CLAIN 2018
XXII Congreso Latinoamericano
de Auditoría Interna y Evaluación
de Riesgos PANAMA, 17-18 de Mayo 2018

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Cómo Prevenir y Gestionar el Fraude en los Procesos Tecnológicos

Dr. José Marangunich R.
Gerente del Área Seguridad Integral para los Negocios
Banco de Crédito del Perú - CREDICORP

Presidente del Comité Estratégico de Seguridad Integral
Asociación de Bancos del Perú - ASBANC
Mayo, 2018

Cómo Prevenir y Gestionar el Fraude en los Procesos Tecnológicos

I. **Introducción:**
   - ¿A dónde vamos?
   - ¿En dónde estamos?

II. **Tendencias:**
   - Grandes números
   - Tecnologías
   - Internet del todo
   - Usuarios
   - Formato de negocio
   - Riesgos

III. **Impacto:** Ciberfraude en las empresas (caso de estudio)

IV. **Ciberfraude:** ¿Cómo enfrentarlo?

V. **Proceso clave:** Gestión del fraude cibernético

VI. **Creando cultura de ciberfraude:**
   - Educación y Concientización al Cliente interno
   - Educación y Concientización al Cliente Externo

I. **De la visión estratégica a la práctica (caso en banca):** Roadmap, Planificación y manejo de las capacidades internas, externas, sinergias y resultados

II. **Reflexiones Finales**

Introducción:
¿A dónde vamos?

Introducción:
¿En dónde estamos?

Percepción

El **86%** de gestores de riesgo auto-evalúa a su organización como **bien o mejor** preparada para responder ante incidentes cibernéticos

¿El Auditor llegó con el mensaje claro y oportuno a la Alta Dirección?

Expertos externos evalúan consistentemente un **desempeño menor** en las prácticas preventivas contra riesgos cibernéticos.

Fuente: Experian & Advisen, Cyber Risk Preparedness and Response Survey 2017

Práctica

El **42%** de compañías ha incrementado su gasto en combatir fraude en los últimos 2 años

El 44% planea incrementar estos gastos en los próximos 2 años.

A pesar del aumento en gasto siguen prevaleciendo enfoque reactivos y defensivos.

Sólo 54% de compañías ha realizado una evaluación de riesgo de fraude en los últimos 2 años.

Sólo 46% de ha realizado evaluaciones de riesgo cibernético.

Una de cada 10 empresas **no ha realizado evaluación de riesgo alguna** en los últimos 2 años.

Fuente: PWC, 2018 Global Economic Crime and Fraud Survey

Plan de acción

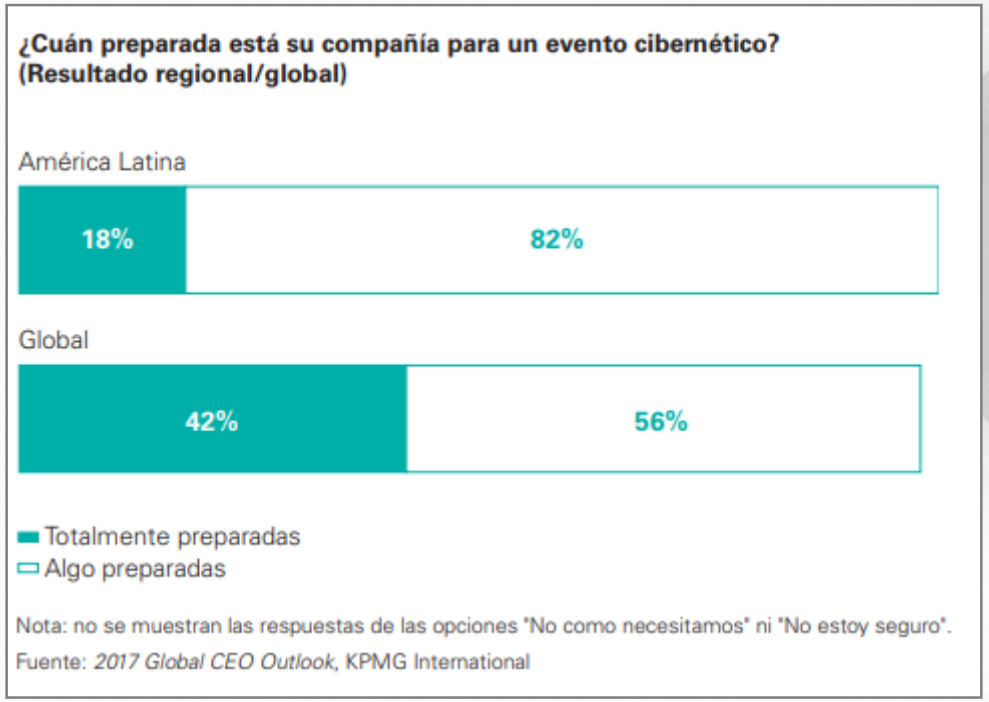
El **37% a más** considera que un enfoque en **Comunicación de crisis** redituará la mayor mejora en **capacidad de respuesta** ante ciberincidentes.

