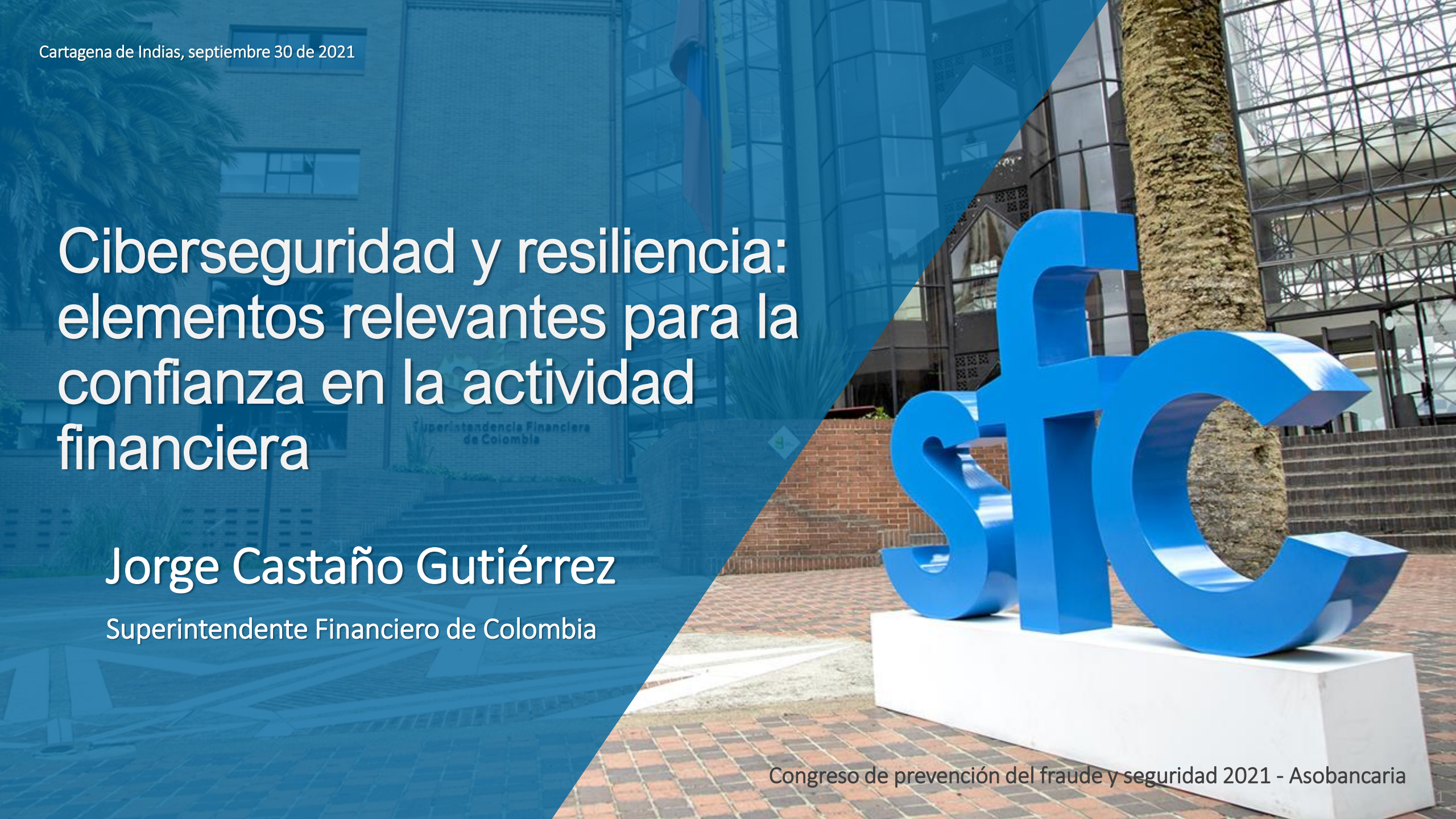
Cartagena de Indias, septiembre 30 de 2021

Ciberseguridad y resiliencia: elementos relevantes para la confianza en la actividad financiera

