Hacia una gestión multidimensional de la ciberseguridad

12º Congreso de prevención del fraude y seguridad - Asobancaria

Jorge Castaño Gutiérrez

Superintendente Financiero

Bogotá, Noviembre 15 de 2018

sfc
Superintendencia Financiera de Colombia

Ante la tendencia creciente del cibercrimen, la gestión de la ciberseguridad es un imperativo

Algunos datos a nivel global

6.4 billones

de "fake e-mails" enviados diariamente en el mundo.

2 millones

de identidades robadas utilizadas para falsificar comentarios durante una investigación en EE.UU. sobre la neutralidad de la red.

1,946,181,599

de registros que contienen datos personales y que fueron comprometidos entre enero de 2017 y marzo de 2018.

US 3.6m

costo promedio de un evento de violación de datos en el último año.

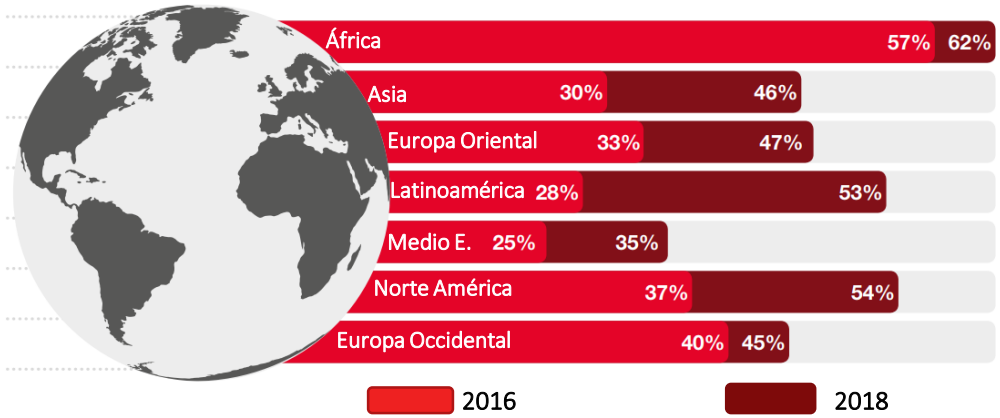
2 billones

de ciberataques a nivel global

Fuente: Adaptado por la SFC de "Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19

Latinoamérica presenta el mayor crecimiento de la tasa de fraude a nivel global

Tasa de fraude o crimen económico a nivel regional



El 49% de las empresas en el mundo afirman haber sufrido algún tipo de fraude en los últimos dos años.
En Colombia, este indicador es de 39%.

El fraude cibernético continúa siendo el principal delito.

Fuente: "Pulling fraud out of the shadows" Global Economic Crime and Fraud Survey 2018 y "Fraude al descubierto" Encuesta Global de Crimen Económico en Colombia PWC 2018

El fraude no es un mal menor, sus consecuencias impactan a toda la organización, incluyendo las partes relacionadas