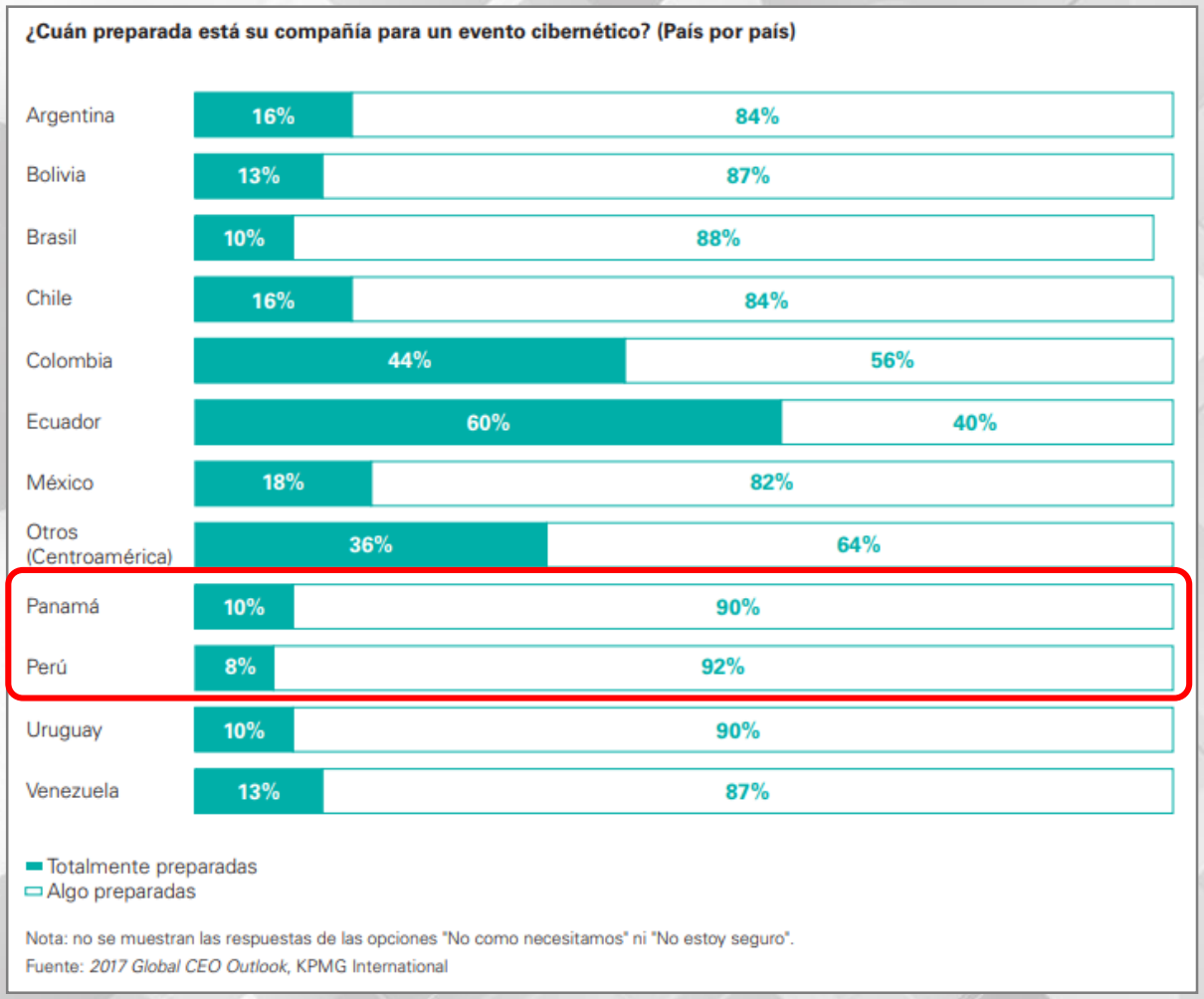
El **32% a más** considera que un enfoque en **educación a empleados** redituará la mejora en **capacidad de prevención** de ciberincidentes.

Fuente: Experian & Advisen, Cyber Risk Preparedness and Response Survey 2017

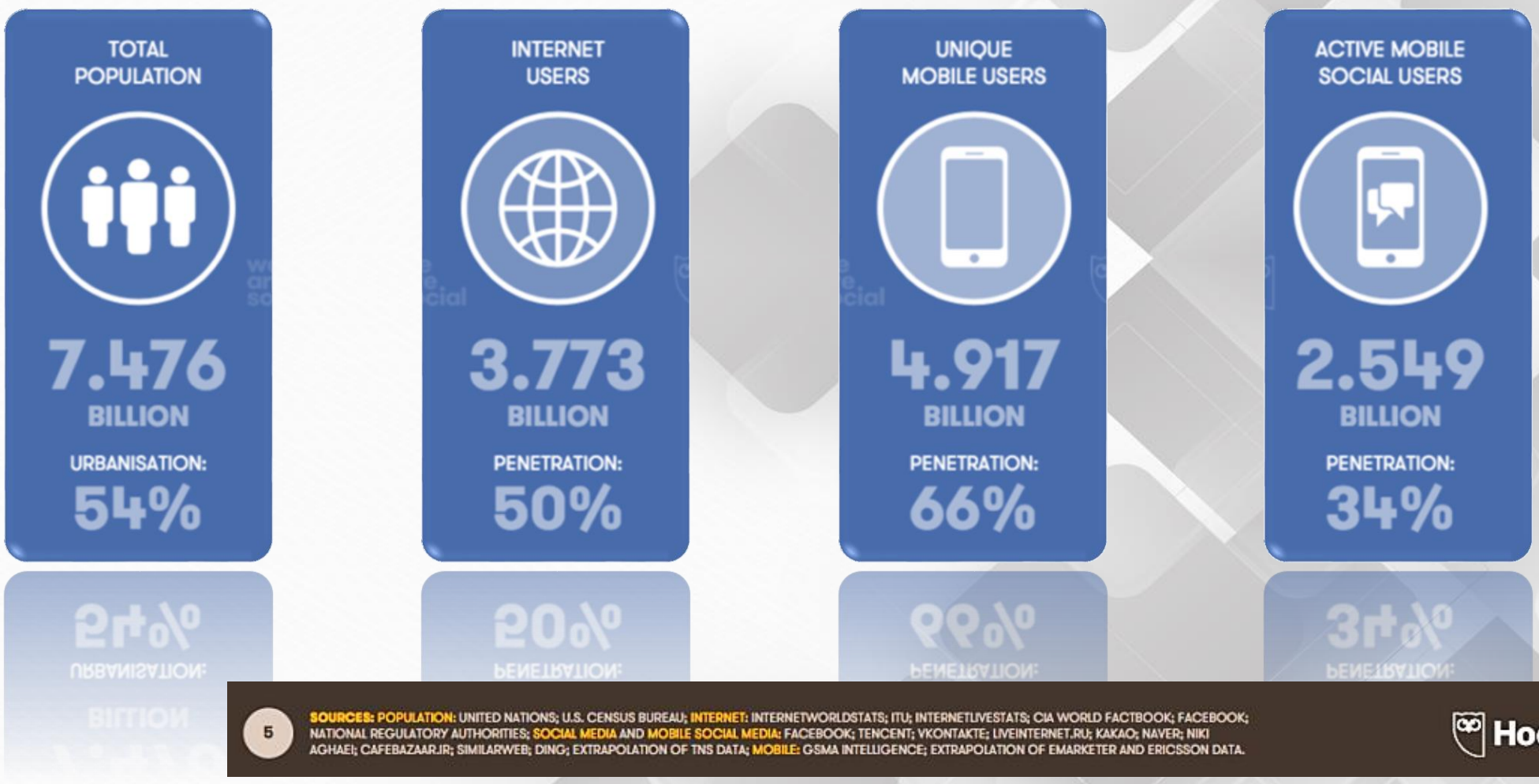
Introducción:
¿En dónde estamos?