Jorge Castaño Gutiérrez

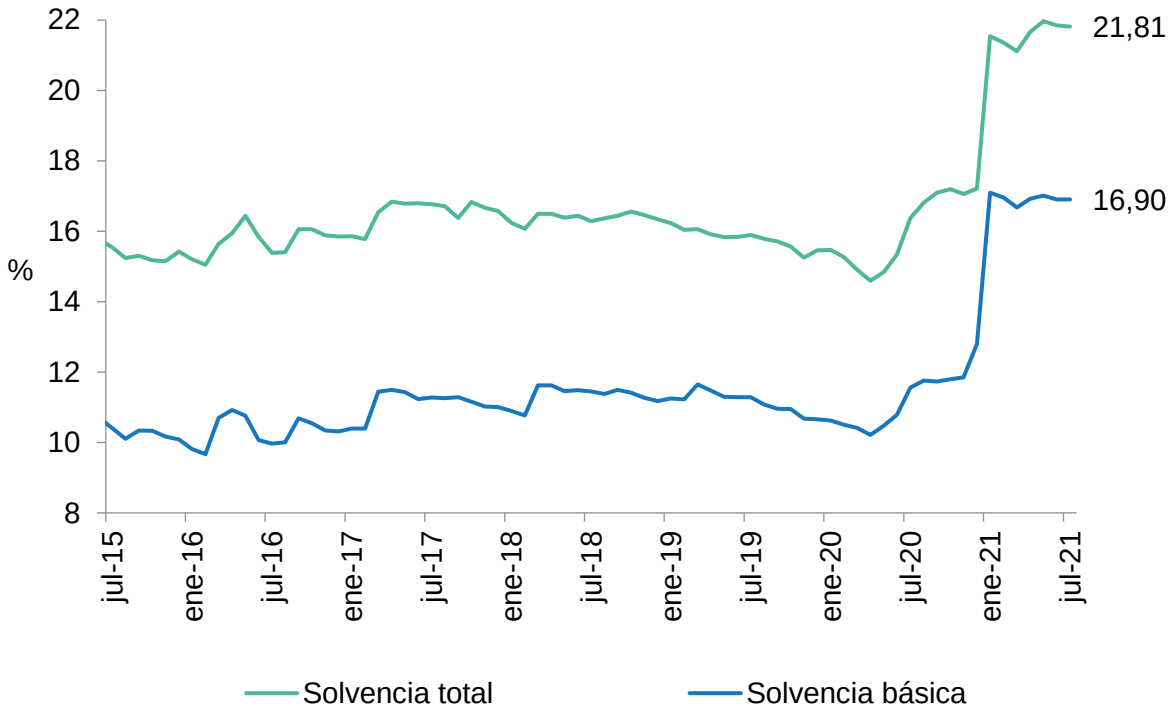
Superintendente Financiero de Colombia



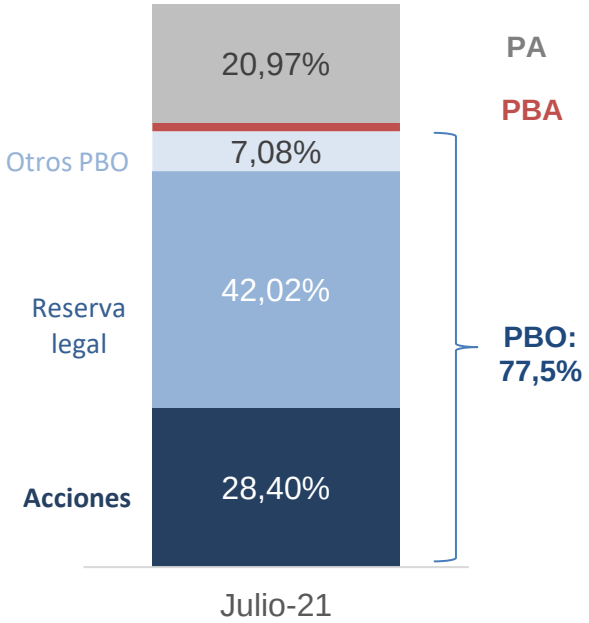
Congreso de prevención del fraude y seguridad 2021 - Asobancaria

La confianza en el sistema financiero se fundamentó por años en la capacidad de proteger el recurso del público mediante el fortalecimiento de la calidad patrimonial de las entidades

Evolución de la relación de solvencia



Un capital de mejor calidad



Esta capacidad fue puesta a prueba durante la pandemia donde quedó demostrada la facilidad de adaptación y la solidez del sistema financiero para enfrentar choques extremos.

Fuente Cálculos SFC, incorpora la convergencia a Basilea III.

