14-15 NOVIEMBRE

HOTEL LAS AMÉRICAS
CARTAGENA DE INDIAS,
COLOMBIA.

18°CONGRESO DE RIESGO FINANCIERO

MEJORES PRÁCTICAS EN
UN CONTEXTO DESAFIANTE

José Marangunich R. – Ph.D
Head of Corporate Security & Cyber-Crime
Banco de Crédito del Perú - CREDICORP

President Strategic Committee of Security Risk Management
Peruvian Banking Association - ASBANC

Tipologías de fraude, Tendencias para su mitigación y principales riesgos

Agenda

I. **Lo importante y necesario para mitigar el fraude…** Política /Gobierno/Estrategia/ Modelo de Gestión/Estructura/Planes & Accountability

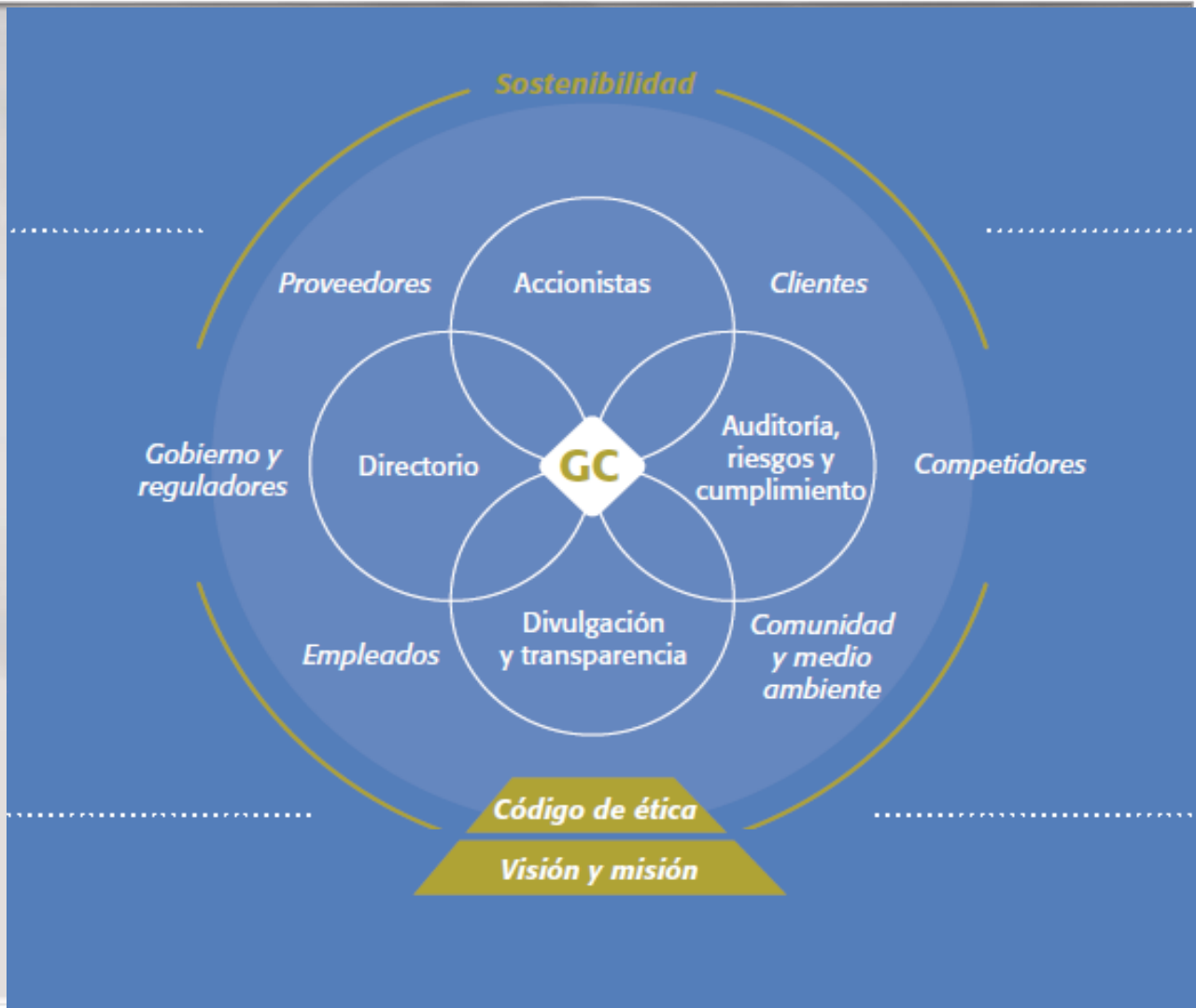
II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios nos trae?

IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital.

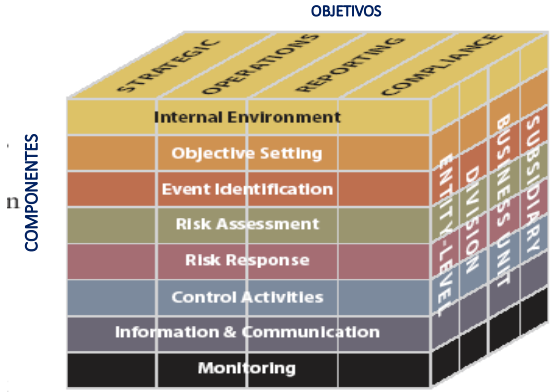
V. Comentarios finales.

Política de Gobierno Corporativo



Lo importante y necesario para mitigar el fraude:
Política

Coso 2013



1. Monitoreo
2. Información y Comunicación
3. Actividades de Control
4. Respuesta a los Riesgos
5. Evaluación de Riesgos
6. Identificación de Eventos
7. Establecimiento de Objetivos
8. Ambientes de Control

Los 17 principios fundamentales de COSO 2013 (asociados a los 5 componentes de control interno)

Ambiente de control

Principio 1: Demostrar compromiso con la integridad y valores éticos.

Principio 2: El consejo de administración ejerce su responsabilidad de supervisión del control interno.

Principio 3: Establecimiento de estructuras, asignación de autoridades y responsabilidades.

Principio 4: Demuestra su compromiso de reclutar, capacitar y retener personas competentes.

Principio 5: Retiene a personal de confianza y comprometido con las responsabilidades de control interno.

Evaluación de riesgos

Principio 6: Se especifican objetivos claros para identificar y evaluar riesgos para el logro de los objetivos.

Principio 7: Identificación y análisis de riesgos para determinar cómo se deben mitigar.

Principio 8: Considerar la posibilidad del fraude en la evaluación de riesgos.

Principio 9: Identificar y evaluar cambios que podrían afectar significativamente el sistema de control interno.

Actividades de control

Principio 10: Selección y desarrollo de actividades de control que contribuyan a mitigar los riesgos a niveles aceptables.

Principio 11: La organización selecciona y desarrolla actividades de controles generales de tecnología para apoyar el logro de los objetivos.

Principio 12: La organización implementa las actividades de control a través de políticas y procedimientos.

Información y Comunicación

Principio 13: Se genera y utiliza información de calidad para apoyar el funcionamiento del control interno.

Principio 14: Se comunica internamente los objetivos y las responsabilidades de control interno.

Principio 15: Se comunica externamente los asuntos que afectan el funcionamiento de los controles internos.

Actividades de monitoreo

Principio 16: Se lleva a cabo evaluaciones sobre la marcha y por separado para determinar si los componentes del control interno están presentes y funcionando.

Principio 17: Se evalúa y comunica oportunamente las deficiencias del control interno a los responsables de tomar acciones correctivas, incluyendo la alta administración y el consejo de administración.

Evaluación de riesgos

Principio 6: Se especifican objetivos claros para identificar y evaluar riesgos para el logro de los objetivos.

Principio 7: Identificación y análisis de riesgos para determinar cómo se deben mitigar.

Principio 8: Considerar la posibilidad del fraude en la evaluación de riesgos.

Principio 9: Identificar y evaluar cambios que podrían afectar significativamente el sistema de control interno.

Agenda

I. **Lo importante y necesario para mitigar el fraude:**

Política/Gobierno y Estrategia/ Modelo de Gestión/Estructura/Planes & Accountability

II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios trae?

IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital.

V. Comentarios finales.

Lo importante y necesario para mitigar el fraude:
Gobierno y estrategia

De la seguridad tradicional a la seguridad emergente

Seguridad Madura

Tomar mercado

Seguridad tradicional

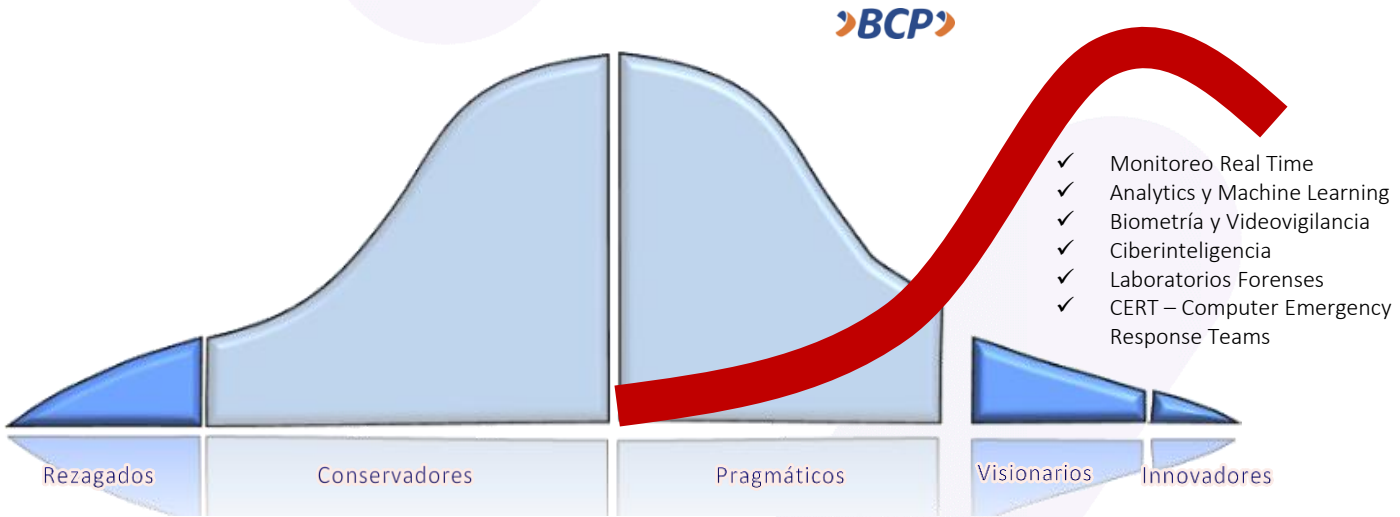
La Seguridad se visualiza como un mal necesario

Seguridad Emergente

Crear mercado

Seguridad Integral

La Seguridad se visualiza como un generador de valor



- ✓ Monitoreo Real Time
- ✓ Analytics y Machine Learning
- ✓ Biometría y Videovigilancia
- ✓ Ciberinteligencia
- ✓ Laboratorios Forenses
- ✓ CERT – Computer Emergency Response Teams

Fuente: Banco Santander, México

Lo importante y necesario para mitigar el fraude:
Gobierno y estrategia

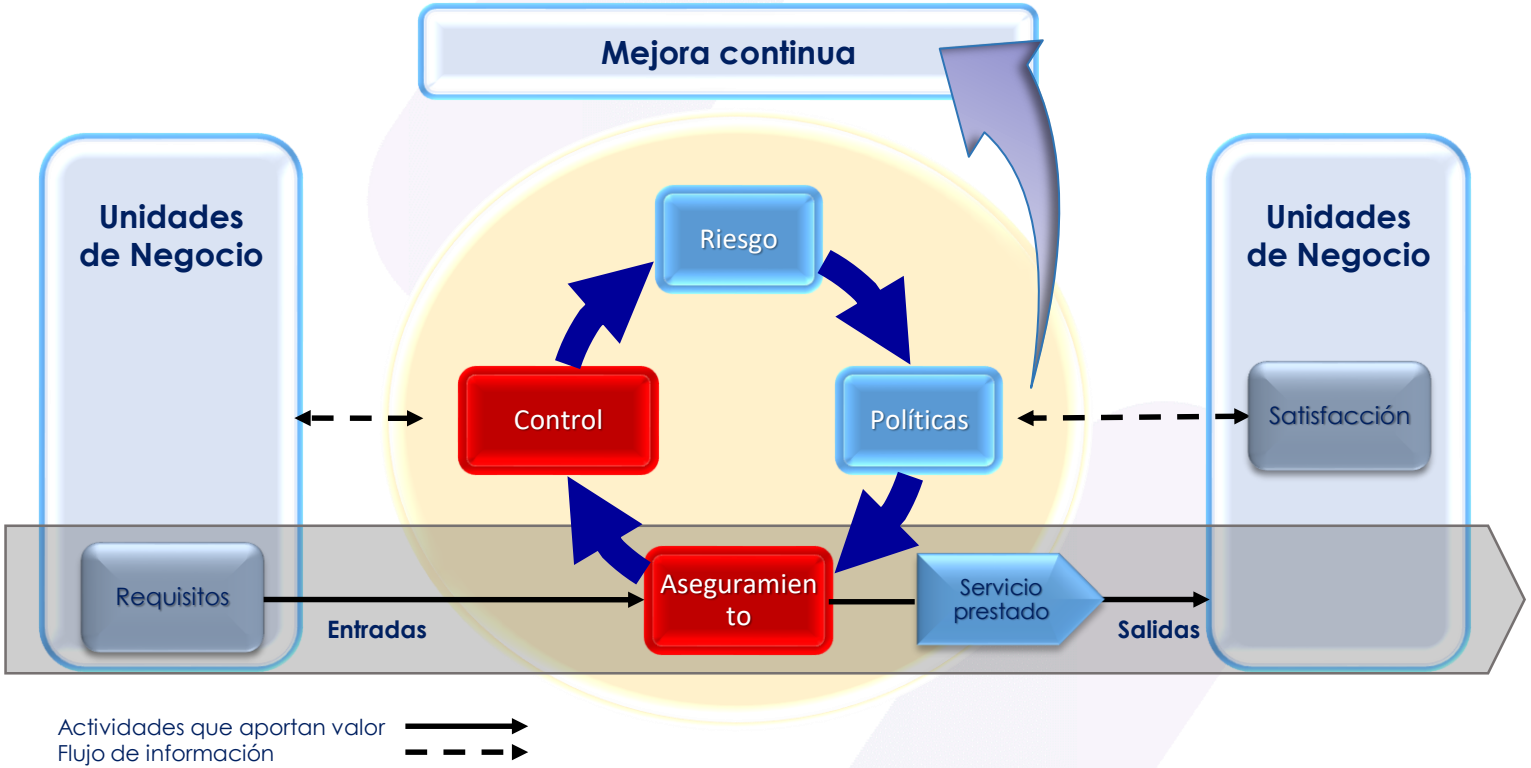
Modelo de seguridad tradicional

Lo importante y necesario para mitigar el fraude:
Gobierno y estrategia

Modelo de Seguridad Integral
Propuesta de enfoque por procesos

Lo importante y necesario para mitigar el fraude:
Gobierno y estrategia

De la función al proceso



Fuente. ISO 900

Agenda

I. **Lo importante y necesario para mitigar el fraude:**

Política/Gobierno y Estrategia/ **Modelo de Gestión**/Estructura/Planes & Accountability

II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios trae?