¿Cómo el fraude cibernético es percibido en las organizaciones?





Tendencias:
Grandes números: Panorama digital en cifras



Tendencias:
Tecnologías mas relevantes y disruptivas de la economía digital

Las tecnologías más

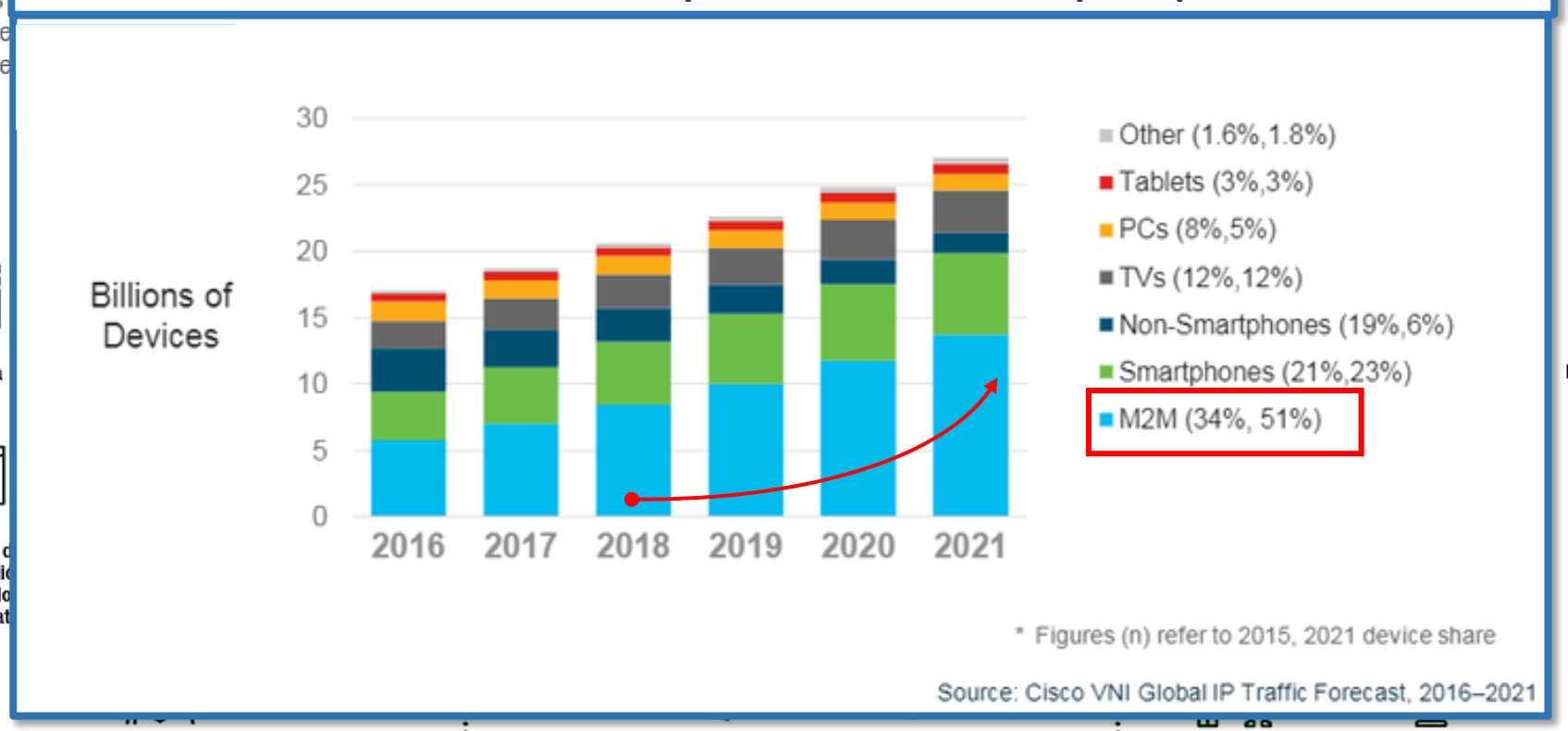
Las tecnologías más disruptivas

Las tecnologías de tendencias que

ucho más

s años

Crecimiento de dispositivos conectados por tipo



Big Data

