Confianza digital: un valor que debemos fortalecer en un entorno de innovación y disrupción

13º Congreso de prevención del fraude y seguridad

Juliana Lagos Camargo

Superintendente Financiero (E)

Cartagena de Indias, Octubre 24 de 2019

Superintendencia Financiera de Colombia

Entidades, autoridades y consumidores tenemos un rol fundamental en la construcción de confianza

Donde los desafíos son cada vez más complejos para una industria que apalanca su crecimiento en los servicios digitales

Ciberseguridad y vulnerabilidad de los datos

Un riesgo que impacta materialmente a las entidades financieras.

Open Banking

Representa un cambio radical de cómo operarán las instituciones financieras en todo el mundo.

Canales digitales en crecimiento

En línea con las tendencias mundiales, los canales digitales en Colombia han crecido más de un 40%.

Ingeniería social

Nuevas formas de aprovechamiento de las diferentes fuentes de información.

Ciberseguridad: avanzamos decididamente en la implementación de mejores estándares

Gobierno

Creación de la Unidad de Seguridad de la Información y la Ciberseguridad.
Participación activa de la Junta Directiva y la Alta Gerencia.

Madurez

Evaluación de la madurez de la seguridad digital, establecer oportunidades de mejora, actualizar los planes y las estrategias de gestión de la ciberseguridad.

Comunicación

Informar sobre los incidentes que afecten la seguridad de la información a los titulares, autoridades y a la SFC.

Buenas prácticas

en el desarrollo de proyectos, particularmente en los relacionados con innovación y transformación digital.

Capacitación

a empleados, proveedores, clientes y usuarios para elevar la cultura de seguridad digital, el desarrollo de capacidades y una mayor sensibilización.

Gestión de incidentes

Estrategia de priorización, contención, respuesta y recuperación frente a incidentes de ciberseguridad y colaboración con equipos de respuesta a incidentes.

Proceso en el que el compromiso de la industria ha sido contundente

Capacitación

- A todos los grupos de interés.
- Estudio de incidentes en otras organizaciones.
- Campañas para prevenir *smishing* y *vishing*.

Gobierno

- Todas las entidades cuentan con políticas, estrategias y unidades de gestión de seguridad de la información y ciberseguridad aprobadas.
- La Junta Directiva y los comités de junta analizaron el tema en al menos dos sesiones entre enero y mayo de este año.
- Las entidades están destinando el 2.46% de su presupuesto a seguridad de la información y ciberseguridad.

Comunicación

- Se informó al COLCERT 51 incidentes en los primeros cinco meses del año.

***Las entidades han reportado un avance del 98% en la implementación de la Circular Externa 007 de 2018.**

Así como el compromiso de las autoridades: la articulación es fundamental

Implementación de la Política Nacional de **Confianza y Seguridad Digital** : protección de las infraestructuras críticas cibernéticas y mesa de trabajo del sector financiero.