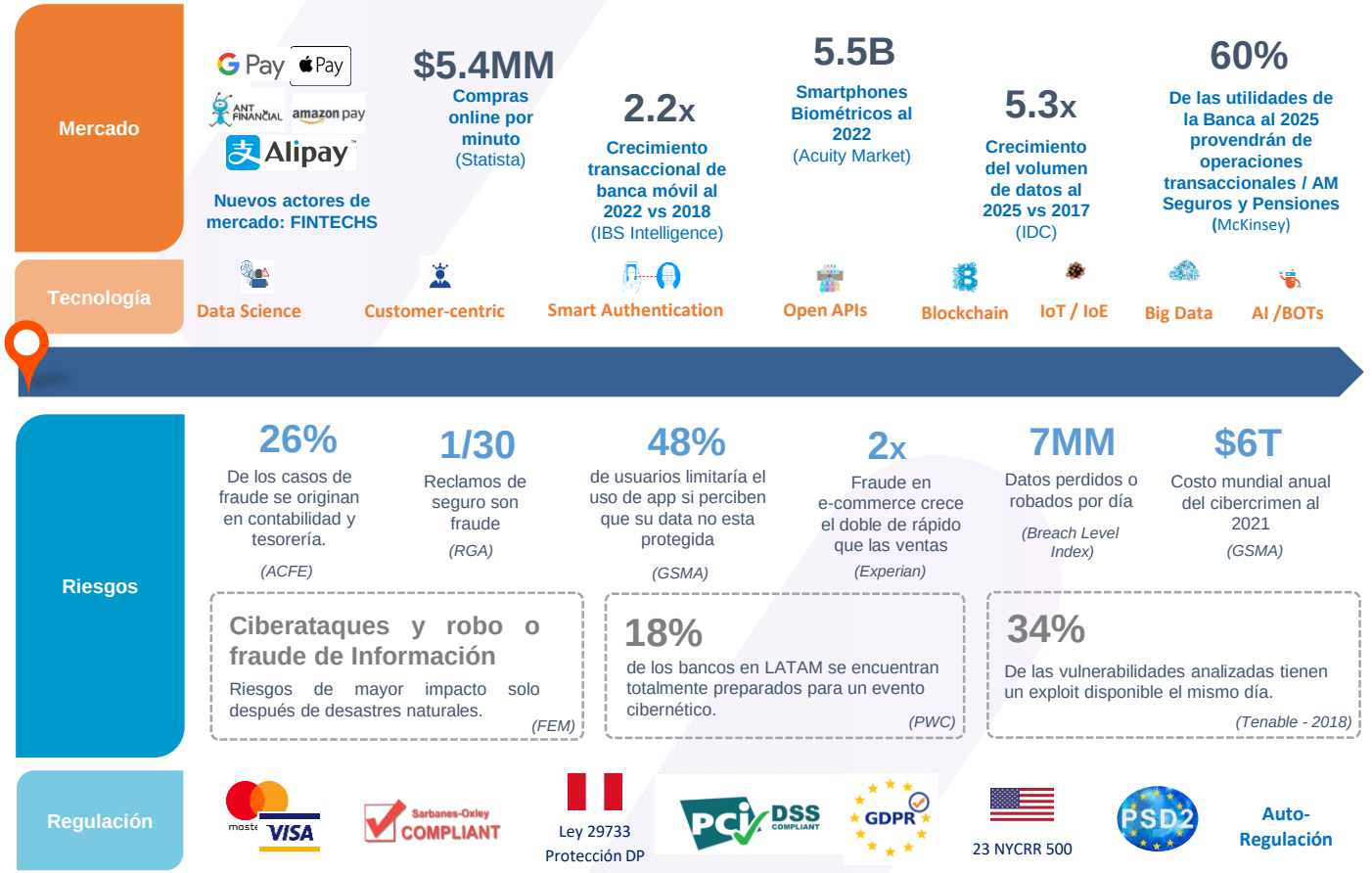
IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital.

V. Comentarios finales.

Lo importante y necesario para mitigar el fraude:

Modelo de Gestión

La evolución tecnológica cambió las necesidades de los clientes y consecuentemente los drivers del negocio. Con ello nuevas amenazas ponen en riesgo a las organizaciones.



Lo importante y necesario para mitigar el fraude:

Modelo de Gestión

Modelo de Seguridad y otros Marcos de Trabajo

	Prevenir	Detectar	Responder	Recuperar
Personas Estructura Organizacional Roles y Responsabilidades	Custodia	Administradores de sistemas / accesos	Equipos funcionales	Equipos de respuesta
Procesos Clasificación de Procesos y Recursos	Protocolos de Seguridad	Gestión de alertas	Plan de reacción inmediata	Procesos de contingencia
Información Inteligencia	Manejo de fuentes Análisis de data Identificación de riesgos	Diseño y aplicación de estrategias	Ejecución de protocolos	Continuidad operativa
Tecnología Uso de Dispositivos Tecnológicos	Arquitectura de Seguridad	Sistemas de seguridad	Centros de monitoreo	Equipos de contingencia
Cliente Productos y Servicios (incorpora Co-creación)	Educación, Autogestión según segmento	Monitoreo por Inteligencia comercial, redes neurales y tiempo real	Procesos automatizados en tiempo real e interacción con cliente	Plan de acción Multisector (comercial, operativo y soporte)

COSO

COBIT 5 AN ISACA® FRAMEWORK

ISO 27001

Lo importante y necesario para mitigar el fraude:

Modelo de Gestión

Gestión Integral de los Riesgos – MISB

Modelo de Governance y Encaje Estratégico

Visibilidad, mejora continua y control interno

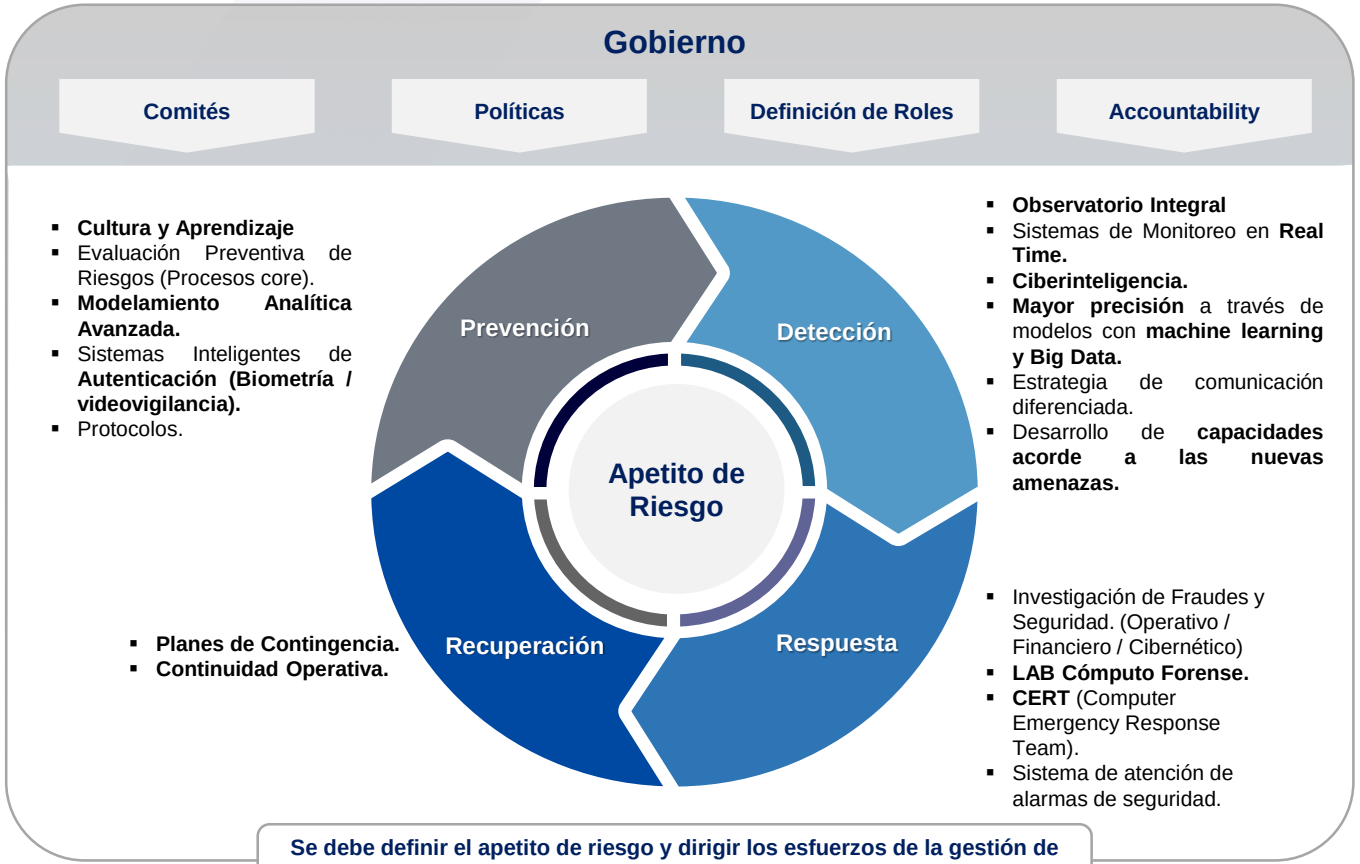
Evaluación y Aseguramiento de la normativa

Modelo de Monitoreo, seguimiento e investigación

Lo importante y necesario para mitigar el fraude:

Modelo de Gestión

Para poder estar preparados ante las nuevas amenazas del mercado es necesario contar con una gestión de riesgos de fraude y seguridad sobresaliente enmarcada en un esquema de gobierno eficaz



Agenda

I. **Lo importante y necesario para mitigar el fraude:**

Política/Gobierno y Estrategia/Modelo de Gestión/**Estructura**/Planes & Accountability

II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios trae?

IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital.

V. Comentarios finales.

Lo importante y necesario para mitigar el fraude:

Estructura

Modelo de Seguridad Bancario

Factores Claves

- **Capital humano**
- **Procesos estandarizados**
- **Soporte tecnológico**
- **Información (de calidad)**
- **Red de contactos**

Modelo Integral de Seguridad y Prevención

BCP

Lo importante y necesario para mitigar el fraude:

Estructura

Gestión Integral de los Riesgos – MISB

Lo importante y necesario para mitigar el fraude:

Estructura

Afinando el modelo de gestión ante incidentes

- Evaluación y valoración de riesgos de fraude.
- Elaboración, difusión y actualización de normas.

- Intervención de Auditoría Interna. Evalúa el riesgo materializado, procesos relacionados, mejoras requeridas y aspectos vinculados.

Prevención:
- Educación
- Inteligencia (casuística global)
- Protección a los sistemas y aplicativos bajo estándares de seguridad tecnológica.
- Medidas de protección a procesos, servicios y productos con riesgo de fraude

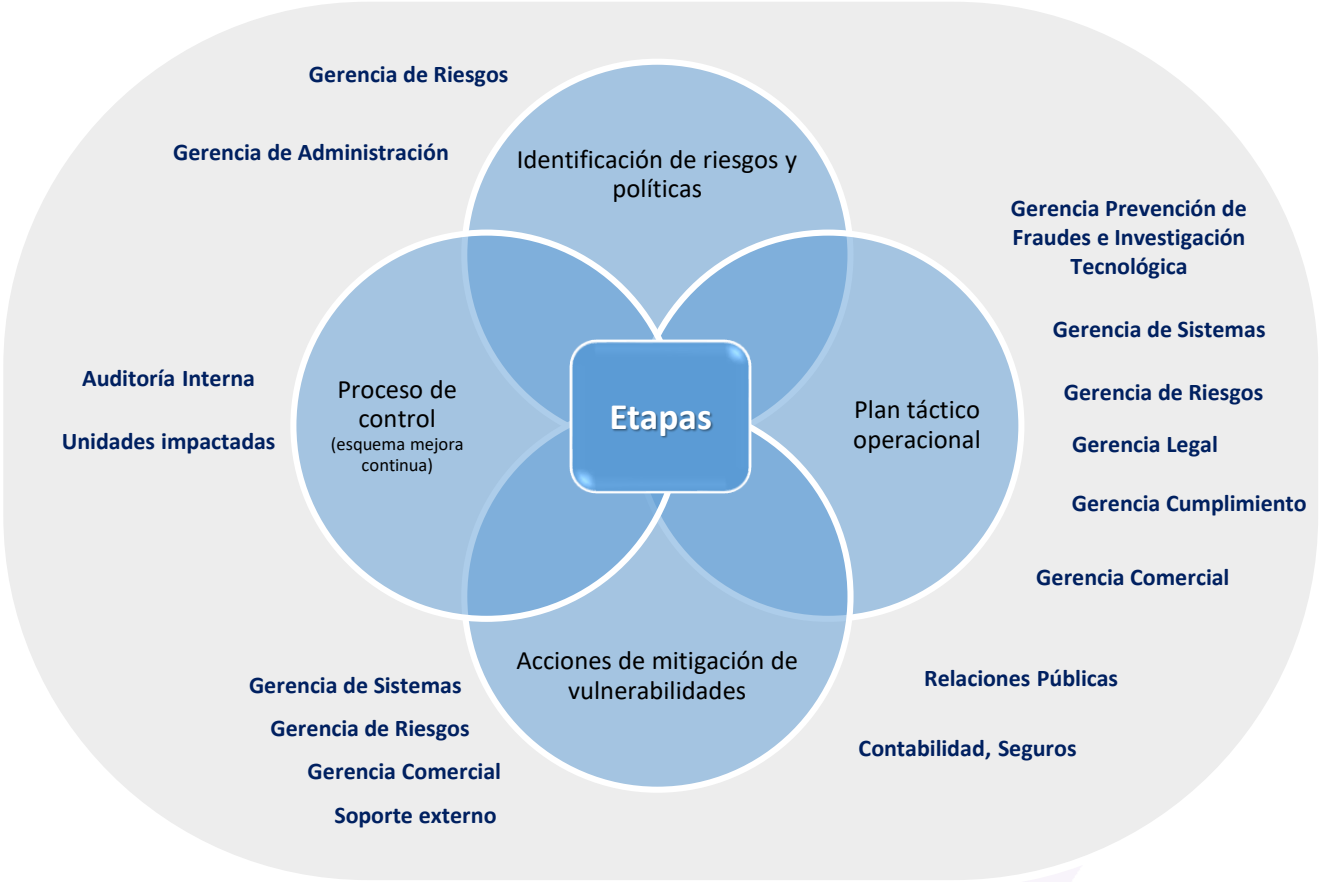
Detección:
- Monitoreo tecnológico
- Alertas tempranas
- Seguimiento reclamos / indicadores
- Reportes internos y externos

Respuesta:
- Protección del canal, producto, activo, sistema, aplicativos, otros.
- Acción contra amenaza (aspecto tecnológico, operativo, legal, otros)
- Alerta ARO, activación CC (por criticidad)
- Determinación del impacto operativo, contable y financiero.