Lenguajes d programacio relacionado con Big Dat

Inteligencia Artificial

Impresión 3D

Huellas Digitales

Smart cities

@icemd

Realidad Virtual & Aumentada

Blockchain

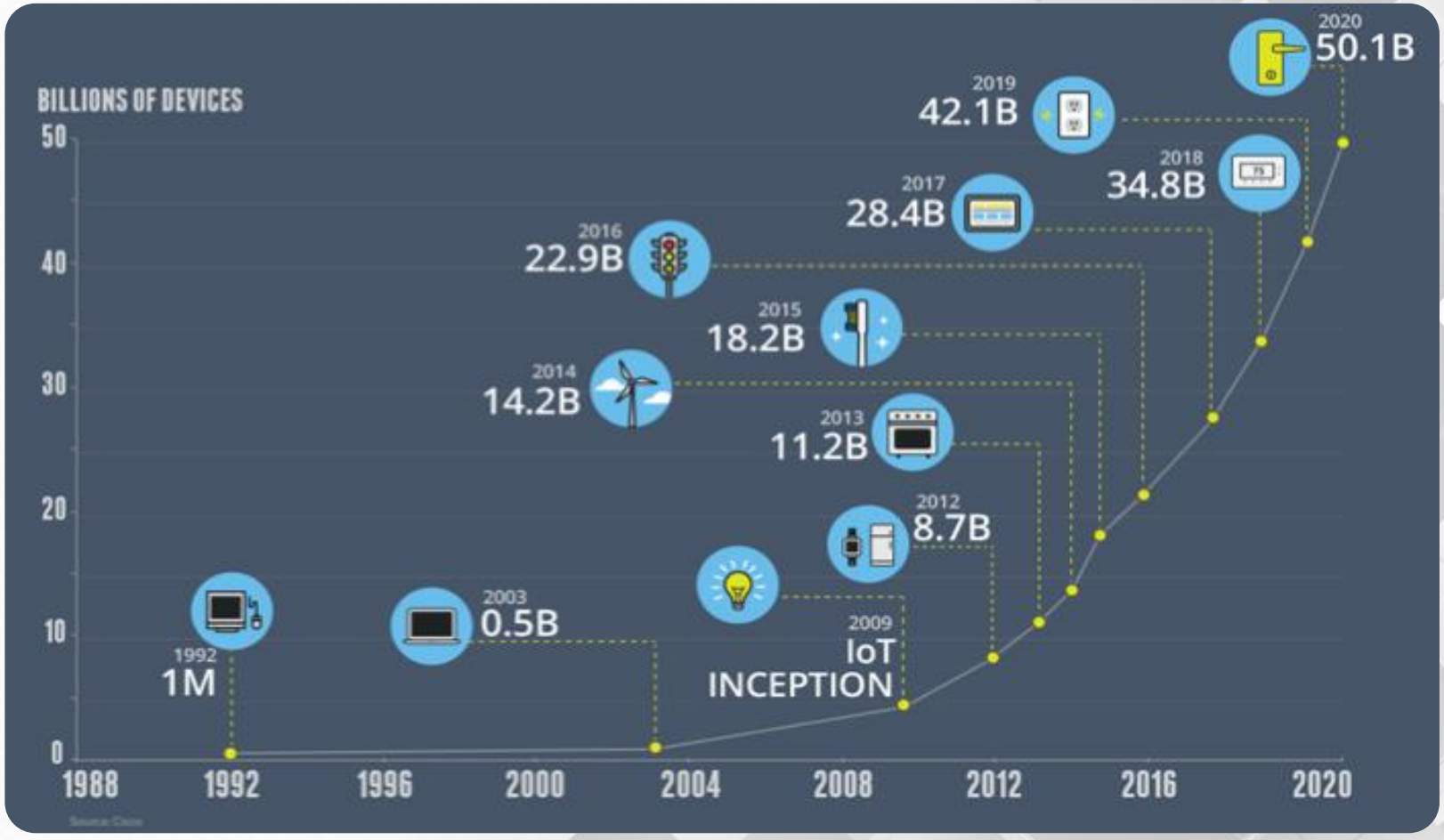
Wearable Technology

Conexión máquina/humano

Convivencia de la logística física y digital

Fuente: ICEMD, Las tecnologías mas relevantes y disruptivas de la tecnología digital, 2017

Tendencias:
Hacia el Internet del Todo (IoE)