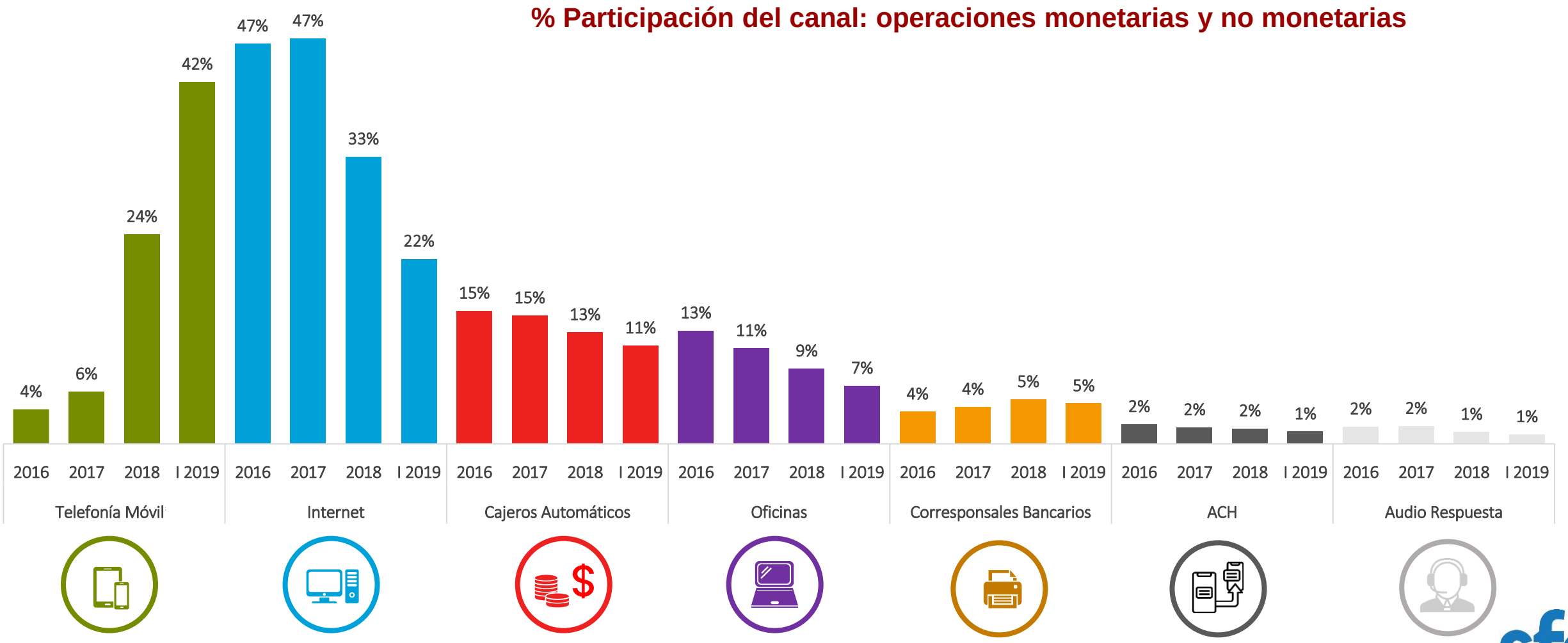
Trabajo conjunto entre la Asociación Bancaria, COLCERT y la Superintendencia para establecer un protocolo de reporte de incidentes.

Adhesión de Colombia al convenio de Budapest: compartir información y evidencias digitales, penalización de delitos informáticos.

Consolidación de mejores prácticas en la región a través de la **interacción de supervisores** y autoridades en el Consejo Centroamericano de Supervisores Bancarios.

Colaboración con otros supervisores para fortalecer la gestión de la ciberseguridad en la Alianza del Pacífico.