La transformación digital nos enfrenta a una nueva dimensión de confianza que se construye a partir de entidades capaces de cumplir la promesa de valor: calidad del servicio, seguridad de la información y de las transacciones

Niveles de madurez

Tipo de entidad	Ciberseguridad	Continuidad del servicio
Corporaciones financieras	Básico	Optimizado
SPBV	Básico	Interiorizado
Bancos	Interiorizado	Interiorizado
Compañías de financiamiento	Interiorizado	Interiorizado
Cooperativas	Básico	Interiorizado

Criterios de evaluación

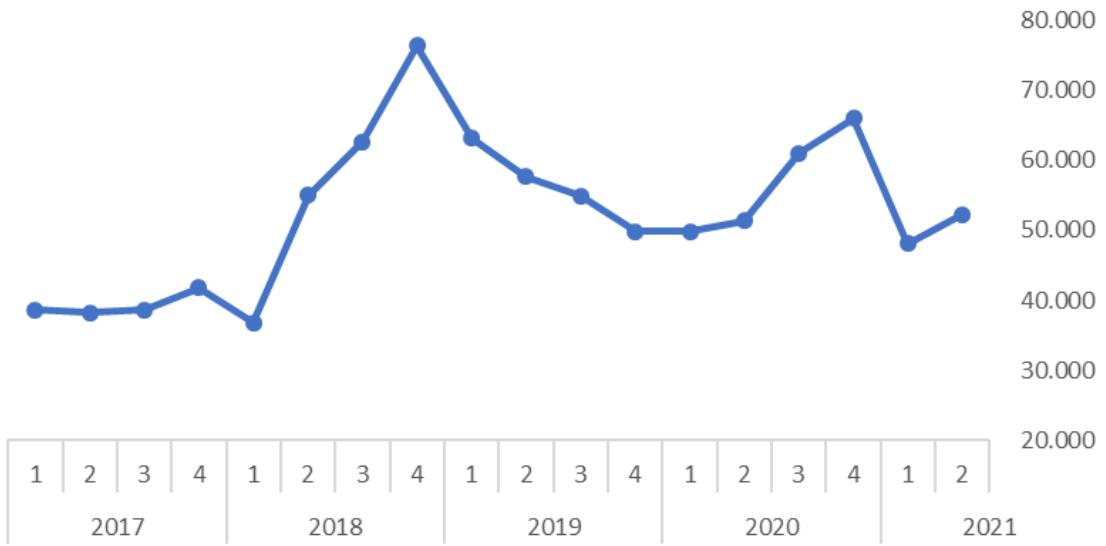
Calif.	Nivel	Controles o planes con:
5	**Visionario**	Máximo grado de automatización, institucionalización y adaptación a cambios del entorno.
4	**Optimizado**	Máximo grado de automatización e institucionalización.
3	**Interiorizado**	Estandarizados, medidos y automatizados de acuerdo con políticas.
2	**Básico**	Documentados y semiautomatizados.
1	**Inicial**	Inexistentes o parcialmente desarrollados.

Disponibilidad bancos

Canal	Disponibilidad agosto 2021	Canal	Disponibilidad agosto 2021
CB	99,7%	Internet	99,5%
IVR	99,6%	Oficinas	98,9%
Banca Móvil	99,5%	ATM	97,8%

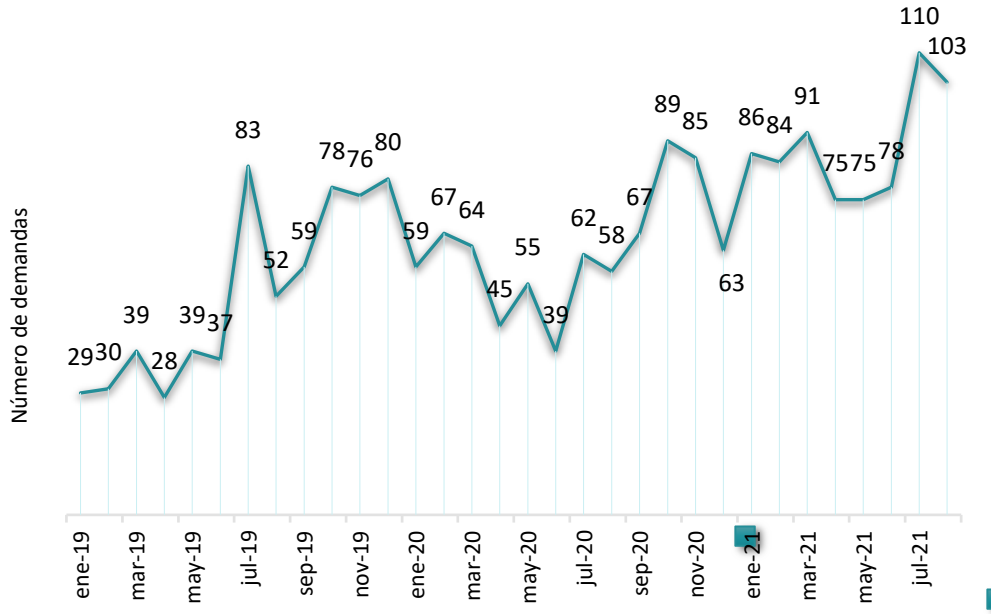
Las inconformidades de los consumidores frente a la seguridad de las transacciones y disponibilidad de los canales crecen a medida que son digitalmente más activos