- Medidas correctivas ante vulnerabilidad
- Pruebas de validación y monitoreo
- Soporte externo de ser necesario

Lo importante y necesario para mitigar el fraude:

Estructura



Agenda

I. **Lo importante y necesario para mitigar el fraude:**

Política/Gobierno y Estrategia/Modelo de Gestión/Estructura/**Planes & Accountability**

II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios trae?

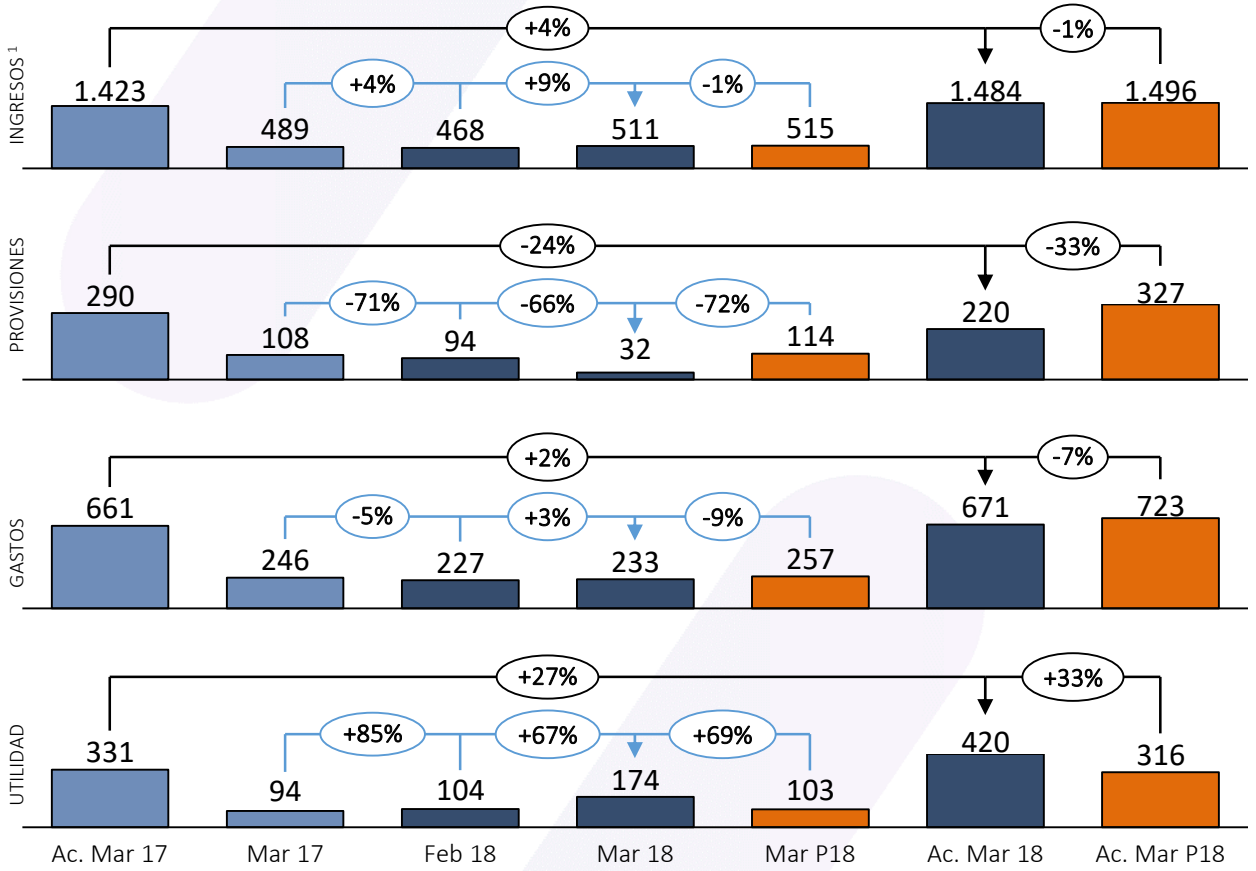
IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital.

V. Comentarios finales.

Lo importante y necesario para mitigar el fraude:

Planes & Accountability

Resultados Banca Minorista (S/ MM)



1/. Margen por Intermediación + GEB + ingresos no financieros

Lo importante y necesario para mitigar el fraude:

Planes & Accountability

26% De los casos de fraude, se originan en contabilidad y tesorería. *(ACFE)*

59% De crecimiento en fraude Ecommerce

82% del total de pérdidas es Fraude digital

55% Del fraude digital es por falla en sistema

23% Crecimiento prima por riesgos cibernéticos

$6T Costo mundial del cibercrimen *(Aite Group)*

17% Crecimiento fraude Ecommerce *(Aite Group)*

48% de usuarios limitaría el uso de app si perciben que su data no esta protegida *(GSMA)*

Big Data | Data Science | IoT | Open APIs | Blockchain | Smart Authentication | Customer Empowerment | Artificial Intelligence

2016 | 2017 | 2018 | 2019 | 2020 | 2021

Información

- Nivel 1: Analítica Avanzada
- Nivel 2: Modelo Cognitivo aplicado al monitoreo
- Modelo de detección de fraude crediticio en originación
- Mapas de riesgos de seguridad y fraude Credicorp

Tecnología

- Comunicación bidireccional y herramientas real time
- Sistemas de video inteligente integrado a SW de monitoreo
- Autenticación biométrica
- GRD – Mapas de posicionamiento real time

Procesos

- Ampliar alcance COSO Operaciones, Negocios y Staff
- Evaluación Riesgo de Fraude Financiero (Mercado Bursátil y Tesorería)
- Implementación del CERT (Computer Emergency Response Team)
- Tercerizaciones
- Monitoreo personal y proveedores (énfasis en Sistemas)
- Adecuación de estructura

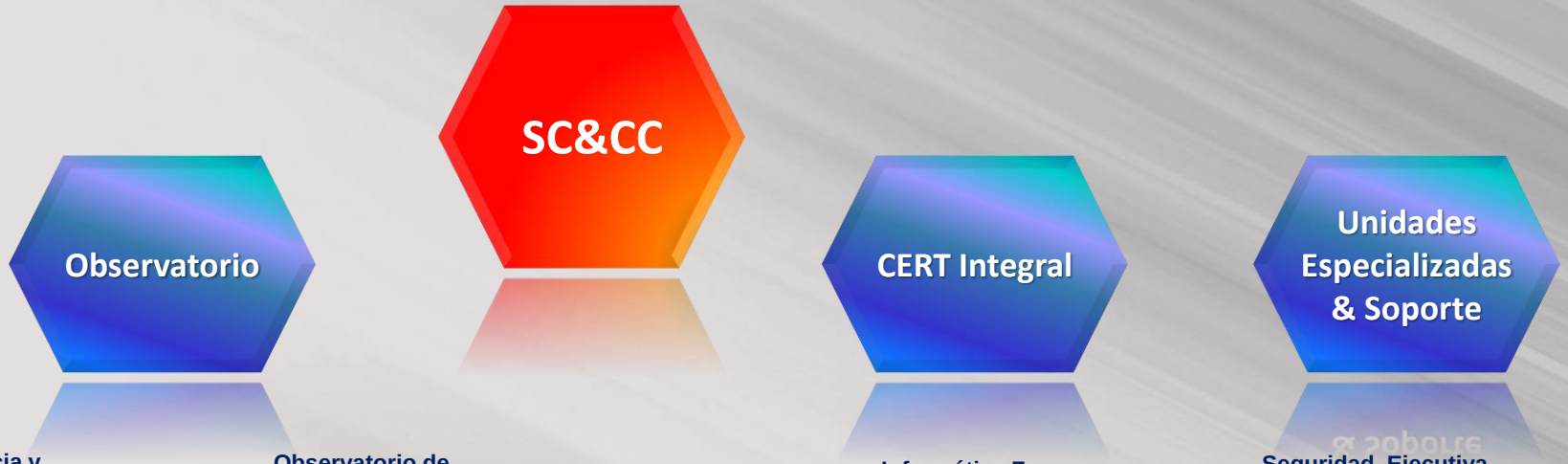
Personas

- E-Learning y training
- Adecuación de perfiles

Proy. estratégicos

Laboratorios

Modelo Booz – Allen – Hamilton



Inteligencia y Estrategia

E-Learning & training

Investigación y Desarrollo

Modelamiento analítica avanzada

Observatorio de Seguridad Integral Automatizado

- ✓Canales / Productos
- ✓Infraestructura
- ✓Data
- ✓Clientes
- ✓Colaboradores
- ✓Proveedores

Informática Forense

LAB y Computer Emergency Response Team

Incidencias de alta complejidad

Invest. Operativa / Finan.

Asuntos Legales

Seguridad Ejecutiva

GRD

Control Interno

COSO Principio 8

CoE Fraudes

Agenda

I. **Lo importante y necesario para mitigar el fraude:**

Política/Gobierno y Estrategia/ **Modelo de Gestión**/Estructura/Planes & Accountability

II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios trae?

IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital.

V. Comentarios finales.

II. Gestionando por riesgos

Consideraciones para la evaluación del riesgo de fraude por Componente COSO:

Ambiente de Control

- Hacer un compromiso organizacional con un programa de gestión de riesgos de fraude.
- Soporte a la gobernabilidad del riesgo de fraude.
- Establecer una política integral de gestión del riesgo de fraude.
- Establecer los roles y responsabilidades para la gobernabilidad del riesgo de fraude en toda la organización.
- Documentación del programa de gestión del riesgo de fraude.
- Comunicar la gestión del riesgo de fraude a todos los niveles de la organización.

II. Gestionando por riesgos

Consideraciones para la evaluación del riesgo de fraude por Componente COSO:

Evaluación de Riesgos

- Involucrar niveles apropiados de gerencia.
- Incluir niveles: entidad, subsidiaria, división, unidad operativa y nivel funcional
- Analizar factores internos y externos.
- Considerar varios tipos de fraude.
- Considerar específicamente la omisión de controles por parte de la gerencia.
- Estimar la probabilidad e impacto de los riesgos identificados.
- Valuar al personal o unidades involucradas en todos los aspectos del triángulo de fraude.
- Identificar actividades existentes de control de fraude y evaluar su efectividad.
- Determinar cómo responder a riesgos.
- Utilizar técnicas de data analytics para la evaluación de riesgos de fraude y para los planes de respuesta.
- Realizar evaluaciones periódicas: programadas y evaluar cambios en riesgos de fraude.
- Documentar la evaluación de riesgos.

II. Gestionando por riesgos

Actividades de Control de Fraude

- Investigaciones de fraude y protocolos de respuesta
- Desarrollo de las investigaciones
- Comunicando los resultados de la investigación
- Tomando las acciones correctivas
- Evaluación del desempeño de la investigación

Administración del Monitoreo del Riesgo de Fraude

- Considerar un mix de evaluaciones continuas y programadas.
- Considerar factores para establecer el alcance y frecuencia de evaluaciones.
- Establecer criterios apropiados de medición.
- Considerar esquemas de fraude conocidos y nuevos casos de fraude.
- Evaluar, comunicar y remediar deficiencias.