Mayor gasto en tecnología/ Herramientas de mitigación

El precio por acción

La percepción de los empleados

Las relaciones empresariales

La reputación/fortaleza de la imagen

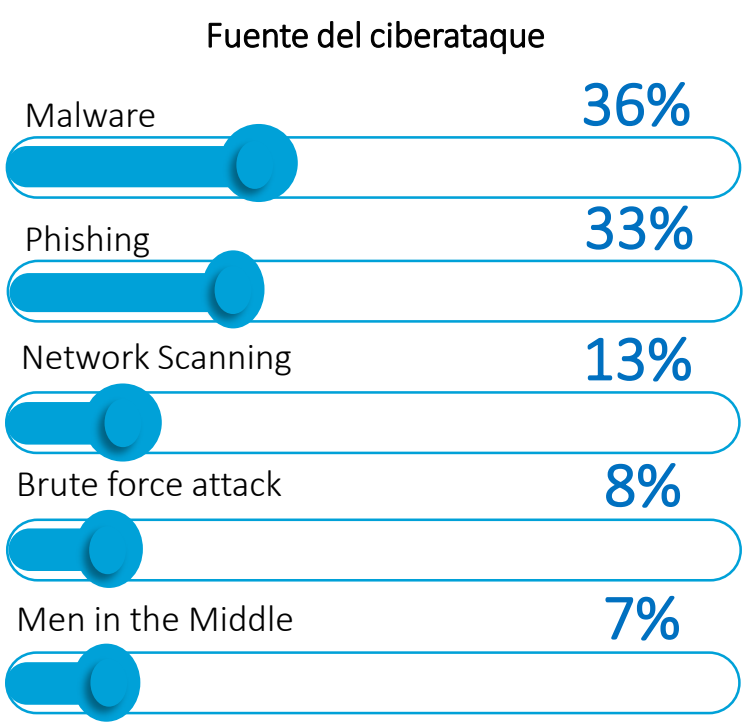
Las relaciones con los reguladores

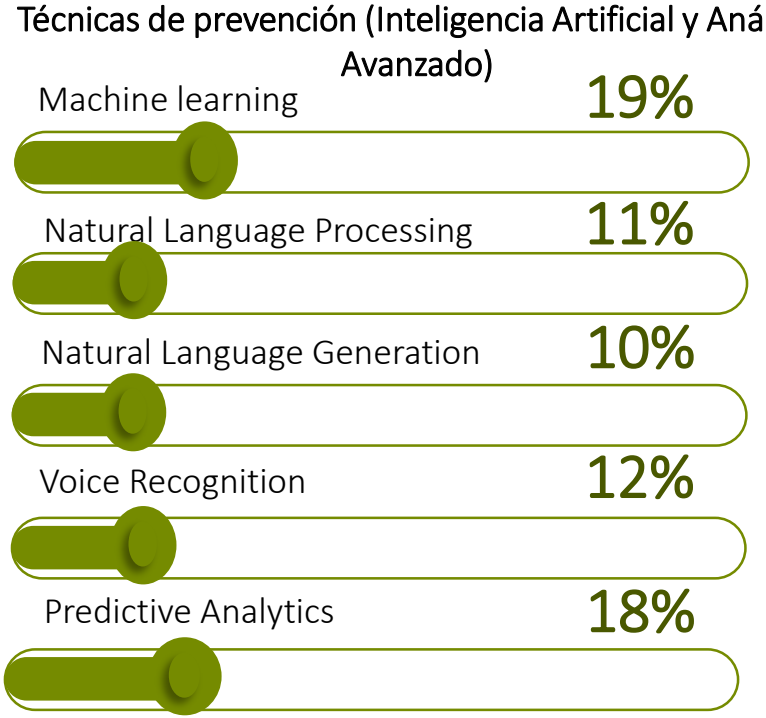
Fuente: Adaptado por la SFC de "Pulling fraud out of the shadows" Global Economic Crime and Fraud Survey 2018

Hay que estudiar al “enemigo”, conocer su *modus operandi* y plantear estrategias para anticiparnos.

Fuente: Citi Cyber & Fintech forum for regulators Nov 2018

La tecnología nos debe ayudar a tener análisis dinámicos basados en comportamientos