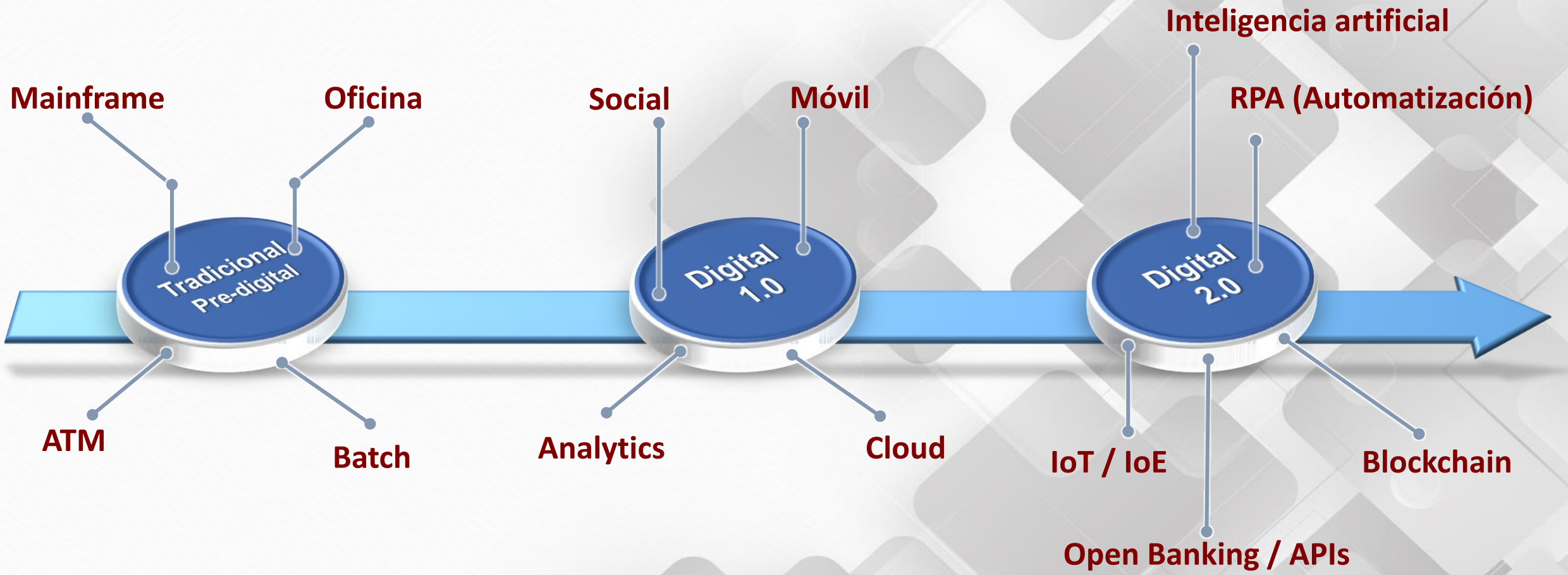
Tendencias:
Crecimiento de IoT

Tendencias:
Perfiles de los Usuarios

1945 — 1960 — 1980 — 1995

	Veteranos (Tradicionalistas)	Baby Boomers	Generación X	Generación Y (Millenials)	Generación Z (Generación Internet)
Producto más usado					
Medios de comunicación					
Preferencia de comunicación	 Cara a Cara	 Cara a Cara preferentemente / Por teléfono o Por correo si es necesario	 Mensaje de Texto o Por Email	 Online y Móvil (Mensaje de Texto)	 Facetime
Porcentaje en USA / HISPANOS	**9 %** **8% Hispanos**	**24%** **11% Hispanos**	**20%** **18% Hispanos**	**22%** **21% Hispanos**	**26%** **22% Hispanos**
Actitud hacia la tecnología	**Análogos** En gran parte desconectados	**Análogos** Primeros adaptadores de las TI	**Inmigrantes Digitales** Transición hacia la era digital	**Nativos Digitales** Dependiente de las TI	**Nativos Digitales** Totalmente dependientes de las TI
Actitud hacia la carrera	Los trabajos son para toda la vida	Organizacional: Las carreras son definidas por los empleadores	Fiel a la carrera, no necesariamente al empleador	Empresarios digitales: trabajan con las organizaciones, no para ellas	Se mueven sin problemas entre organizaciones y negocios emergentes