Inconformidades por suplantación o fraude por trimestre



El incremento reciente de las inconformidades asociadas al fraude y suplantación coincide con el período de auge transaccional en la pandemia.

Demandas por fraude electrónico y presencial

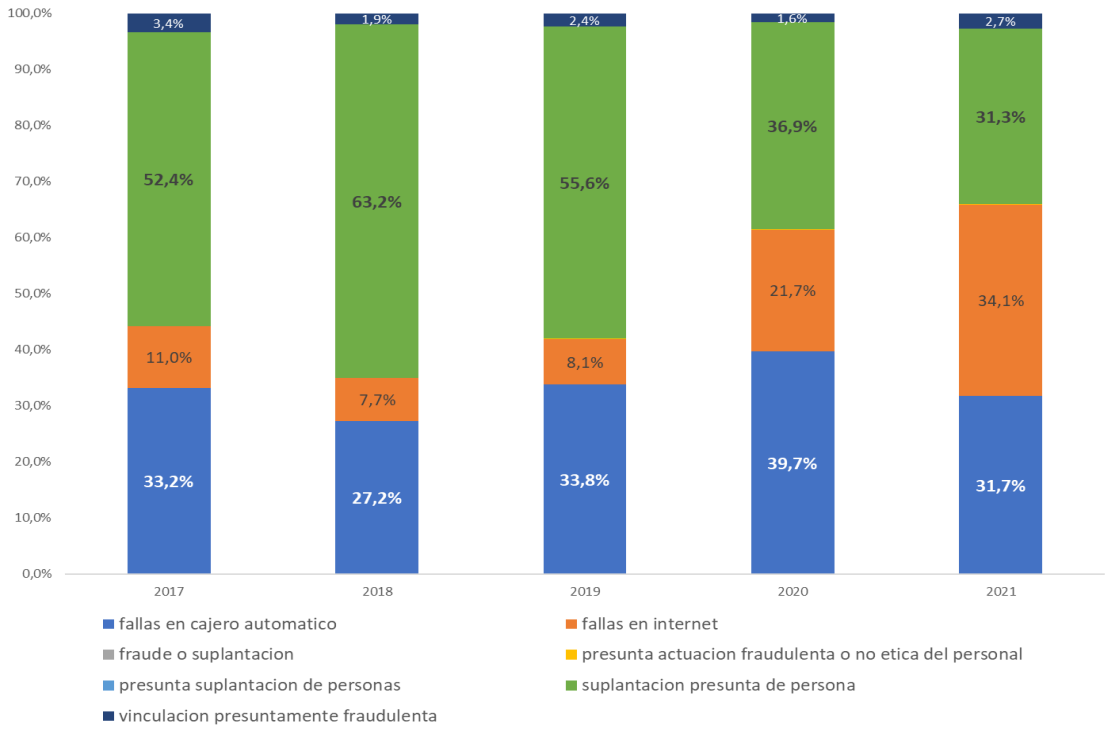


El motivo de demanda por fraude electrónico y presencial ha tenido un incremento comparativo (enero 2020 – agosto 2020 Vs. enero 2021- agosto 2021) del **56,3%.**