II. Gestionando por riesgos

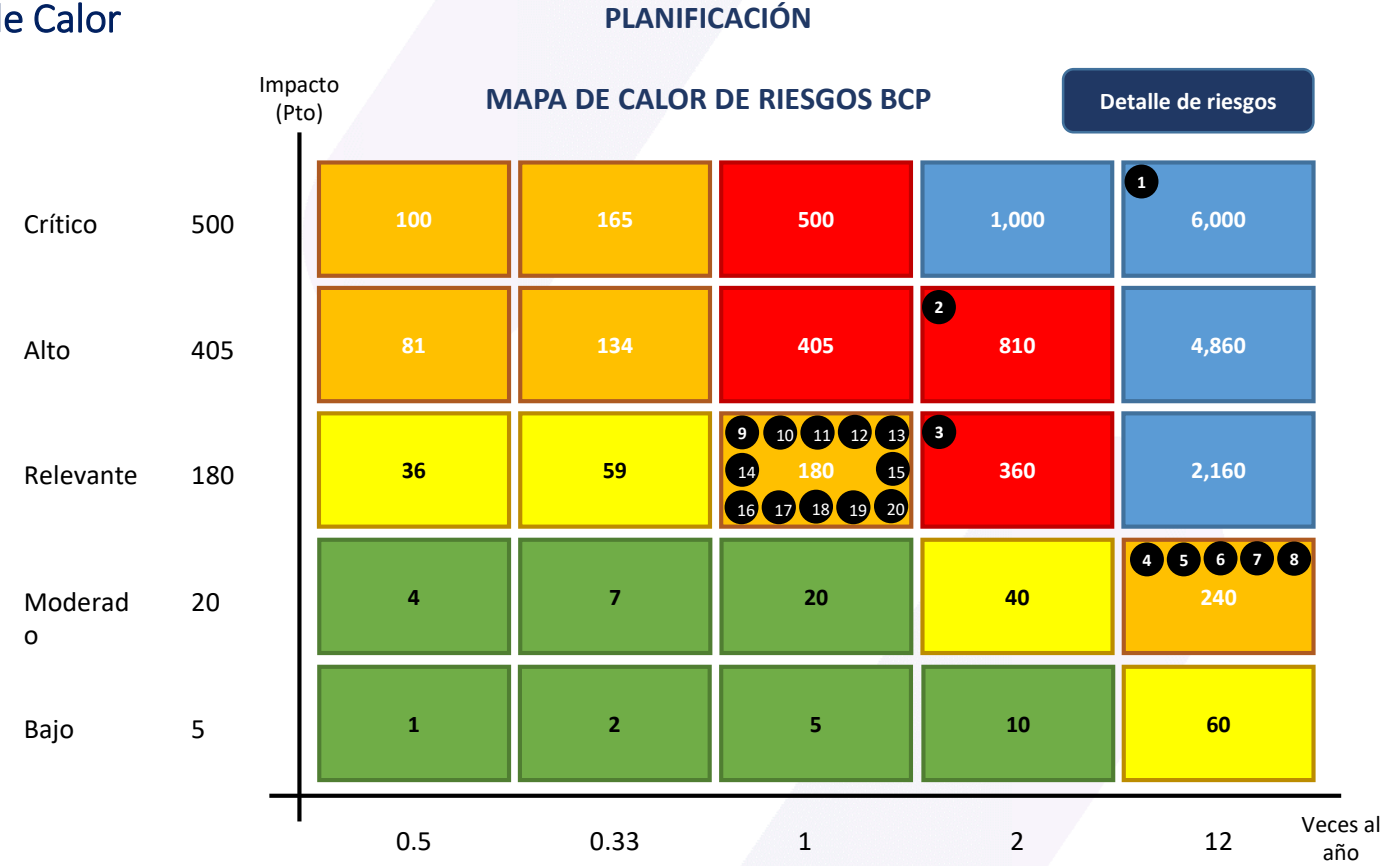
Consideraciones para la evaluación del riesgo de fraude por Componente COSO:

Información y comunicación

- Promover la disuasión del fraude mediante actividades de control preventivo y detectivo.
- Integración con la evaluación de riesgos de fraude.
- Considerando los factores específicos de la organización y los procesos de negocios relevantes.
- Considerando la aplicación de las actividades de control a los diferentes niveles de la organización.
- Utilizando una combinación de actividades de control de fraude.
- Considerando la anulación de los controles.
- Uso de procedimientos proactivos de análisis de datos.
- Desarrollo de actividades de control a través de políticas y procedimientos.

II. Gestionando por riesgos

Mapa de Calor



Queremos modificar la forma de trabajo para que se realice todo el proceso en línea; de esta forma, se revisa el proceso punta a punta de cada riesgo

1.- Identificación del Riesgo:

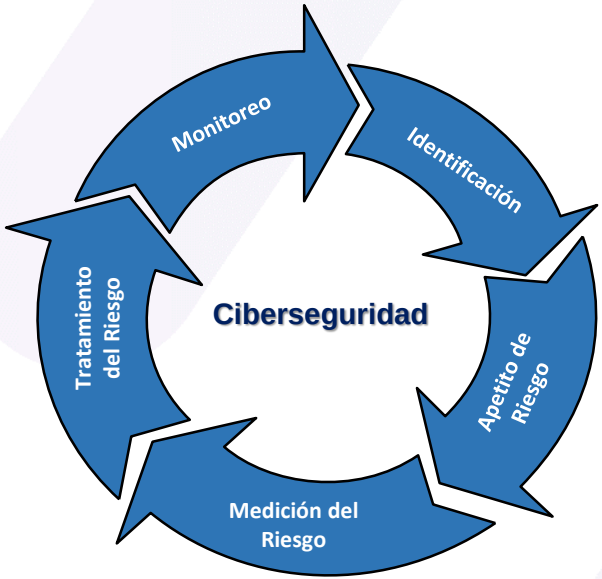
- **Definir una taxonomía común** → lenguaje sencillo para los gestores y mesas.
- Identificar los **top risks.**
- Identificar **activos expuestos, controles existentes, suficiencia de controles y vulnerabilidades**.
- Definir **principales escenarios de riesgo a evaluar.**

2.- Apetito de Riesgo:

- ¿Métricas operativas son **suficientes** para medir los **top risks**?.
- Complementar con **métricas cualitativas**.
- **¿Cuál es el target de riesgo para los principales escenarios de riesgo identificados en el punto1?**
- Definir **gobierno** para incumplimiento y para mantenimiento de métricas.

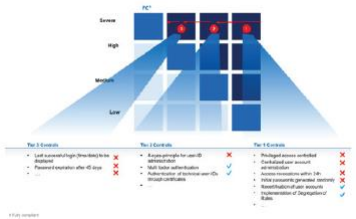
3.- Medición del Riesgo:

- **Evaluar el impacto que tienen los distintos escenarios de riesgo identificados** → en términos de probabilidad e impacto.
- Identificar principales mitigantes para cada escenario que **nos llevaría a niveles dentro de apetito.**



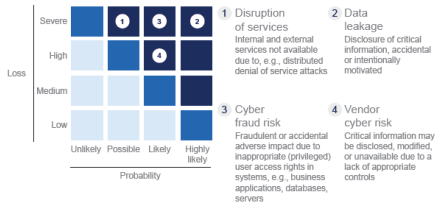
4.- Tratamiento del Riesgo :

- **Plan de mitigación de los riesgos priorizados.**
- **¿El riesgo residual es aceptable vs el apetito de riesgo?.**
- **Mostrar el plan de trabajo para reducir riesgo residual**



5.- Monitoreo:

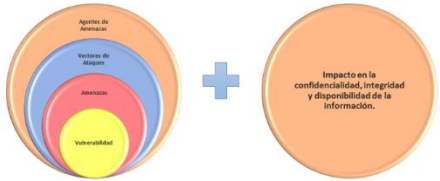
- Seguimiento a los planes de remediación para regresar a apetito a los riesgos identificados.
- Medición consolidada top – down.
- **Definir necesidades de data analytics.**
- **Desarrollo de herramienta de soporte que permita almacenar la información y generar reportes.**



Objetivos de cada etapa del proceso:

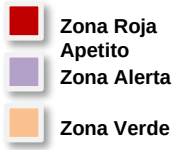
Identificación

- Definir principales riesgos → top risks.
- Definir taxonomía de ciberseguridad con lenguaje simple para los usuarios (mesas y gestores).
- Identificar principales activos críticos, vulnerabilidades y posibles eventos → escenarios de riesgo a priorizar.
- Mapeo de controles y respectivo impacto en la vulnerabilidad.



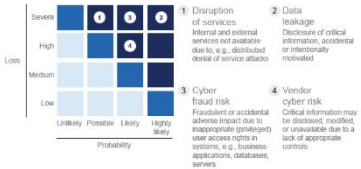
Apetito de Riesgo

- Complementar Tablero de Apetito Operativo con métricas cualitativas.
- Complementar tablero operativo → ¿métricas actuales incluyen los top risks identificados?.
- ¿Cuál es el nivel de riesgo que quisiera tener? → Target de los escenarios de riesgo (cualitativo o cuantitativo).
- Definir gobierno, responsables para los distintos tipos de riesgo.



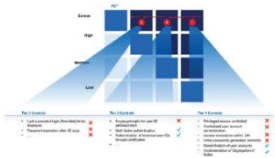
Medición del Riesgo

- Medición de los principales escenarios de riesgo priorizados.
- Situación actual y riesgo residual→ considerando controles existentes.
- Identificar principales mitigantes para cada escenario
- Considerando la medición se identifican los principales escenarios que estén fuera de apetito



Tratamiento del Riesgo

- Armar plan de trabajo para mitigar principales escenarios de riesgo.
  Concluir con etapas de plan de acción:
  - Quick-wins
  - Plan de Corto/Mediano Plazo
  - Plan de Largo Plazo → decisiones más estructurales.



Monitoreo

- Definir frecuencia del monitoreo
- Definir reportes para cada nivel de reportes → detalle de confidencialidad a compartir entre las distintas listas de distribución.
- Reporte top-down del seguimiento de las iniciativas de remediación y planes de acción.
- Identificar necesidades de analytics.
- Desarrollar herramienta de soporte que permita almacenar los eventos y automatizar reportes.

Agenda

I. **Lo importante y necesario para mitigar el fraude:**

Política/Gobierno y Estrategia/ **Modelo de Gestión**/Estructura/Planes & Accountability

II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios trae?

IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital.

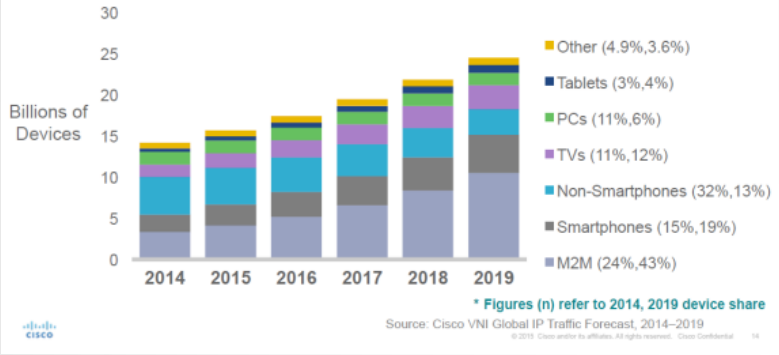
V. Comentarios finales.

III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

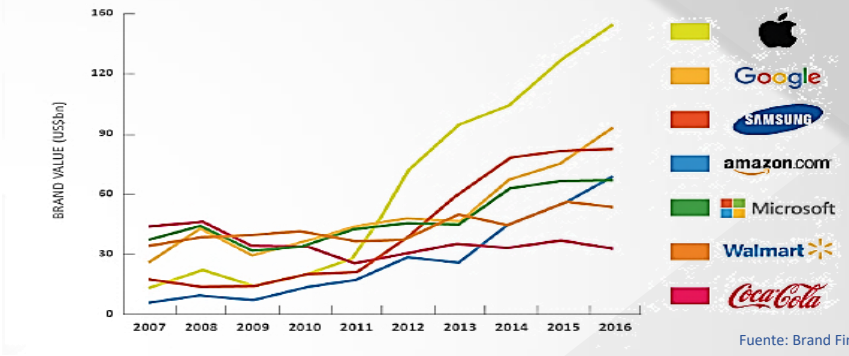
Evolución del negocio y TICs en la experiencia digital del cliente

Global connected device growth by type

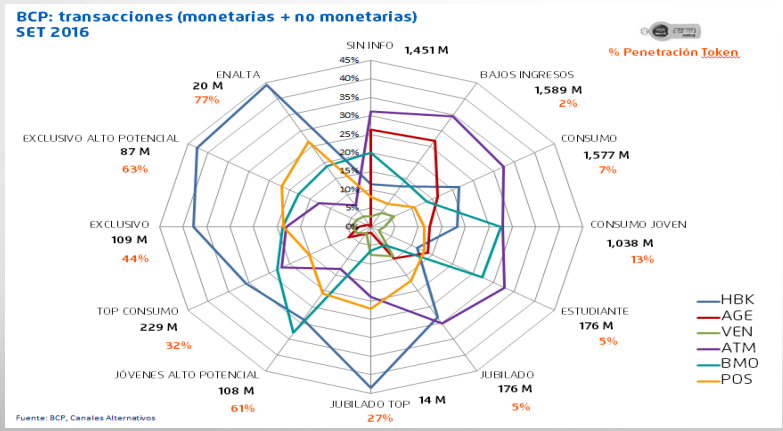
By 2019, M2M connections will be more than 40% of total connections

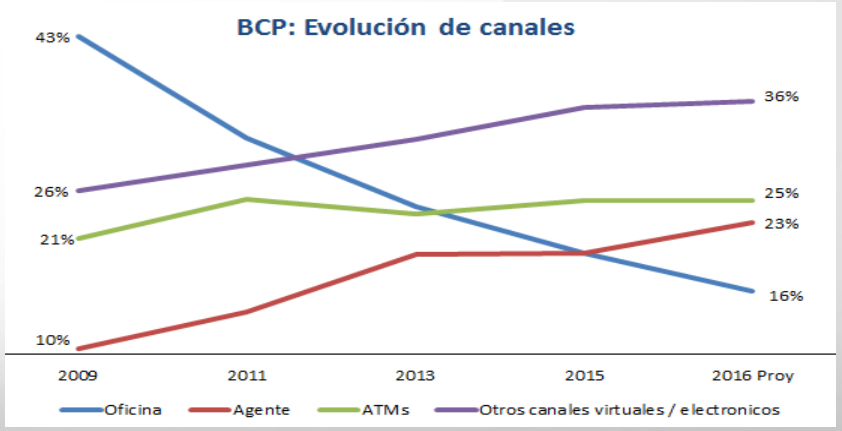


Marcas mas valiosas del mundo



Fuente: Brand Finance, 2016





Fuente: Área Canales Alternativos BCP

III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

Modalidades de fraude en la gestión de cajeros automáticos

- Ausencia deliberada del proceso de cuadre diario.
- Castigo injustificado de diferencias no explicadas.
- Incumplimiento deliberado del control dual en el proceso de abastecimiento.

Modalidades de fraude en el Proceso de Compras

- Ausencia deliberada de un manual de funciones o evitar documentar los procesos para diluir responsabilidades. (Desorganización organizada)
- Selección inadecuada de los proveedores (amigos de los defraudadores).
- Pedidos a proveedores no autorizados
- Pedidos innecesarios por fraude
- Pedidos a precios diferentes a los pactados o superiores al mercado
- Aceptación de cantidades superiores o inferiores al pedido en beneficio de colaboradores o terceros.
- Contabilización de facturas incorrectas por fraude
- Cobro duplicado de facturas
- Falsificación de órdenes de compra o cotizaciones.

Modalidades de fraude en el proceso crediticio

- Suplantación de personas o entidades.
- Falsificación de documentos de sustento de la solicitud crediticia.
- Concentración en un solo tasador de garantías.
- Sobreestimación de las garantías.