Tendencias:
Del Negocio Tradicional al Digital

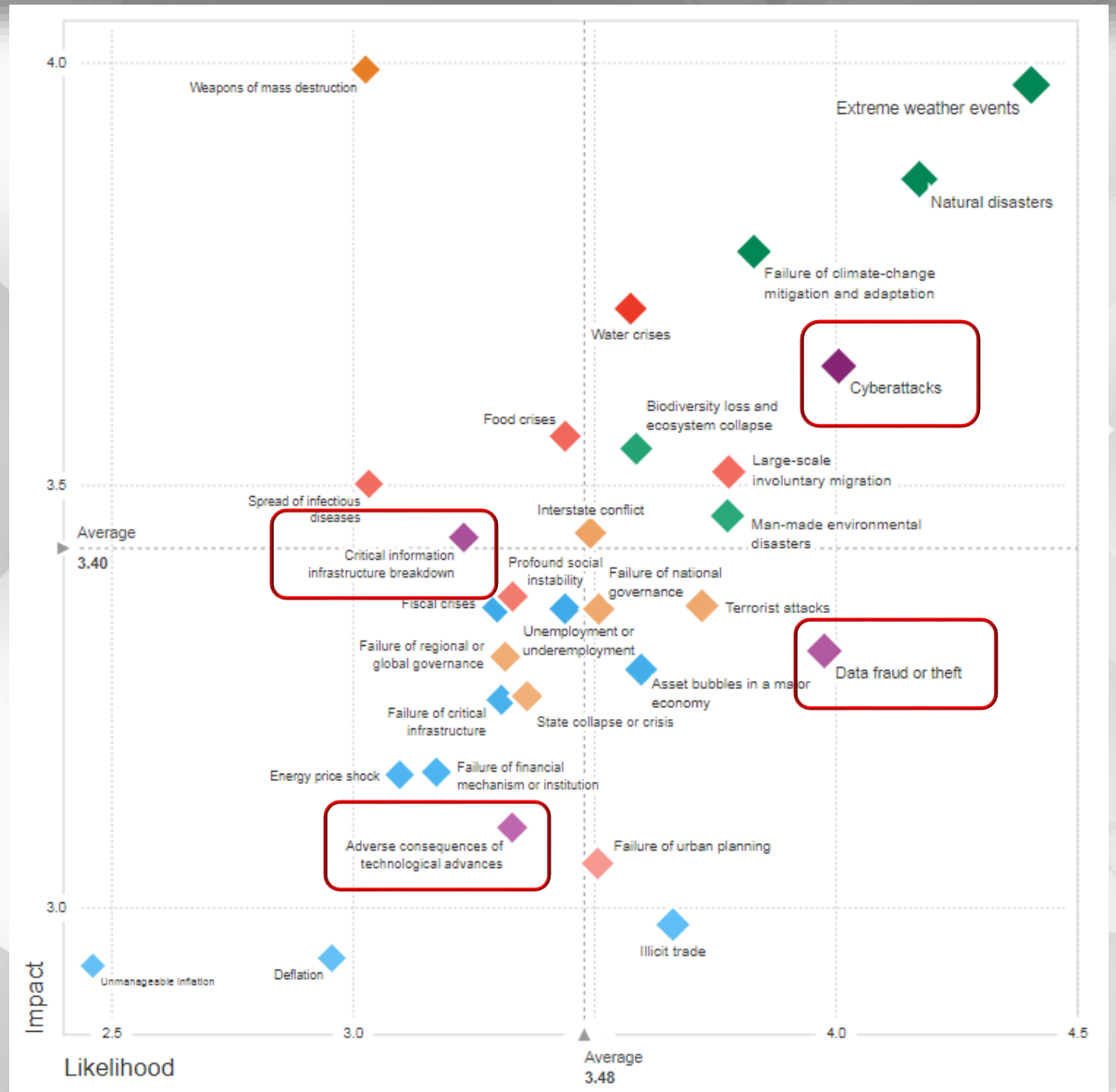


Fuente: The Financial Brand, 2017

Tendencias:
Evolución del Riesgo

	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 natuales mayores	Cíber-ataques
4to	Cambio climático	Colapso o crisis estatal	Falla del gobierno nacional	Ataque terrorista de escala mayor	Robo o fraude de información
5to	Cíber-ataques	Alto desempleo estructural o subempleo	Catástrofes natuales mayores	Incidente masivo de robo/fraude de información	Falla de mitigación o adaptación al cambio climático

Económico Medioambiental Geopolítico Social Tecnológico



Fuente: Global Risk Report 2018

Impacto: Ciberfraude en las empresas (Caso de estudio)

Caso Facebook: Compromiso de información

Fuente: Nasdaq Real Time 2018

Ciberfraude: ¿Cómo enfrentarlo?

CLAIN 2018
XXII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos PANAMA, 17-18 de Mayo 2018

ABP

FELABAN

Gobierno Corporativo
Auto-regulación

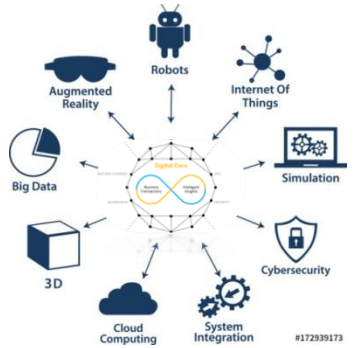
Preventivo

Autoridades
Regulación

Visionario

Tendencias
Nuevos enfoques de negocio

Desarrollo Digital e Innovación

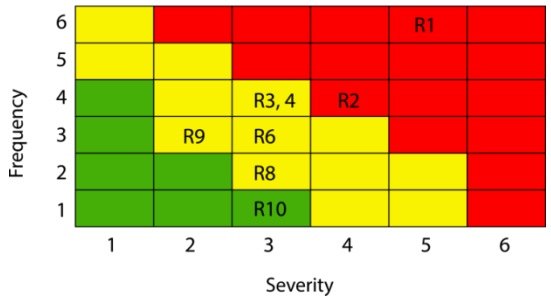


Reactivo
(aspecto reputacional)

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

POLICIA NACIONAL DEL PERU
PATRIA

Tradicional
(por riesgos)