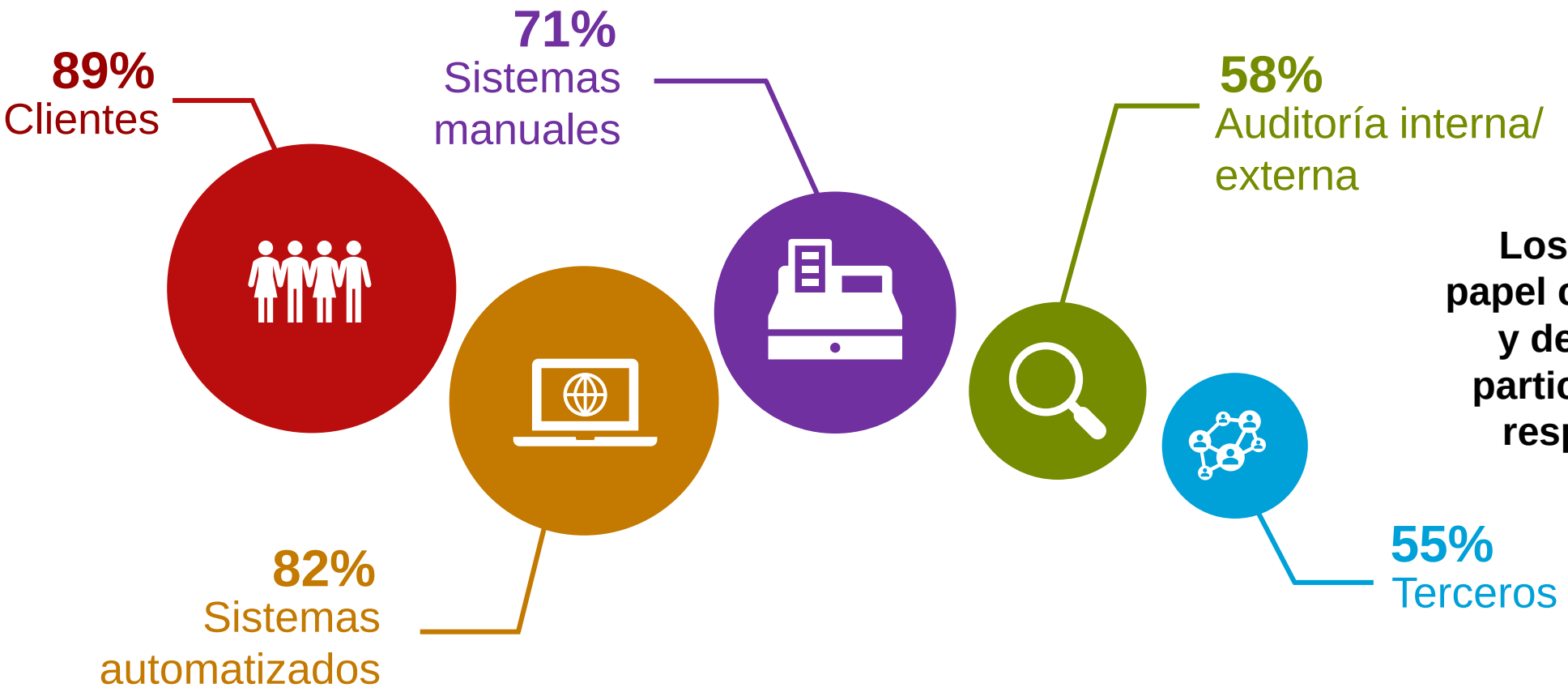
Canales digitales: la respuesta a la necesidad de inmediatez de los consumidores



Fuente: Superintendencia Financiera de Colombia, Informe de Operaciones Primer Semestre 2019

En donde el reto cada vez es más complejo frente a la oportunidad de detección del fraude: el rol del consumidor

¿Cuál es el mecanismo para identificar la actividad fraudulenta?



Los clientes juegan un papel clave en la prevención y detección del fraude, particularmente en lo que respecta a las estafas.

Fuente: Global Banking Fraud Survey, KPMG international 2019 y Pulling Fraud out of the shadow, PWC 2018

Superfinanciera
@SFCsupervisor

Sabemos que te encanta realizar tus compras y tus pagos desde el celular, por eso, sólo debes activar las conexiones por bluetooth y wifi cuando vayas a usarlas, evitando que se conviertan en puerta de acceso para ataques cibernéticos #MisTransaccionesSeguras

Superfinanciera
@SFCsupervisor

#MisTransaccionesSeguras No respondas correos electrónicos o mensajes de texto en los que te pidan datos personales o de tus productos financieros. OJO Las entidades financieras nunca piden esta clase de información por estos medios

Superfinanciera
@SFCsupervisor

✈️ ¡Así como cuando tomas todas las medidas de seguridad para comprar ese plan de viaje que tanto soñaste, bueno, SÍ, así! ✈️ #MisTransaccionesSeguras