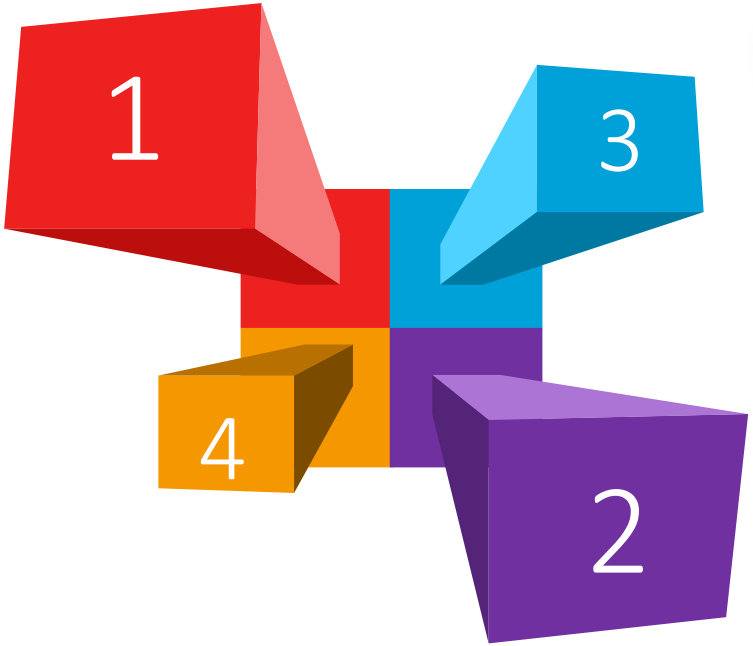




Esta área especializada está llamada a usar la tecnología como blindaje frente a las posibles amenazas de fraude

Fuente: Adaptado por la SFC de "Pulling fraud out of the shadows" Global Economic Crime and Fraud Survey 2018

Las entidades deben tener un enfoque multidimensional para garantizar una gestión preventiva del riesgo de ciberseguridad



Es un tema de cultura que va mas allá de la organización.

La JD, riesgos y auditoría interna deben participar activamente, adicionalmente se deben diseñar estrategias que fortalezcan la cultura organizacional y la vinculación de expertos en el tema. Clientes y proveedores son igualmente relevantes.

Apoyo de terceros especializados

Aprovechar la experiencia de entidades especializadas y visionarias en la gestión de ciberseguridad.

Estrategia colaborativa

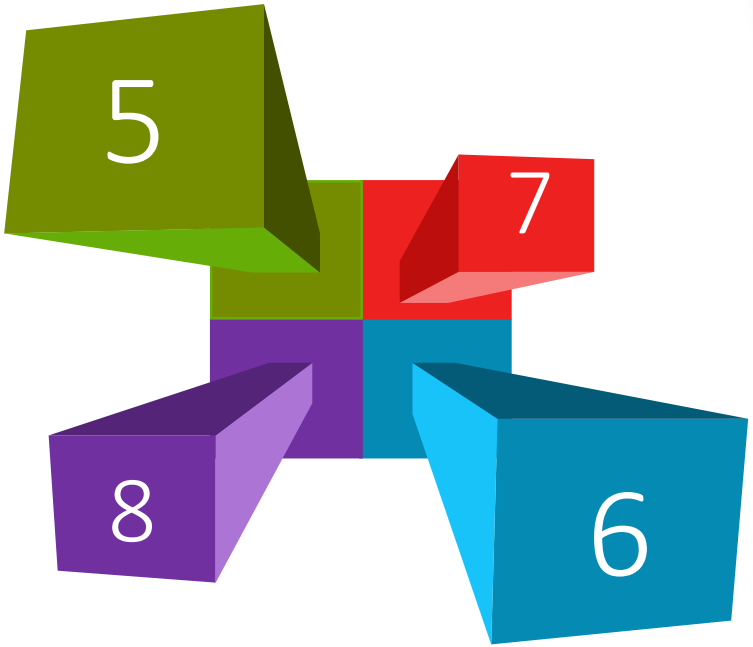
Se deben reportar los incidentes con los pares y las autoridades.

Detección oportuna

En el 80% de los casos el daño se hace en minutos y las entidades lo detectan semanas o meses después.

Fuente: SFC.

Las entidades deben tener un enfoque multidimensional para garantizar una gestión preventiva del riesgo de ciberseguridad



Aprovechar el poder protector de la tecnología

Big Data para identificar ataques, correlacionando eventos. Inteligencia artificial y machine learning para analizar comportamientos de usuarios y equipos y detectar situaciones inusuales.

Reducir la superficie de ataque

Dar acceso a los sistemas y la información solamente a quienes lo necesitan. Ejm: email, plataformas, chats y móviles

Simulación de incidentes basado en otras experiencias

Estudiar el software malicioso y replicar ataques sufridos por otras entidades para identificar controles adicionales.