III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

Oportunidades para cometer fraude

- Debilidad o inexistencia de controles, así como falta de validación o monitoreo en los procesos.
- Ausencia de normas , indefinición en los roles y responsabilidades de personal clave.
- Historial conocido de incumplimiento de la normativa sobre valores y otras disposiciones legales o reglamentarias.
- Registros contables desactualizados, sin análisis ni conciliaciones.
- Partidas antiguas pendientes, sin análisis ni adopción de medidas para regularizarlas.
- Registro de gastos sin control presupuestal.
- Observaciones de auditoría de alto riesgo sin seguimiento.

Actitudes y racionalizaciones

- Tolerancia respecto a sustracciones menores.
- Cambios en el comportamiento del estilo de vida.
- Comportamiento del empleado que muestre su disgusto o insatisfacción con la entidad o el trato que recibe (“Falta de reconocimiento a mi esfuerzo”, “Mi salario no justifica el trabajo que realizo”, “son injustos en las premiaciones”, etc.).

III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

Información financiera fraudulenta:

- Contabilidad creativa.
- Incremento indebido de ingresos.
- Omisión de registros de gastos.
- Ajustes de las diferencias de ingresos y gastos en periodos incorrectos.
- Valuaciones inadecuadas (sobrevaloración de activos).
- Cálculos incorrectos en las Provisiones.
- Activación de gastos.

Información NO financiera fraudulenta:

- Reporte de ventas ficticias.
- Pérdidas de activos no reportados a la Alta Dirección.
- Cálculos incorrectos para la determinación de indicadores de desempeño.
- Reporte de falsos recuperos.
- Información parcial de las pérdidas operativas.

III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

Corrupción:

- Ausencia de políticas sobre conflicto de intereses.
- Falta de monitoreo al cumplimiento de los Códigos de ética y conducta.
- Falta de una políticas corporativa de regalos y atenciones.
- Aceptación de comisiones indebidas para la contratación de bienes y servicios a proveedores.
- Recepción de prebendas de funcionarios de crédito por el otorganiento de facilidades crediticias.
- Concertación en la selección de proveedores.
- Entrega indebida a terceros de información reservada en los concursos de adjudicación de bienes y servicios.

III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

Evolución de las amenazas Cibernéticas

	2014	2015	2016	2017	2018
1ro	Disparidad de ingresos	Conflictos entre estados con consecuencias regionales	Migraciones involuntarias a gran escala	Eventos de clima extremo	Eventos de clima extremo
2do	Eventos de clima extremo	Eventos de clima extremo	Eventos de clima extremo	Migraciones involuntarias a gran escala	Desastres naturales
3ro	Desempleo y subempleo	Falla del gobierno nacional	Falla de mitigación o adaptación al cambio climático	Catástrofes naturales mayores	Ciber-ataques
4to	Cambio climático	Colapso o crisis estatal	Falla del gobierno nacional	Ataque terrorista de escala mayor	Robo o fraude de información
5to	Ciber-ataques	Alto desempleo estructural o subempleo	Catástrofes naturales mayores	Incidente masivo de robo/fraude de información	Falla de mitigación o adaptación al cambio climático

Económico Medioambiental Geopolítico Social Tecnológico

Fuente: World Economic Forum, Global Risk Report 2018

CIBERESPACIO

Surface Web

10% del contenido web

980MM de sitios webs

Contenido accesible a personas comunes. Todos los sitios web son indexados por los motores de búsqueda para su fácil acceso

TARINGA!

MEGA

4chan

µTorrent

The Pirate Bay

vni

Tor

ANONYMOUS

The Hidden Wiki

bitcoin

Venta de drogas

Venta de armas

Alquiler de Botnets (pc zoombies)

Trata de personas

Venta de ToolKits para Hacking

Contrato de sicarios

Pornografía ilegal Pedofilia

Comunicación entre terroristas

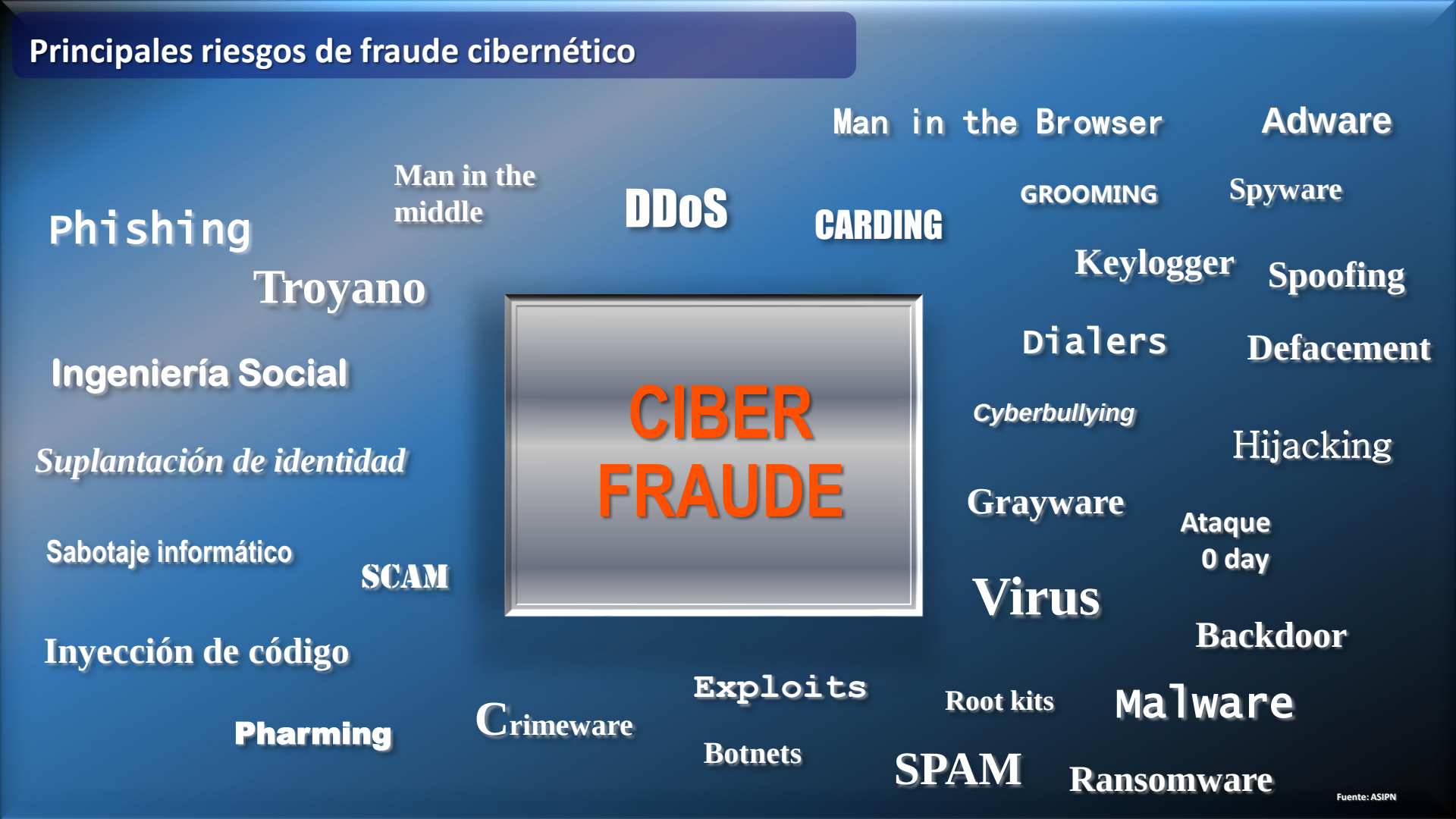
Documentación clasificada

Venta de dispositivos para fraude

Deep Web

90% del contenido web

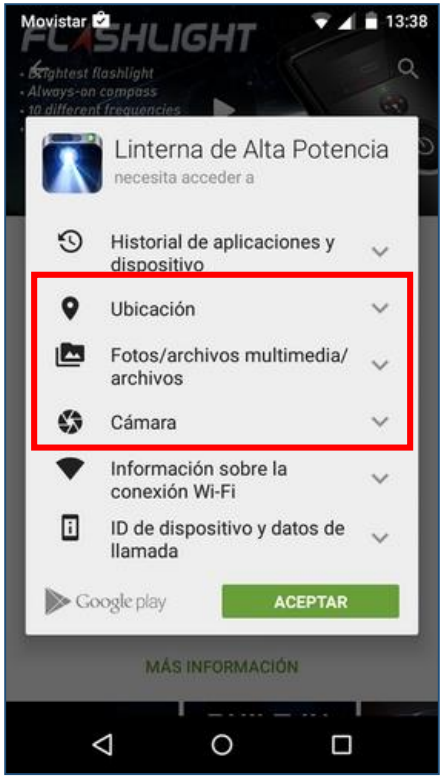
Principales riesgos de fraude cibernético

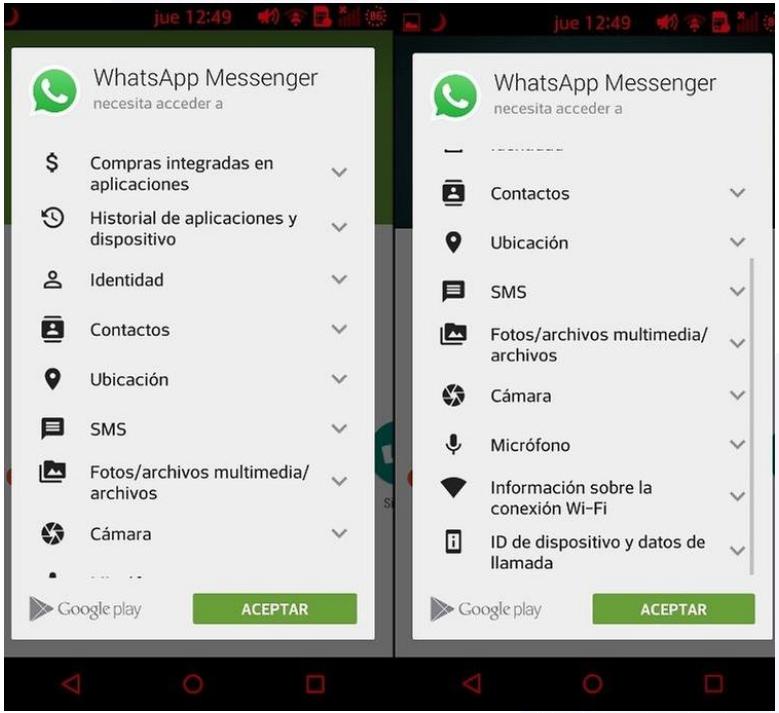


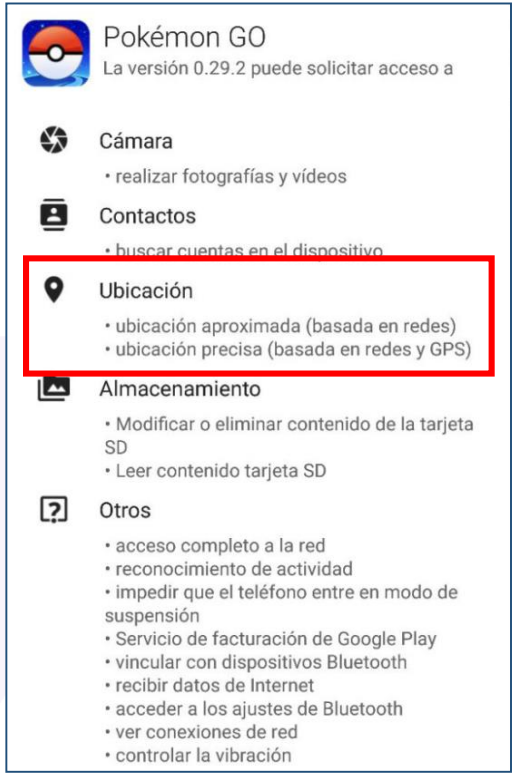
III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

III. Principales tipologías de fraude y lecciones aprendidas: ¿Qué escenarios trae?

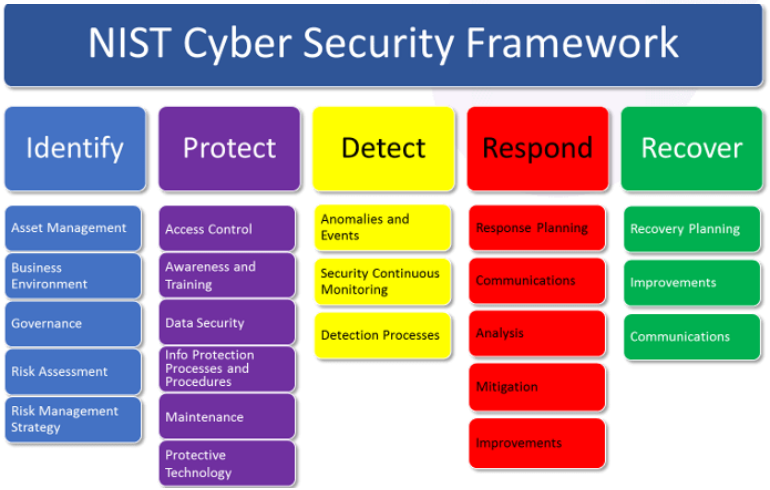
¿Cómo se facilita el acceso a tu información?