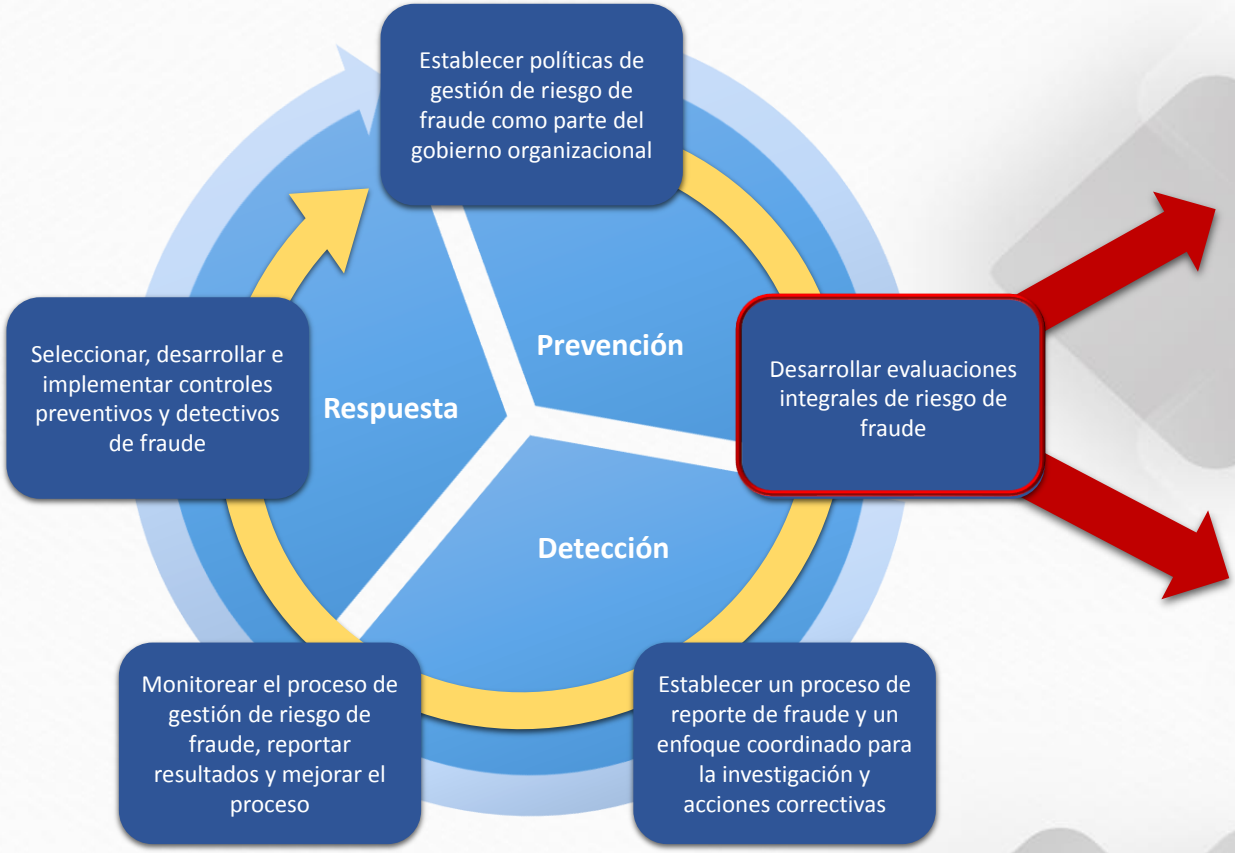


Pro-Cliente

Proceso clave: Gestión del fraude cibernético

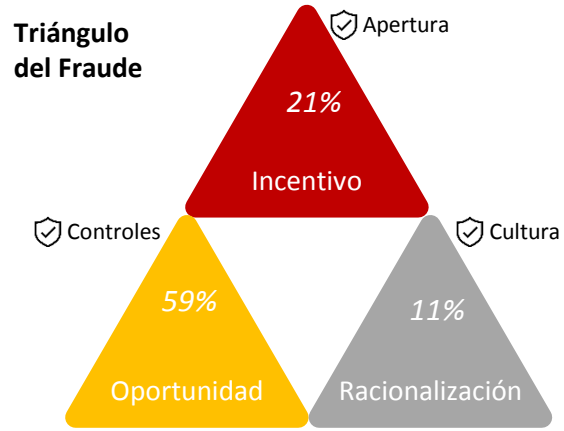
Modelo de Prevención de Fraude según COSO

Ciclo de Gestión de Riesgos de Fraude COSO



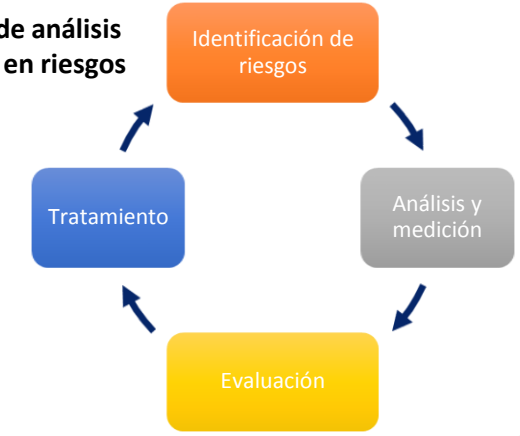
Fuente: ECA, Fraud Audit Brief 2017 (basado en COSO Framework)

Triángulo del Fraude



Fuente: COSO, Marco de Control Interno 2013 & PWC, Global Economic Crime and Fraud Survey 2018
(% de respuestas que clasificaron al factor como el principal factor contribuyente en fraude interno)

Marco de análisis basado en riesgos

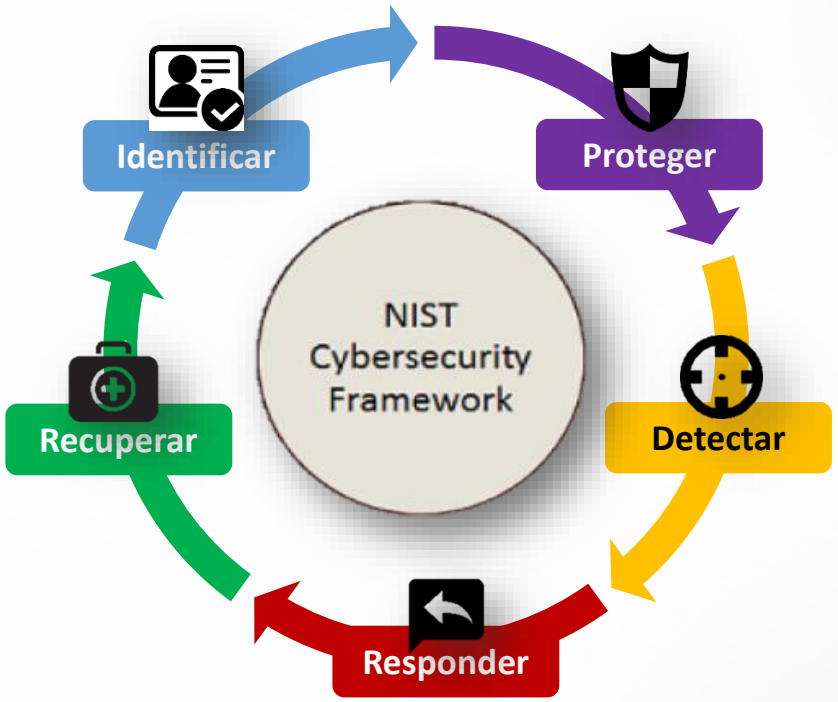


Fuente: Área Riesgo de Operación, BCP

Proceso clave: Gestión del fraude cibernético

Implementación de un Modelo de Prevención de Fraude Cibernético basado en un Marco de Trabajo Estándar