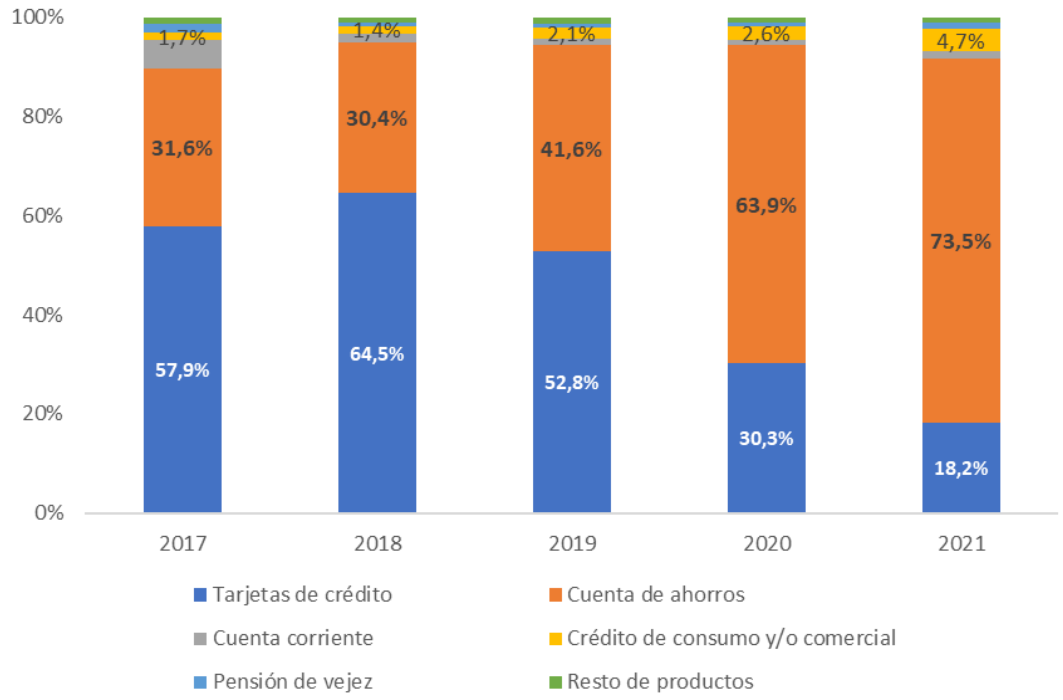
Fuente: Formatos 378, 379 y 537

Suplantación y fallas en la prestación del servicio en los productos masivos de ahorro y crédito son los motivos de inconformidad más frecuentes en los consumidores

Quejas por fallas en la prestación del servicio



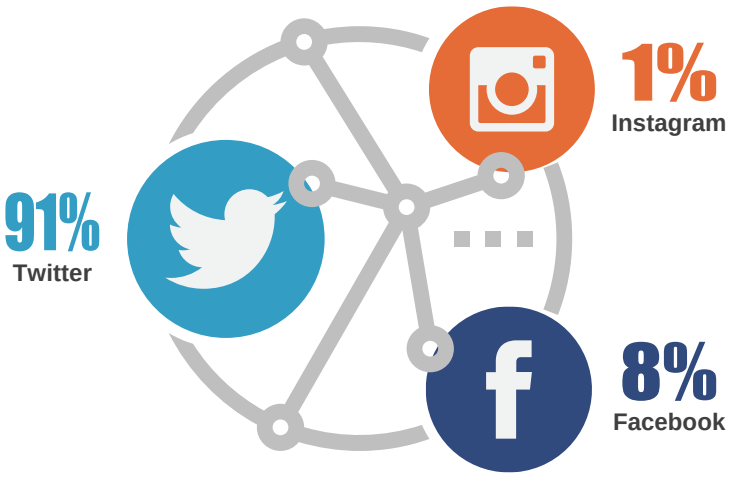
Quejas por fraude debido a suplantación



La suplantación sigue siendo un fenómeno que requiere acciones concretas que mantengan un balance entre **agilidad e inmediatez** de los servicios y la adecuada validación de la identidad de los usuarios.

Se incluyen también los motivos “Fallas en cajero electrónico” y “Fallas en Internet”.
Fuente: Formatos 378, 379 y 537 e Inconformidades que llegan a la SFC radicadas por los Consumidores Financieros. Reporte entre Ene-17 y Jun-21

Los consumidores son cada vez más activos en redes sociales y se convierten en una fuente de información sobre conductas o fallas relevantes al momento de gestionar los riesgos. No es solo un tema reputacional



Cultura de ciberseguridad: para la industria es imperativo priorizar la gestión de los riesgos de ciberseguridad y los que se derivan de las tecnologías disruptivas

Encuesta de los principales riesgos emergentes desde la perspectiva de los CEO

2020		2021	
1	Riesgos de RR.HH.	1	Riesgo de ciberseguridad
2	Riesgo de cadena de valor	1	Riesgo de cambio climático
3	Retorno al proteccionismo	1	Riesgo de cadena de valor
4	Riesgo de cambio climático	2	Tecnologías disruptivas
4	Riesgo de ciberseguridad	2	Riesgo regulatorio
6	Tecnologías disruptivas	2	Riesgo operacional

Retos en materia de gestión de riesgos sector real y financiero

Elaboración propia, basado en KPMG 2021 CEO Outlook. Link

Reconociendo además que el trabajo remoto, la integración al ecosistema Fintech y el aumento del e-commerce requieren estrategias concretas

Trabajo remoto

Teletrabajo

46%

De los 107.106 colaboradores de la industria bancaria, 49.575 se encuentra en teletrabajo.