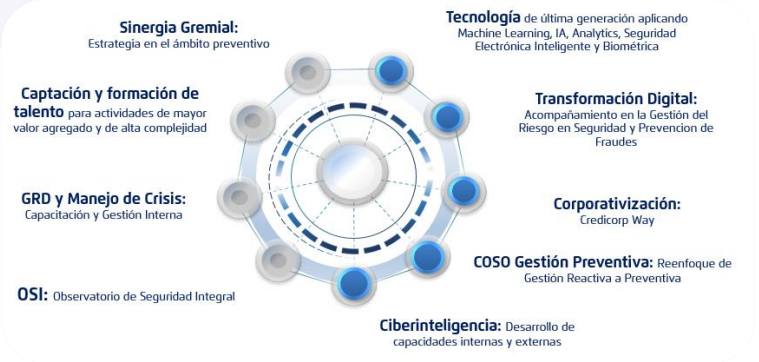


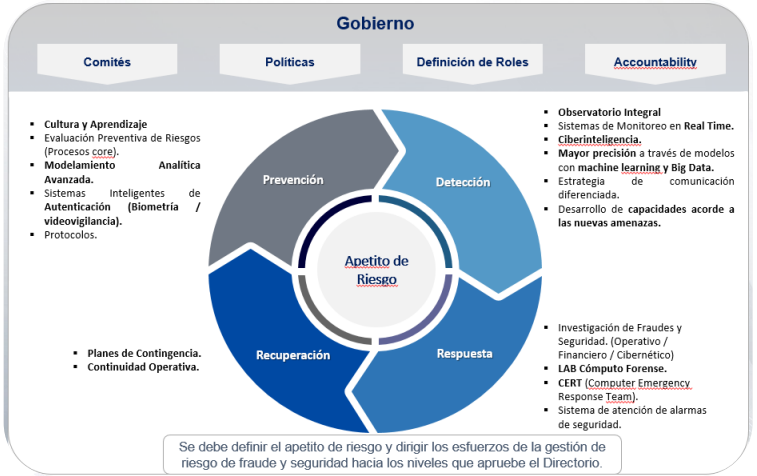




Lo importante y necesario para mitigar el fraude:
Modelo de Seguridad y otros Marcos de Trabajo







Esquema de un Ciberataque: Complejidad para su detección

Definición y planificación del ataque
- Investigación y recolección de información.
- Selección de objetivo

Reconocimiento externo
- Acciones para la identificación de vectores de acceso
- Identificación de vulnerabilidades

Compromiso inicial
- Explotación de vulnerabilidades
- Primer acceso a activo de la empresa

Acceso interno
- Acceso privilegiado al sistema y visibilidad de la red interna

Elevación de privilegios y persistencia
- Obtención de privilegios elevados en la infraestructura

Ejecución de acciones
- Movimiento lateral
- Acceso a activos críticos e información sensible
- Selección, recolección y extracción de información

Permanencia en los sistemas sin ser detectado y eliminación de rastros.

Manejo de Crisis:

Primeros síntomas no detectados

Detección de la amenaza y tardía activación de Comité Crisis (juicio experto)

Proceso de ordenamiento y mejora del diagnóstico. **Ataque en desarrollo**

Apoyo de capacidades internas con capacidades externas

Estrategia de comunicación interna/externa. Monitoreo permanente sobre medidas e impacto

Proceso de remediación a mediano plazo

Nuevo enfoque

Inicio de la amenaza / ataque

Etapa de negación

Dificultad para llevar la estrategia/protocolo a la práctica

Exploración de medidas de **contención**. Ejercicio prueba error

Ejecución de soluciones parciales a sobrecostos

Identificación de limitaciones para análisis forense. Se opera sólo en base a hipótesis.

Mejora en la planificación e inversión

compromiso | **DIA 0** | **DIA 1**

Fuente: J. Marangunich R.

Al terminar los sprints entregamos un producto mínimo viable (MVP) de gran valor para nuestros

Clientes

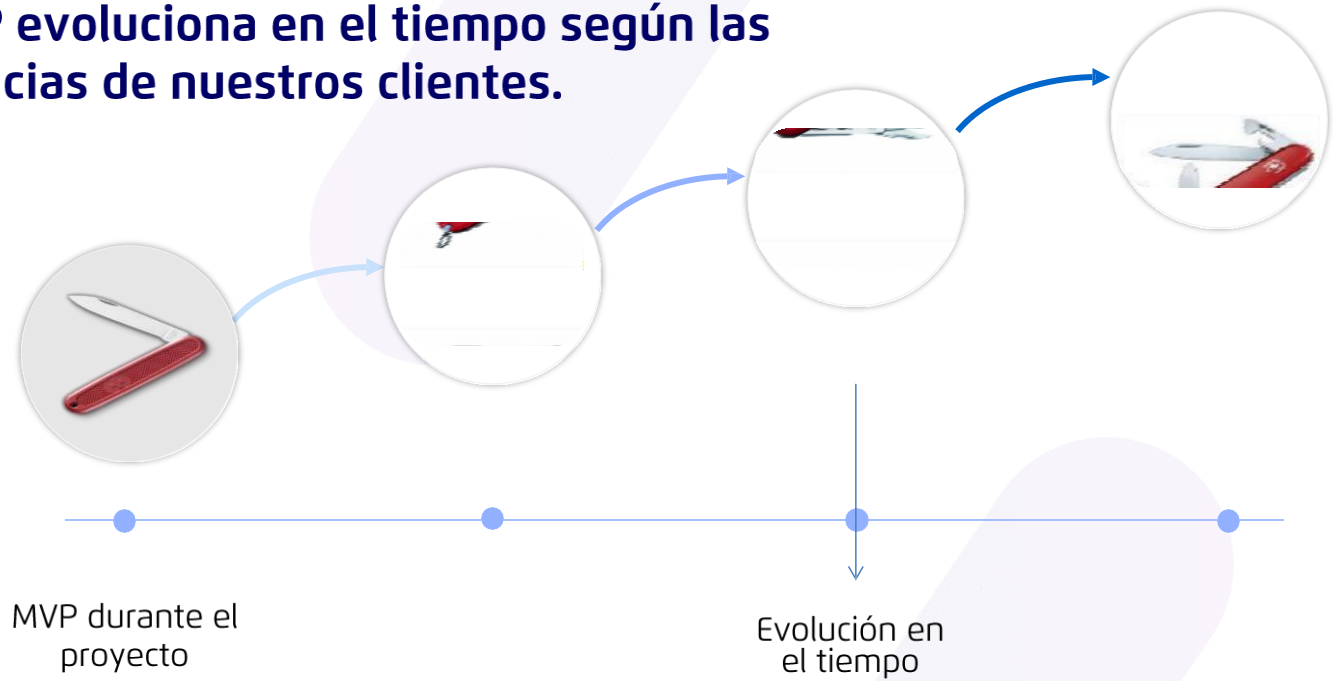
MVP

✓

Not MVP

✗

El MVP evoluciona en el tiempo según las exigencias de nuestros clientes.



Estadísticas
Perú

POBLACIÓN TOTAL DEL PAÍS	30.973.148
Abonos a teléfonos celulares	31.666.244
Personas con acceso a Internet	12.389.259

Penetración de Internet

40%

Educación

Disponibilidad nacional de la educación y formación cibernéticas

- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética

- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas

- Capacitación de empleados en seguridad cibernética

Gobernanza corporativa, conocimiento y normas

- Comprensión de la seguridad cibernética por parte de empresas privadas y estatales

Cultura y sociedad

Mentalidad de seguridad cibernética

- En el gobierno
- En el sector privado
- En la sociedad

Conciencia de seguridad cibernética

- Sensibilización

Confianza en el uso de Internet

- En los servicios en línea
- En el gobierno electrónico
- En el comercio electrónico

Privacidad en línea

- Normas de privacidad
- Privacidad del empleado

BID
Banco Interamericano de Desarrollo

Fuente: Informe de Ciber-seguridad 2016, OEA

14-15
NOVIEMBRE

HOTEL LAS AMÉRICAS
CARTAGENA DE INDIAS,
COLOMBIA.

18°CONGRESO DE RIESGO FINANCIERO

MEJORES PRÁCTICAS EN
UN CONTEXTO DESAFIANTE

Transformación digital de la seguridad: Pasado, presente y futuro

Agenda

I. **Lo importante y necesario para mitigar el fraude:**

Política/Gobierno y Estrategia/ **Modelo de Gestión**/Estructura/Planes & Accountability

II. **Gestionando por riesgos:** Riesgo Operativo, Crédito, Financiero, Reputacional, otros.

III. **Principales tipologías de fraude y lecciones aprendidas:** ¿Qué escenarios trae?

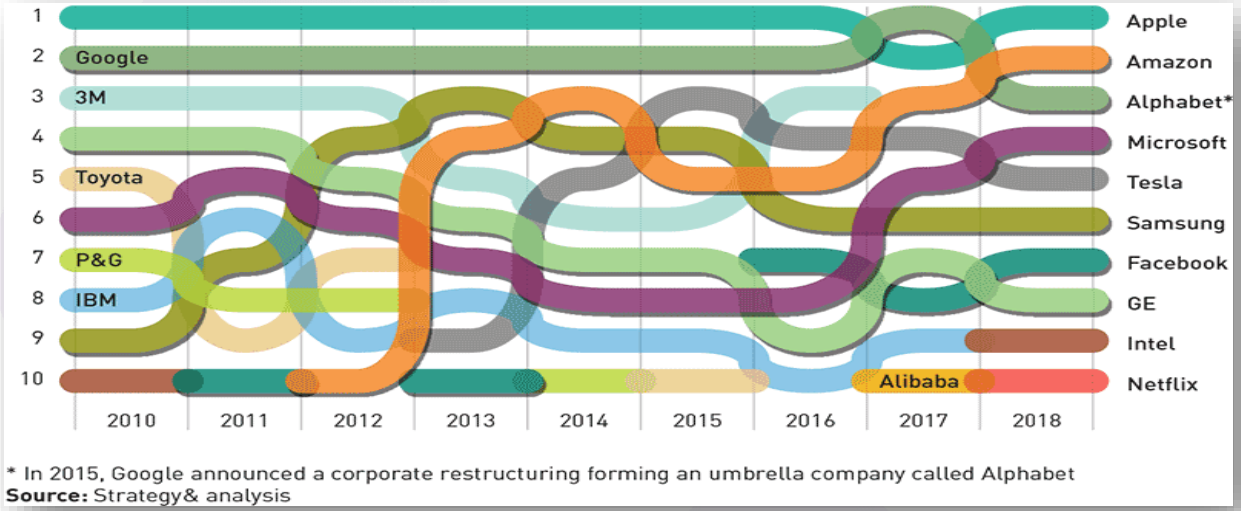
IV. **¿Qué viene?** Gestionando la incertidumbre en la transformación digital

V. Comentarios finales.

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

Empresas Líderes en Innovación y sus Características

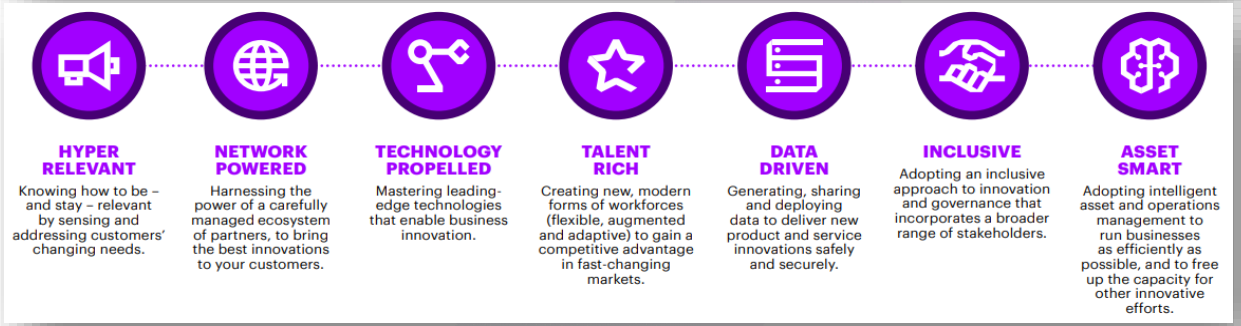
El LIDERAZGO no es permanente



* In 2015, Google announced a corporate restructuring forming an umbrella company called Alphabet

Source: Strategy& analysis

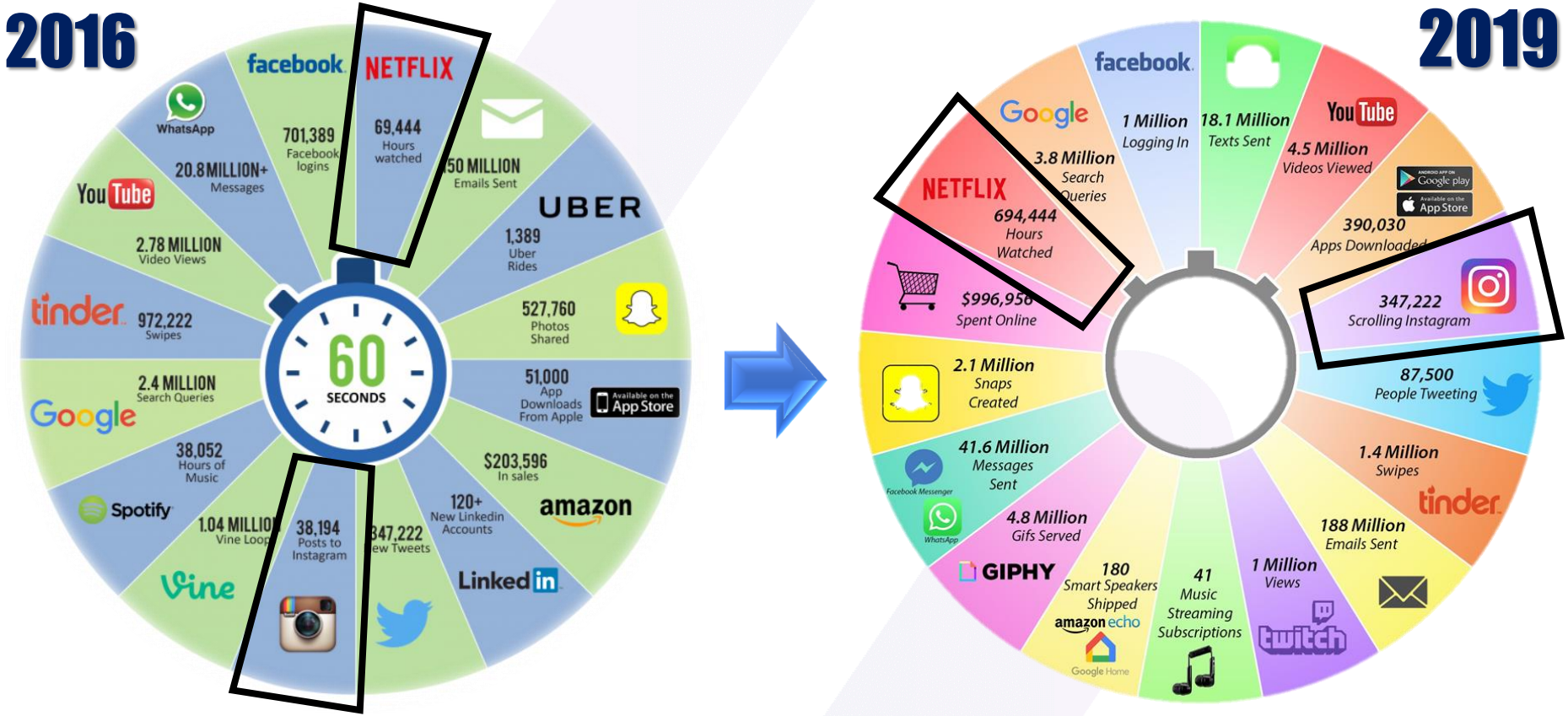
Condiciones para ser empresas líder y referente en el mercado



Fuente: Accenture. Unlocking Innovation Investment Value

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

Internet en un minuto y su crecimiento exponencial



IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

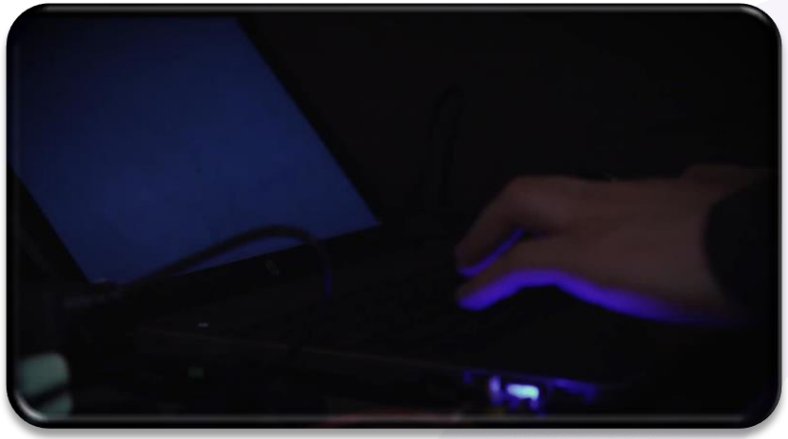
Factores del riesgo de seguridad en el ecosistema de innovación: Gaps entre líderes y seguidores

***Referencias: Cybersecurity Assessment Tool**
FFIEC. Cybersecurity Maturity.
FFIEC. Inherent Risk Profile.

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

Factores del riesgo de seguridad en el ecosistema de innovación: Gaps entre líderes y seguidores

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital



IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

¿Quién se sube al tren de la innovación?