Superfinanciera
@SFCsupervisor

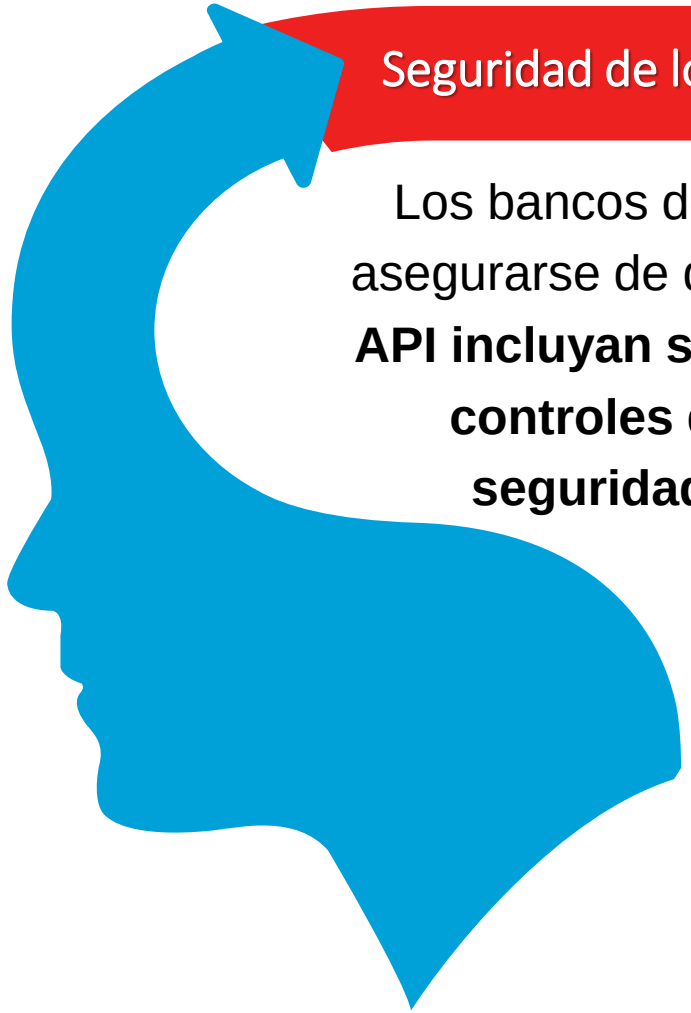
#MisTransaccionesSeguras
importantes de dinero no le
servicio de acompañamient

ula! Para acceder a los
oveedor de streaming
rección y no desde enlaces
ner en riesgo tu información
sTransaccionesSeguras

La prevención desde la fuente es fundamental: conciencia de los consumidores

sfc
Superintendencia Financiera de Colombia

Open Banking: el futuro de los servicios financieros



Seguridad de los datos

Los bancos deben asegurarse de que las **API incluyan sólidos controles de seguridad.**

Identidad digital

Open Banking depende en gran medida de un sistema integrado de identidad digital.

+

Experiencia de **autenticación segura** y sin problemas.

Gestión de acceso

Vinculación de forma segura y confidencial de un cliente a sus datos.

+

Protocolos de gestión de acceso definidos para el intercambio y uso de datos con proveedores de servicios externos.