Presencialidad

60%

De los 49.575 colaboradores en teletrabajo, el 60% volverá en 2021 a las instalaciones.

Terceros

16%

Los bancos cuentan con 65.881 colaboradores de los terceros, 10.717 se encuentran en teletrabajo.

Ecosistema Fintech

Incumbentes

Modernización de estrategias de transformación digital.

Cooperación

Modelos de BaaS, BaaP, marketplace y corresponsalía digital.

Nuevos jugadores

Certificado de Operación Temporal para nuevos jugadores.

E-commerce

Adquirentes no bancarios

Estándares para interacción con terceros

Recomendaciones

- Evaluar la consistencia de las alternativas de recuperación
- Incrementar la frecuencia de las pruebas al PCN
- Dimensionar los recursos tecnológicos para cumplir la promesa de servicio

Superintendencia Financiera de Colombia

Fuente: Reporte de resultados transversal “Evaluación sobre la gestión de los riesgos y controles en la operación de entidades vigiladas, derivados de la emergencia sanitaria” SFC junio 2021.

La SFC cuenta con una estrategia integral basada en el fortalecimiento de las capacidades en materia de ciberseguridad y ecosistema seguro: CSD

Monitoreo de canales no presenciales

- Monitoreo desde tres localizaciones: Colombia, Europa y Estados Unidos.
- Monitoreo de ataques de *Defacement* (cambios en la página web).
- Monitoreo en listas negras.

176 Entidades

- 398 URLs
- 103 URLs

Alertas de disponibilidad, caducidad de certificados digitales y dominio en tiempo real.

Seguimiento a las entidades y elaboración de planes de mejora.

Postura de ciberseguridad

Seguimiento a la postura de ciberseguridad de las entidades vigiladas.

Configuración de **grupos de análisis** por industria o grupo de interés.

Promedio score de riesgo aplicado a 156 entidades: B – 8,1.

Alertas en tiempo real e informes semanales y diarios.

Requerimiento a 156 entidades
Implementar planes para corregir los hallazgos.

Fuente: Reporte de resultados transversal “Evaluación sobre la gestión de los riesgos y controles en la operación de entidades vigiladas, derivados de la emergencia sanitaria” SFC junio 2021.

Los instrumentos de medición son fundamentales para avanzar en la estrategia: contamos con resultados concretos en múltiples frentes, sin olvidar los simulacros