Tecnologías

Negocios

Seguridad

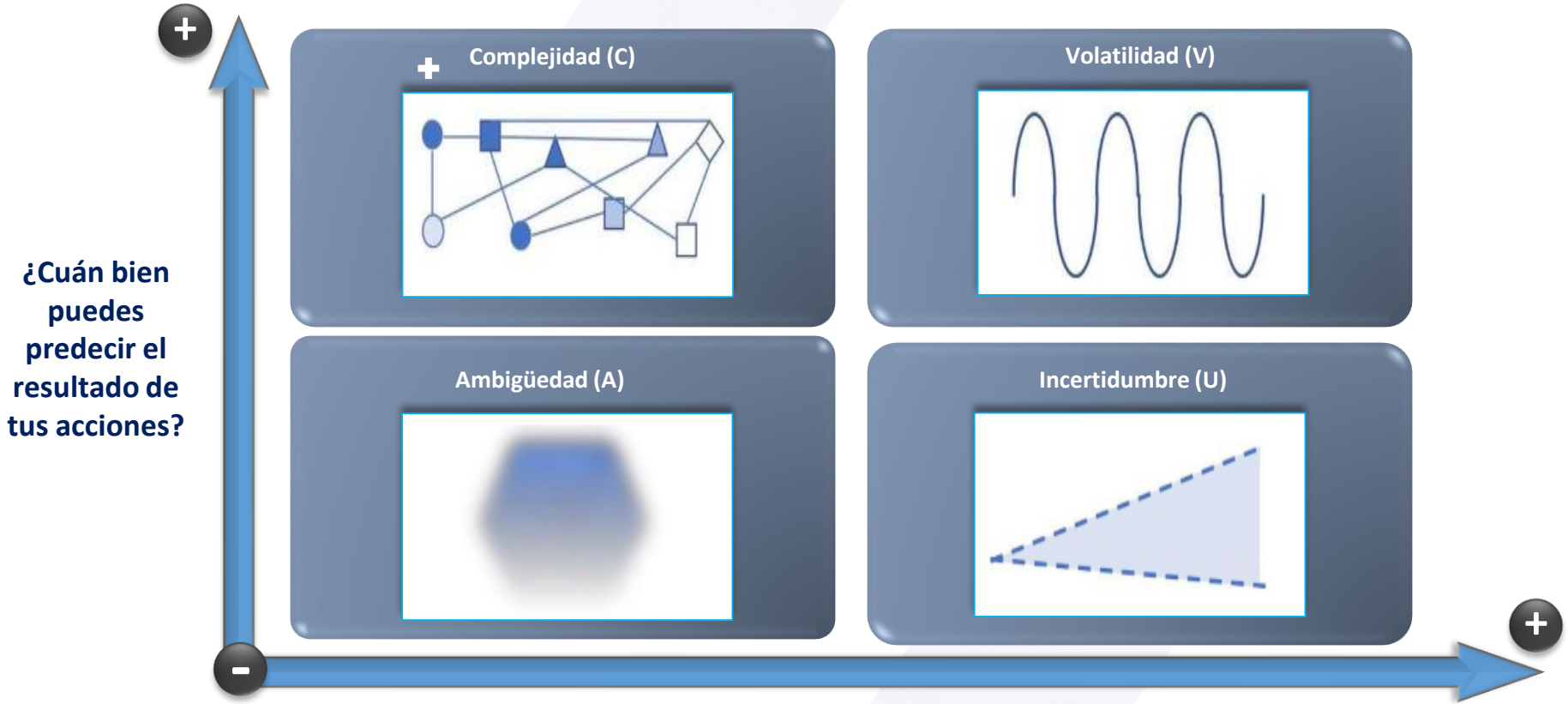

Hi, how can I help?
Make me a haircut appointment on Tuesday morning anytime between 10 and 12.
No problem. I'll make you an appointment and update you soon.


sci


Bloomberg

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

El constante cambio nos lleva a interactuar en un entorno VUCA



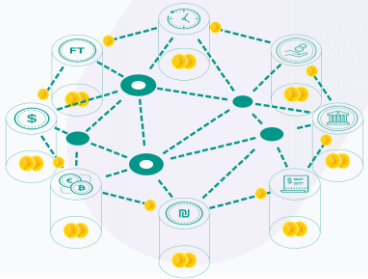
Fuente: Adaptado de Harvard Business Review y Forbes.

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

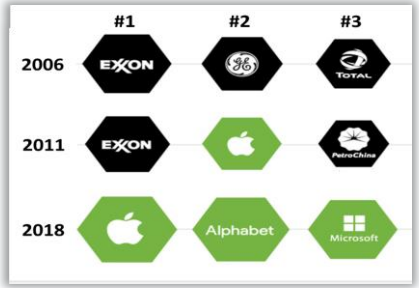
El constante cambio nos lleva a interactuar en un entorno VUCA

¿Cuán bien puedes predecir el resultado de tus acciones?

Complejidad (C)



Volatilidad (V)



Ambigüedad (A)

Google Pay · Apple Pay · ANT FINANCIAL · amazon pay · Alipay

Nuevos actores: FINTECHS

Incertidumbre (U)

¿Cuánto conoces de la situación/contexto?

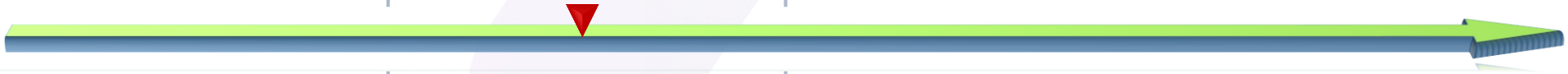
Fuente: Adaptado de HBR y Forbes.

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

Futuro: ¿Época de cambio o cambio de época?

"No nos encontramos en un entorno que esta cambiando, sino en un entorno que nunca va a dejar de cambiar"

Banca Computacional | **Banca Inteligente** | **Banca Exponencial**



Seguridad: Gestionando la incertidumbre

- ✓ Campañas masivas
- ✓ Experiencia multicanal
- ✓ Herramientas automatizadas genéricas

- ✓ Mejorar experiencia del cliente.
- ✓ Inicios de explotación de BIG Data
- ✓ Real Time
- ✓ Nuevas plataformas de automatización

Retos en la Banca de hoy:

I. Experiencia del cliente
II. Eficiencia operativa
III. Gestión del dato
IV. Personalización y asesoramiento al cliente
V. Regulación más estricta y dinámica
VI. Nuevo competidores tecnológicos

Banca aumentada | **Banca abierta**

Banca cognitiva | **Banca automatizada**

Existirán 2 tipos de bancos:

- Supervivientes que han sabido adaptarse
- Reliquias luchando por sobrevivir

Fuente: Investigación Grupo GFT

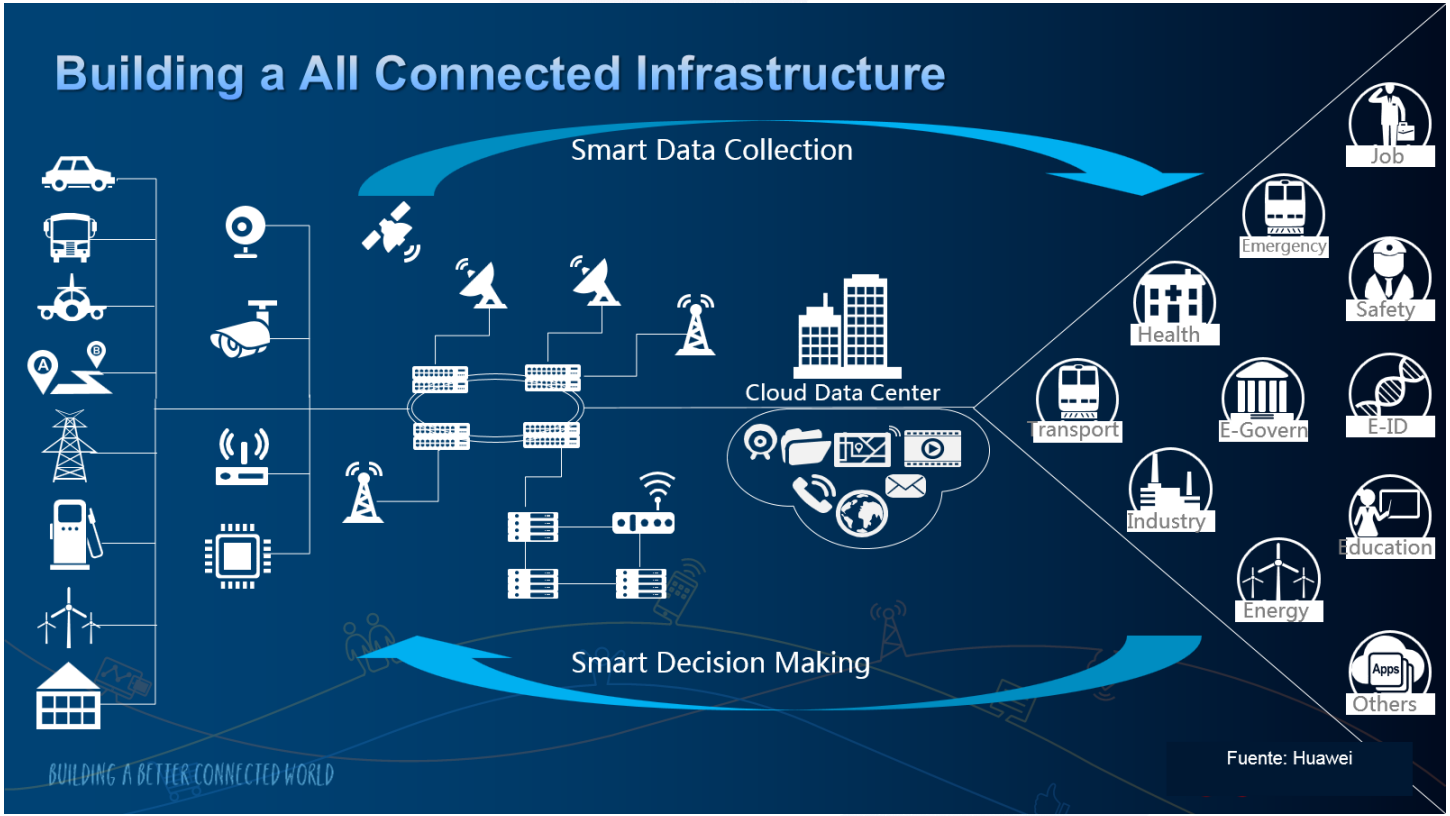
¿Época de cambio o cambio de época?

Visión 2050

Fuente: Kaspersky

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

Smart Cities: Construyendo una infraestructura interconectada



IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

El efecto camaleón: las amenazas del cambio
La seguridad puede ser un facilitador del cambio o un inhibidor del negocio si no se gestiona de forma adecuada.

¿Cómo impacta el uso de la tecnología en nuestro día a día?

- Salud: ↓ 8% del costo social de la salud.
- Seguridad: ↓ 30% en crímenes.
- Medio Ambiente: ↓ 30% de consumo de agua

- Enfoque en tareas de valor agregado: ~50% de tareas automatizables[3].
- Necesidad de carreras relacionadas a TI: 1.8M de puestos en Ciberseguridad por cubrir (gap)[4].
- Fuerza de trabajo remota.