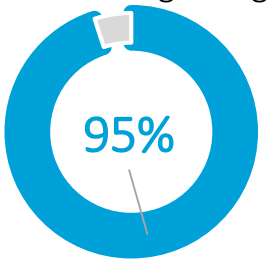
Enfoque de inversión y no de gasto

El costo económico y reputacional de los ataques cibernéticos supera la inversión en estrategias de prevención.

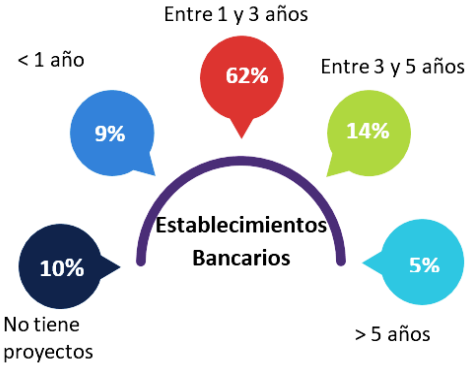
Fuente: SFC.

Ciberseguridad (CS) y Seguridad de la Información (SI) en establecimientos bancarios en Colombia

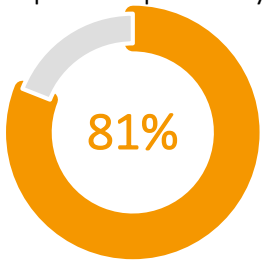
Cuenta con planes para fomentar tecnologías digitales.



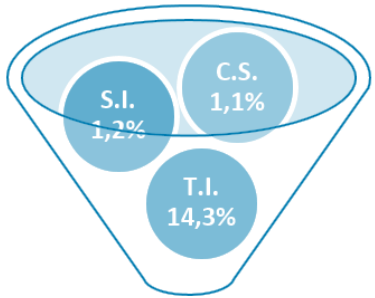
Tiempo para desarrollar proyectos que fortalezcan la SI y CS.



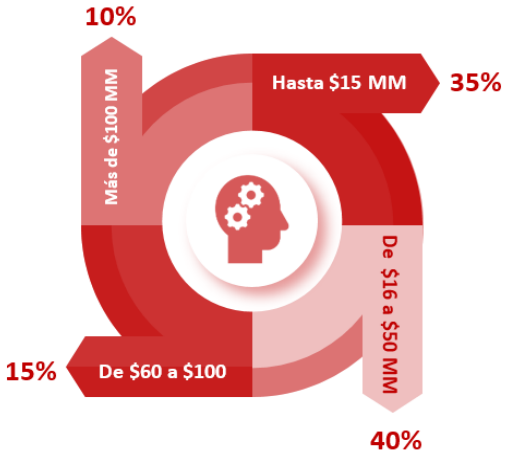
Asigna a la gestión de riesgos presupuesto para SI y CS