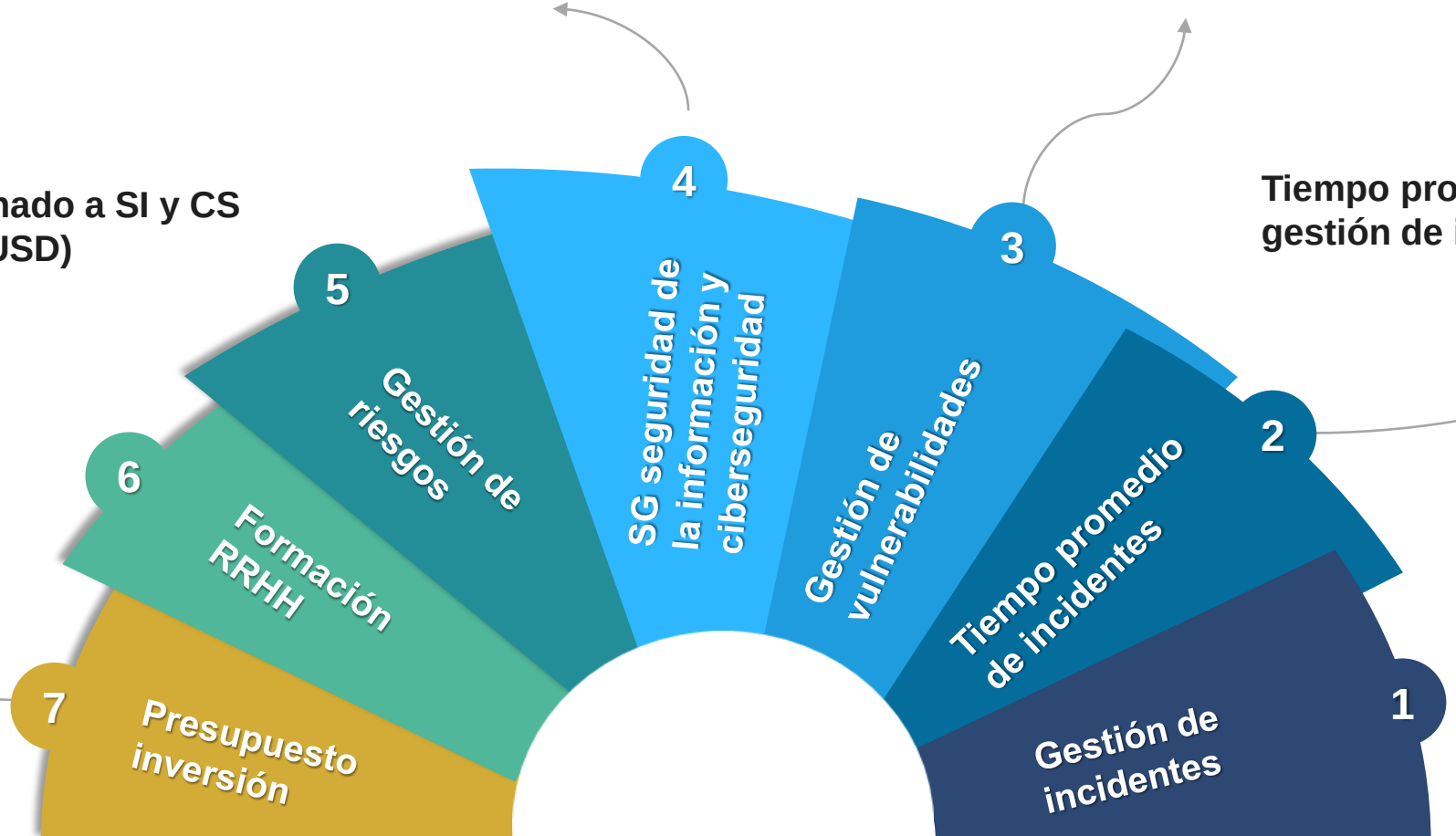
Indicadores Circular Externa 033 de 2020 a junio 2021

Efectividad de contención de ataques cibernéticos
2T
99,97%

Gestión de incidentes cibernéticos
2T
92,00%

1T
$89,5
Presupuesto anual asignado a SI y CS
(Valores en millones de USD)

Tiempo promedio de gestión de incidentes
2T
6,4 días



La puesta en marcha de la Circular Externa 029 de 2019 contribuye a mejorar la confianza de los consumidores financieros. Es necesario gestionar continuamente los riesgos emergentes implementando:

Mecanismos fuertes de autenticación

Seguimiento a la inclusión de MFA para las operaciones que generen mayor exposición al riesgo de fraude o suplantación.

Biometría como factor de verificación

Implementación de biometría como un segundo factor de autenticación y requisitos mínimos de seguridad para su aplicación.