Fuente: Global Banking Fraud Survey, KPMG international 2019

Un modelo de supervisión que promueve la cultura de gestión del riesgo

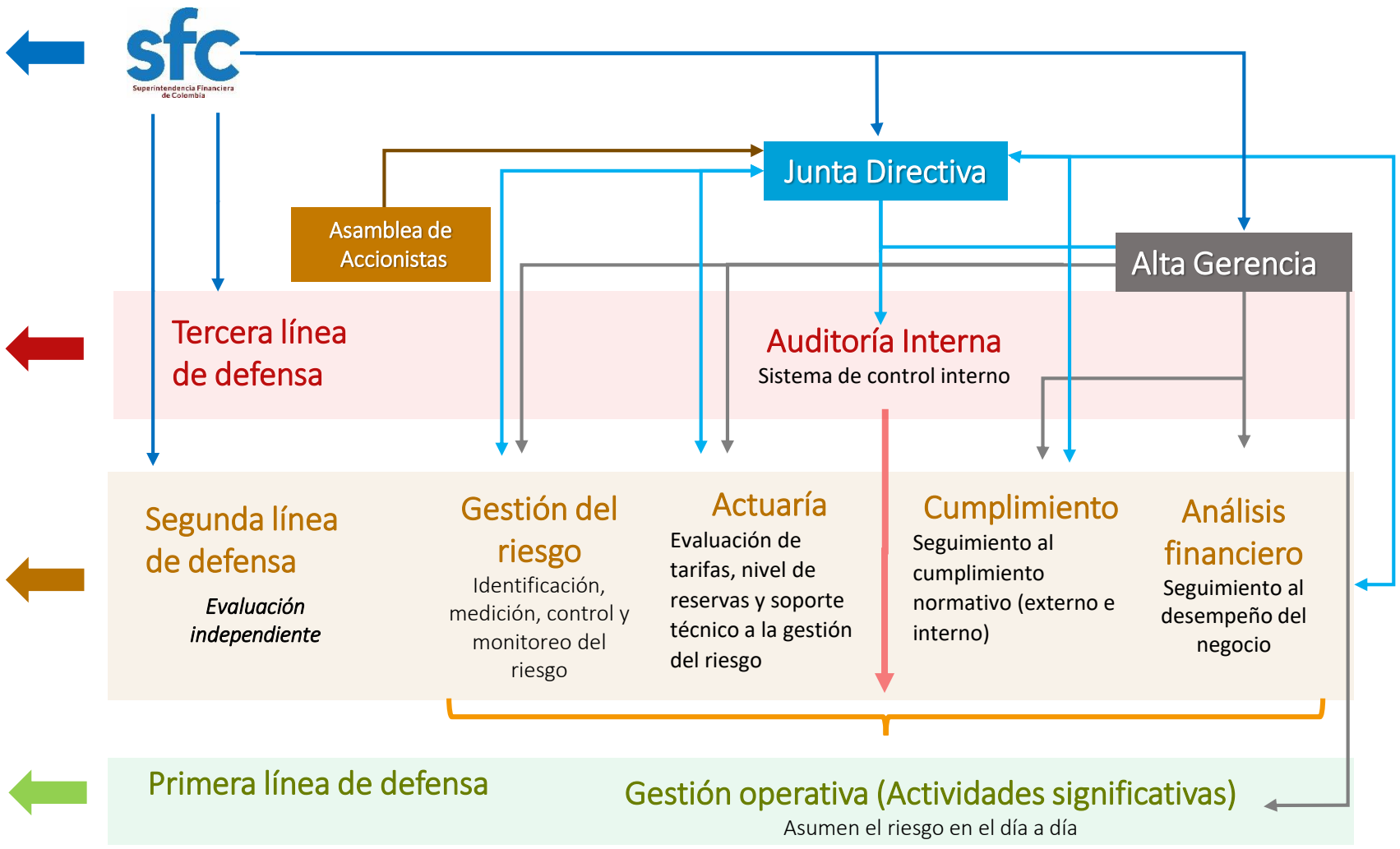
En el modelo de Supervisión Basada en Riesgos, el fraude se gestiona a través de las tres líneas de defensa de la entidad

El supervisor busca fortalecer la Estructura de Gobierno de Riesgos de las entidades supervisadas para que puedan gestionar sus riesgos de manera adecuada de acuerdo con los mejores estándares internacionales.

Evalúa de forma independiente el trabajo realizado por las dos anteriores líneas en cuanto a la gestión del riesgo de fraude. Hace recomendaciones y solicita planes de mejora.

Gestiona, mide y monitorea el riesgo de fraude como supervisión a la primera línea de defensa, establece políticas y controles adicionales para su mitigación.

Identifica el riesgo de fraude en el desarrollo de sus operaciones diarias y establece controles para su mitigación.



En resumen: se requiere un enfoque multidimensional de prevención, articulación y gestión que consolide la confianza digital

1 **Es un tema de cultura que va más allá de la organización**

2 **Estrategia colaborativa**

3 **Detección oportuna**

4 **Aprovechar el poder protector de la tecnología**

5 **Concientización del consumidor**

6 **Simulación de incidentes basado en otras experiencias**

7 **Enfoque de inversión y no de gasto**

Fuente: SFC.

Descárguela en su dispositivo

superintendencia.financiera

@SFCsupervisor

Superfinanciera

/superfinancieracol

Gracias

super@superfinanciera.gov.co

www.superfinanciera.gov.co