Participación SI, CS, TI en presupuesto total 2017



Presupuesto destinado para capacitaciones en SI y CS 2017

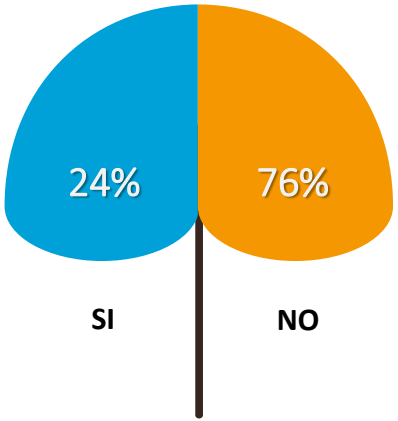


Estadísticas de SI y CS

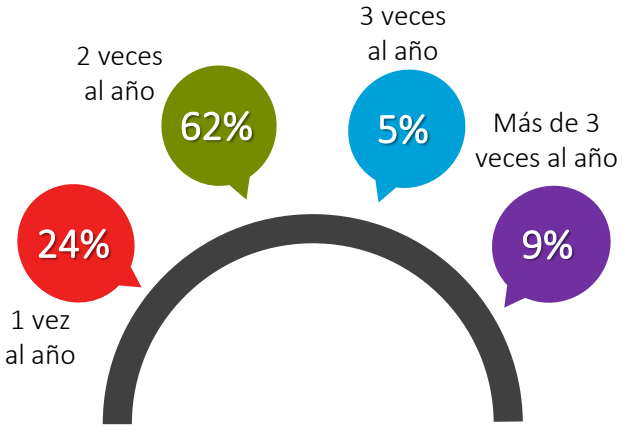
Fuente: SFC, Informe de Seguridad de la Información y Ciberseguridad

Ciberseguridad (CS) y Seguridad de la Información (SI) en establecimientos bancarios en Colombia

Cuentan con alguna certificación en SI



Periodicidad de las pruebas de hacking ético



Número de ataques cibernéticos (phishing, malware, denegación de servicio, etc.) recibidos en todas las entidades

39.145.253

- de ataques cibernéticos en 2016

17.821.293

- de ataques cibernéticos 1S17

Los ataques recibidos fueron detectados y contenidos, por lo tanto, NO afectaron la operación, el servicio ni la reputación de las entidades.

Fuente: SFC, Informe de Seguridad de la Información y Ciberseguridad

La mitigación de este riesgo está en la agenda del Supervisor: Circular Externa 007 de 2018 sobre Ciberseguridad

1. Prevención

Desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la ciberseguridad.

✓Ajustar los Planes de Continuidad del Negocio.
✓ Informar a los consumidores financieros las medidas de seguridad para la realización de operaciones.

2. Protección y detección

Desarrollar e implementar actividades para identificar eventos de ciberseguridad.

✓Gestionar vulnerabilidades.
✓ Monitorear la plataforma tecnológica para identificar comportamientos inusuales.

3. Respuesta y comunicación

Desarrollar e implementar actividades para mitigar los incidentes de ciberseguridad.

✓Reportar al ColCERT los ataques cibernéticos.
✓ Informar al consumidor financiero y a la SFC los incidentes de ciberseguridad.

4. Recuperación y aprendizaje

Mantener planes de resiliencia y restaurar la capacidad o servicios deteriorados.

✓ Ajustar los sistemas de seguridad de la información y ciberseguridad como consecuencia de los incidentes presentados.
✓ Socializar las lecciones aprendidas.

En la SFC estamos comprometidos con la innovación y la mejora continua de los productos y servicios del sector financiero

Avance de la implementación de la Circular Externa 007 de 2018 sobre Ciberseguridad

Entidades Vigiladas

Las malas noticias viajan rápido: el riesgo reputacional ahora supera el regulatorio y hemos definido una hoja de ruta

Marco normativo y regulatorio

- Planes sectoriales para la gestión de la ciberseguridad.
- Computación en la nube.
- Biometría para la realización de algunas operaciones.
- Estándar para el uso de códigos QR en el sistema de pagos.
- Metodologías de cuantificación del RO.

Cooperación

- Convenios con ColCERT y CSIRT del sistema financiero para el intercambio de información sobre amenazas cibernéticas.
- Compartir experiencias y buenas prácticas sobre ciberseguridad en el Comité de Tecnología del CCSBSO.

Supervisión

- Evaluar el nivel de madurez de la gestión de la Ciberseguridad.
- Gestión de riesgos de ciberseguridad en filiales.
- Verificar la adopción de marcos de seguridad para transferencias interbancarias.

Fortalecimiento institucional

- Plataforma para el registro y el seguimiento de incidentes cibernéticos de las entidades vigiladas.

Competencias

- Fortalecer el equipo de supervisores y las metodologías para la evaluación de la gestión de ciberseguridad.

Resiliencia operacional del sistema financiero

Descárguela en su dispositivo

superintendencia.financiera

@SFCsupervisor

Superfinanciera

/superfinancieracol

Gracias

super@superfinanciera.gov.co

www.superfinanciera.gov.co