Notificación de la inscripción de pagos

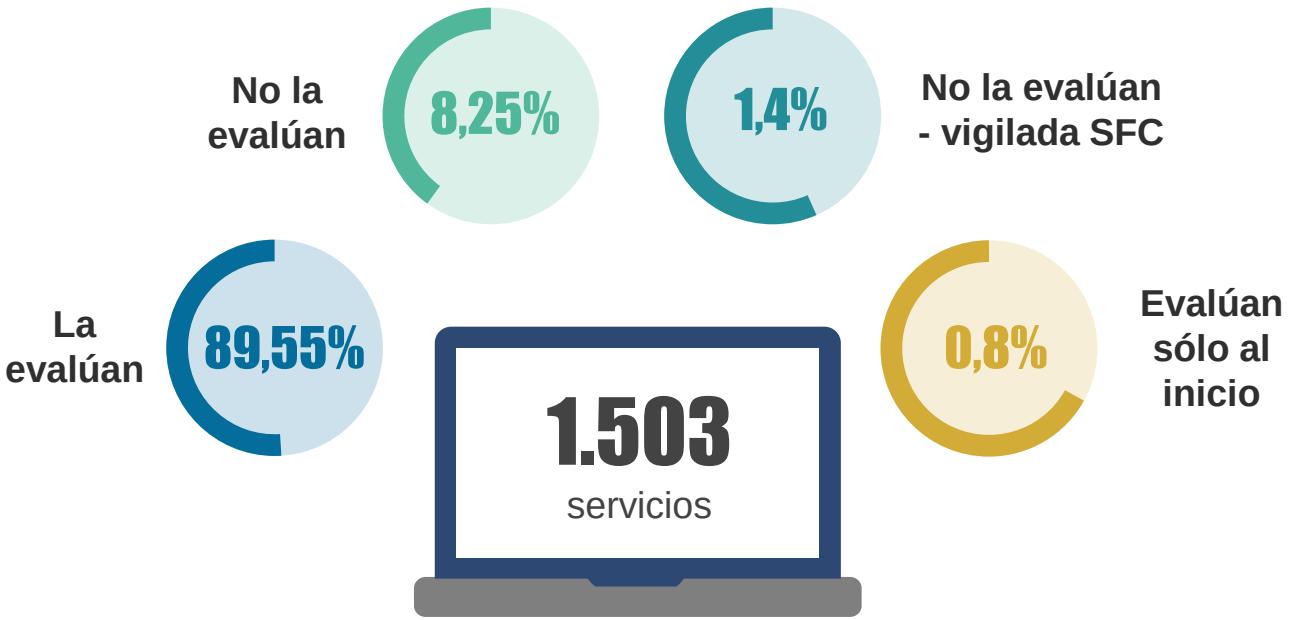
Incentivar la domiciliación y notificar la inscripción de pagos de cuentas y tarjetas de los consumidores.

Recursos de seguridad

Adopción de herramientas confiables que permitan realizar operaciones en ambiente no presente.

La inadecuada gestión de los terceros críticos incrementa los riesgos operacionales y de ciberseguridad de las entidades

Evaluación de la capacidad operativa



El 16% de las entidades requiere mejorar los ciclos de evaluación de riesgos y análisis de impactos.

El 11% de las entidades debe realizar evaluaciones periódicas a la capacidad operativa de los terceros críticos.

¿Qué se debe fortalecer?

1. Los recursos y los procesos para su **evaluación**.

2. Las políticas, estrategias y mecanismos de evaluación de los PCN y el **nivel de exigencia** de pruebas con otros escenarios como: pandemias, desastres naturales y ciberataques.

3. La gestión de riesgos de los terceros y los del uso, procesamiento, almacenamiento o pérdida de información confidencial **durante y después** de la finalización de los contratos.

Fuente: estudio trasversal SFC

La figura de los líderes de seguridad de la información (CISO) tiene un papel indispensable en el éxito de esta estrategia

Formación de capacidades del Chief Information Security Officer (CISO)

1 Ventajas competitivas

Sostenibles a través de métodos pragmáticos e innovadores y soluciones de seguridad.

2 Integridad y capacidad

Para mantener los principios bajo presión interna y/o externa.

3 Habilidades analíticas de alta calidad

Así como toma de decisiones fundamentadas en el análisis de datos.

4 Participación activa en planificación estratégica

Desarrollo de políticas a nivel superior.

5 Visionario

Para anticipar, influir y ayudar a la organización a evaluar y adaptarse rápidamente a condiciones cambiantes.

6 Eficacia en la comunicación

Con relación a los cursos de acción recomendados y la adopción de respuestas innovadoras, orientadas a preservar la resiliencia del negocio.

Desde la SFC seguiremos impulsando espacios colaborativos para fortalecer las capacidades de atención a incidentes e intercambio de información que consoliden los avances alcanzados

Actividades para la promoción de un ecosistema financiero digital y más seguro

Supervisión de gestión de incidentes en arquitectura cloud

Alianza del Pacífico

Guía de seguimiento de incidentes en cloud.

Plataforma única para el reporte de incidentes

BID Banco Interamericano de Desarrollo

Definición de la plataforma.

Simulación incidente cibernético

Colombia y México. **(Nov. 2021)**
Chile y Perú. **(Marzo 2022)**

Infraestructura crítica cibernética (ICC)

Metodología de identificación de ICC.

Jornadas de capacitación y sensibilización sobre ciberseguridad.

Encuentro AP-21. Ciberseguridad: reflexiones de un riesgo sistémico, emergente y disruptivo.
Octubre 2021.

Descárguela en su dispositivo

Superintendencia Financiera de Colombia

#LaSuperSomosTodos

super@superfinanciera.gov.co
www.superfinanciera.gov.co

superfinanciera

superintendencia.financiera

@SFCsupervisor

/superfinancieracol