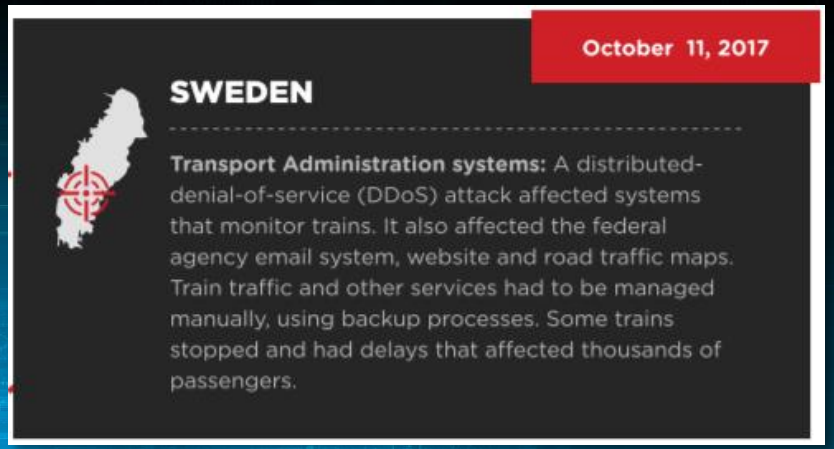
- Mejora de los journeys del cliente (+Digital: 20B dispositivos IoT conectados al 2020).
- Decisiones de negocio data-driven.
- Mejor conocimiento del cliente → Microleads

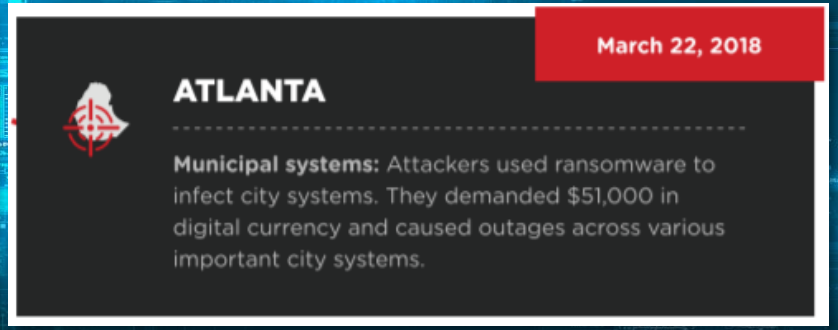
(1) Smart Cities: Digital Solutions for a more available future. Mckinsey, 2018. (2) Realizing 2030: A divided vision of the future. Dell Technologies. (3). Jobs lost, Jobs gained: Workforce transitions in a time of automation. Mckinsey, 2017. (4). The cybersecurity workforce GAP. CSIS, 2019.

"80% de ejecutivos TI indica que no puede mantenerse al día con la creciente sofisticación de los ciberataques… Si esto continúa, el cyberbacklash podría desacelerar la transformación digital (-$3T en productividad)."
Mckinsey

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital

Smart Cities: Principales ataques



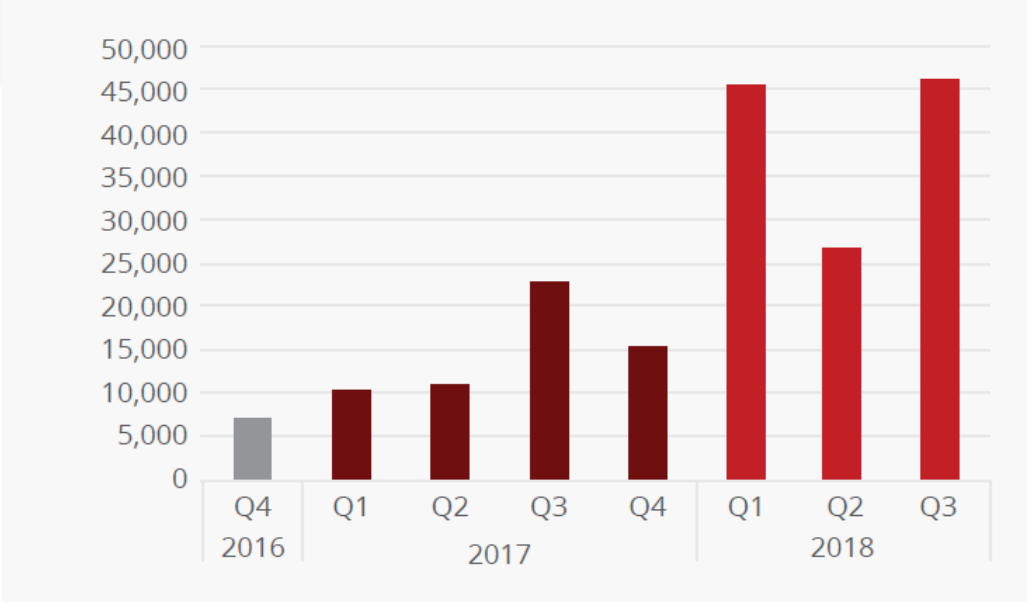


Fuente: IOActive.com

IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital.

IoT: Crecimiento del malware en dispositivos

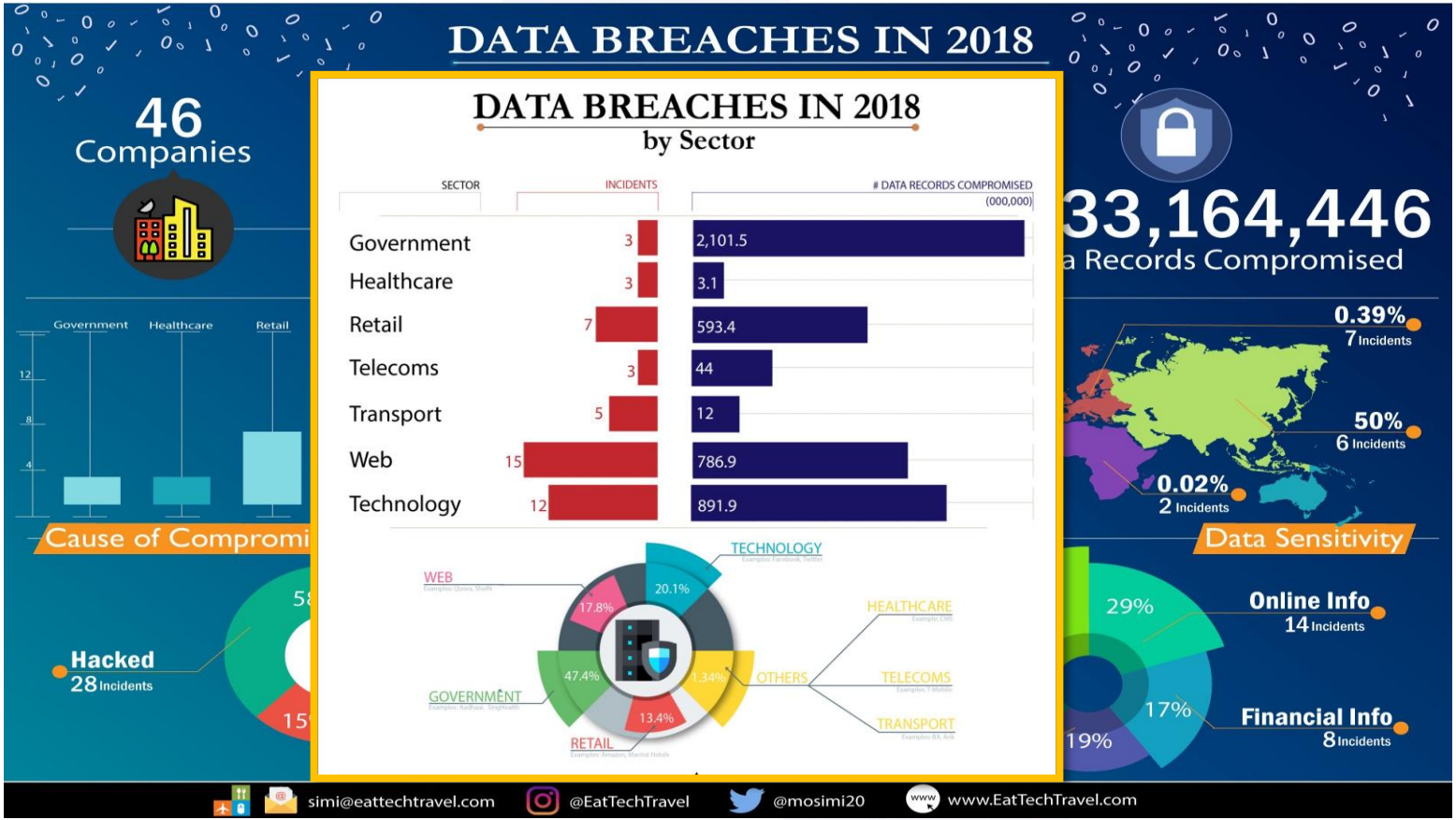
Las amenazas a los dispositivos de la Internet de las cosas apuntan a una variedad de hardware, incluidas cámaras IP, enrutadores domésticos y dispositivos inteligentes.



Fuente: McAfee Labs Threats Report – December 2018

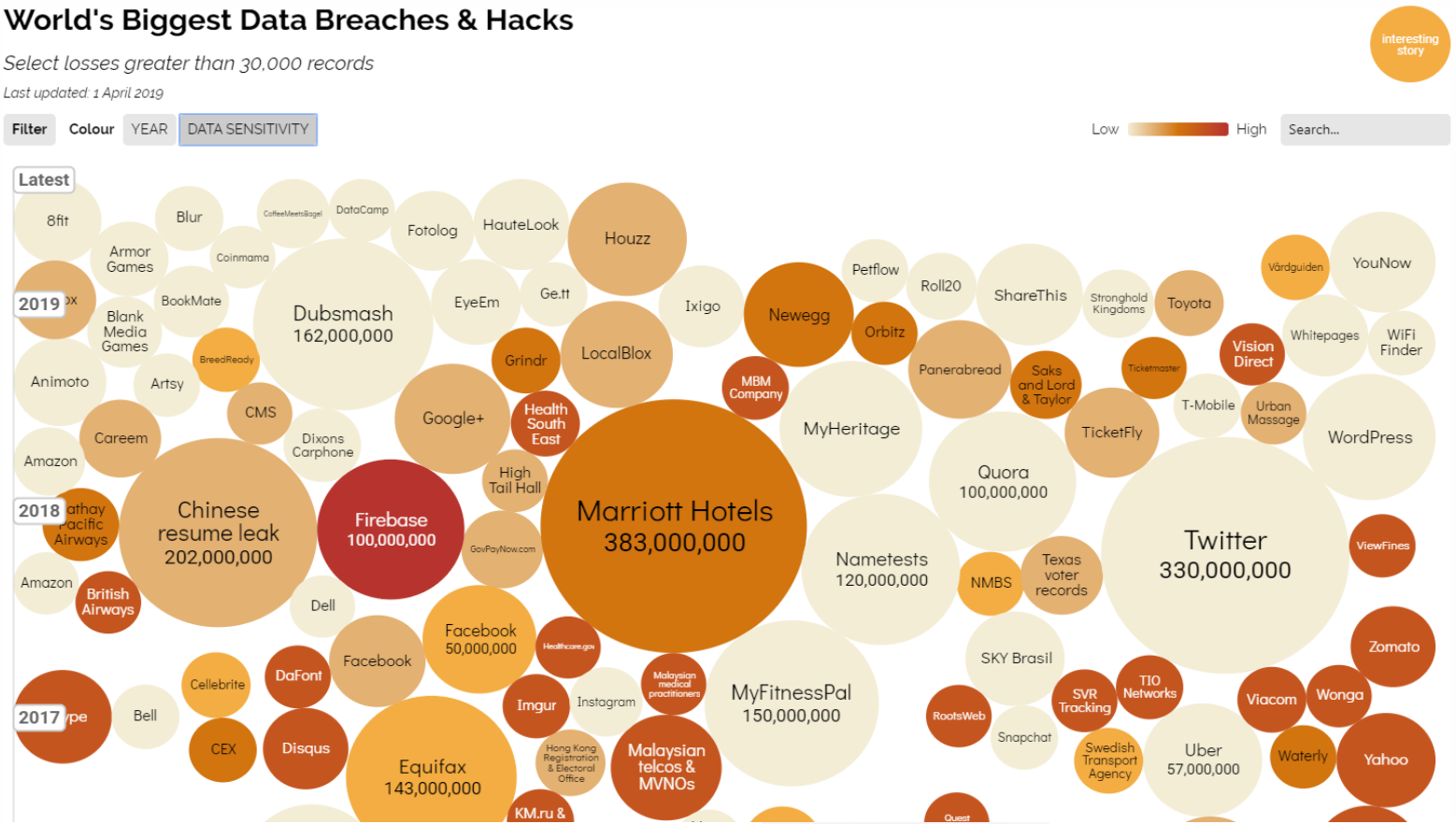
IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital.

La información como uno de los principales targets



IV. ¿Qué viene? Gestionando la incertidumbre en la transformación digital.

La información como uno de los principales targets



La inteligencia artificial como recurso para la sofisticación del uso de malware.

Fuente: Security Intelligence

Como entendemos en el BCP el Principio Profesionalismo

V. Comentarios Finales

Presente y Pasado de la Transformación Digital: ¿Qué, cómo y cuándo?
El concepto de la **ESCALABILIDAD** está presente tanto en el **PRODUCTO** como en el **RIESGO** asociado al desarrollo tecnológico. Esto exige al frente de la seguridad actuar y planificar con **prospectiva**, generando estrategias ante situaciones de crisis y **planes de contingencia** donde las decisiones de soporte al negocio permitan cubrir de manera **integral el aspecto cualitativo y principalmente el cuantitativo.**

Futuro: ¿Época de cambio o cambio de época?
El **CAMBIO DE EPOCA** muestra un presente retador en el ámbito de la seguridad por la diversidad de frentes y constante innovación generada por la transformación digital. Esto orientado a satisfacer las **necesidades de los nuevos usuarios** que exigen mejorar **su experiencia a través del uso de la tecnología de última generación.**

El efecto camaleón: las amenazas del cambio
En este contexto de innovación los ciberdelincuentes resultan beneficiados con la oferta de productos y servicios que debido al desarrollo tecnológico están en constante cambio **permitiéndoles mimetizarse**. Por ejemplo, en el caso de los **desarrollos bajo metodología ágil** que **no cuentan con una base sólida de controles** se facilita la **poca visibilidad de los escenarios de riesgo** que hoy enfrenta la Industria Bancaria como **Fast Follower**.

De la seguridad tradicional a la Seguridad ante la Incertidumbre
En el caso de la gestión de la incertidumbre se deberán considerar: i) los desarrollos de los líderes tecnológicos y ii) los cambios de hábitos y nuevas costumbres de los usuarios. Lo que si sabemos es que los factores indispensables para la **gestión del riesgo serán el desarrollo de capabilities y talento, el uso de herramientas, las decisiones basadas en información y la rápida capacidad de adecuación.**

14-15 NOVIEMBRE

HOTEL LAS AMÉRICAS
CARTAGENA DE INDIAS,
COLOMBIA.

18°CONGRESO DE RIESGO FINANCIERO

MEJORES PRÁCTICAS EN
UN CONTEXTO DESAFIANTE

José Marangunich R. – Ph.D
Head of Corporate Security & Cyber-Crime
Banco de Crédito del Perú - CREDICORP

President Strategic Committee of Security Risk Management
Peruvian Banking Association - ASBANC

Tipologías de fraude, Tendencias para su mitigación y principales riesgos