ISO 27001 · COSO · COBIT 5 AN ISACA® FRAMEWORK

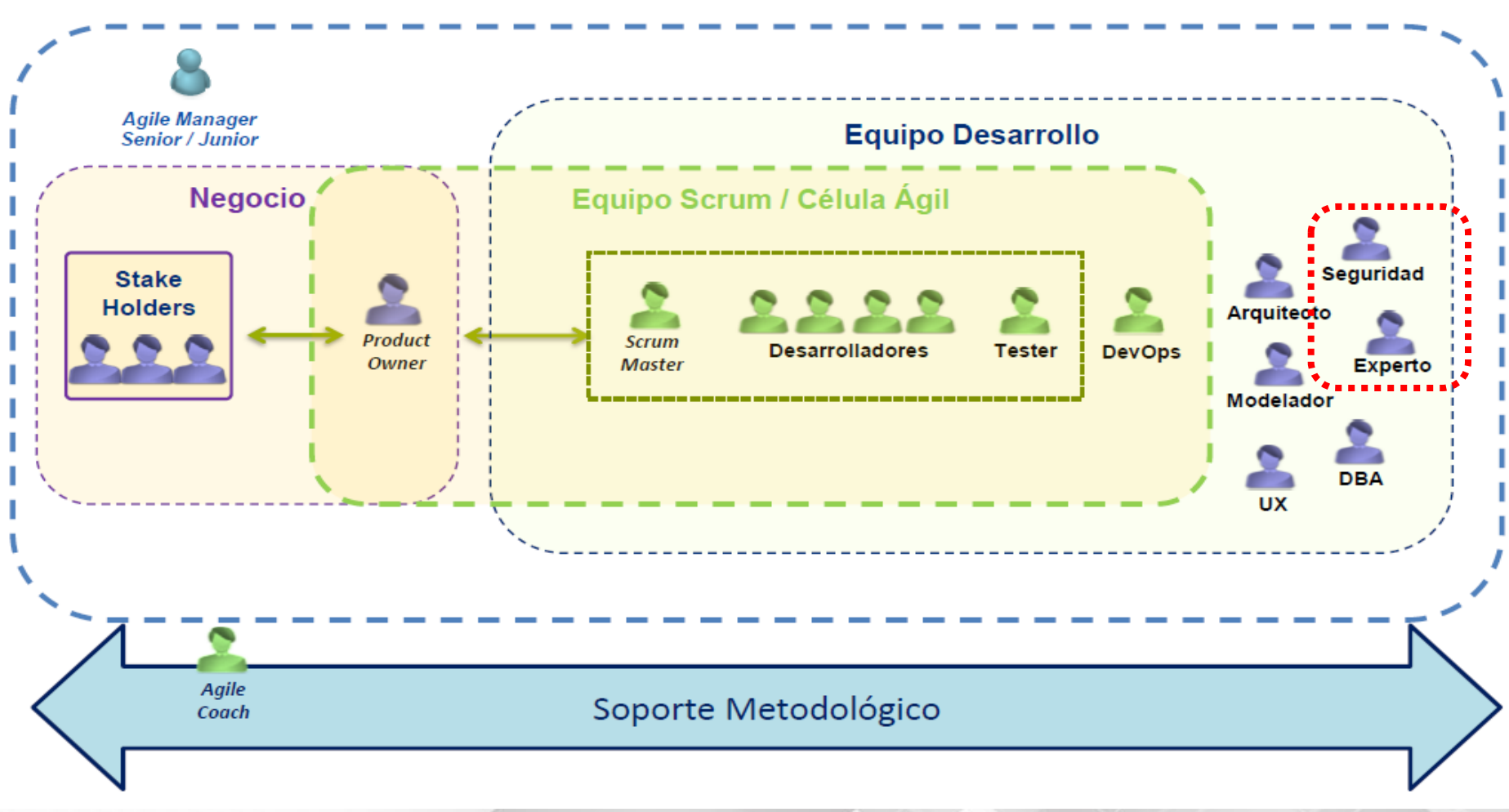


Booz Allen Hamilton

	Prevenir	Detectar	Responder	Recuperar
Personas	Custodia	Administradores de sistemas / accesos	Equipos funcionales	Equipos de respuesta
Procesos	Protocolos de Seguridad	Gestión de alertas	Plan de reacción inmediata	Procesos de contingencia
Información	Manejo de fuentes Análisis de data Identificación de riesgos	Diseño y aplicación de estrategias	Ejecución de protocolos	Continuidad operativa
Tecnología	Arquitectura de Seguridad	Sistemas de seguridad	Centros de monitoreo	Equipos de contingencia

Proceso clave: Gestión del fraude cibernético

Modelo de Prevención de Fraudes bajo un Esquema de Trabajo Ágil



Proceso clave: Gestión del fraude cibernético

Proceso clave: Gestión del fraude cibernético

Aspectos regulatorios: Inteligencia Artificial y Protección de Datos Personales

Fases de la Tecnología

Las personas se conectan a internet

Las personas se conectan a través de internet

Son las cosas las que conectan a internet para mejorar la vida de las personas

Fase Actual

Las cosas (robots) interactúan con el entorno de forma autónoma e independiente del control humano.

Industria 4.0

"European Civil Law Rules in Robotics" – Eurocámara

Febrero 2017

9 principios éticos a ser desarrollados en la robótica

2 principios orientados a la gestión de datos personales

4 Proteger a la humanidad contra las violaciones de la privacidad cometidas por un robot

5 Gestión de los datos personales procesados por robots

LOPD Ley Orgánica de Protección de Datos

GDPR The General Data Protection Regulation

Protección de Datos Personales

Desafíos Regulatorios en Ciberseguridad para la Robótica

En el caso de los robots inteligentes existe una interconexión continua e instantánea entre el mundo físico y digital y se deberá velar simultáneamente por la seguridad en ambos entornos.

Los robots inteligentes, como sistemas físicos cibernéticos, no están libres de sufrir ataques y **las principales amenazas a las que se enfrentan son:**

- Malware
- Ciberespionaje
- Denegación de servicio
- Pérdida de Información
- Spam
- Phishing
- Daño Físico

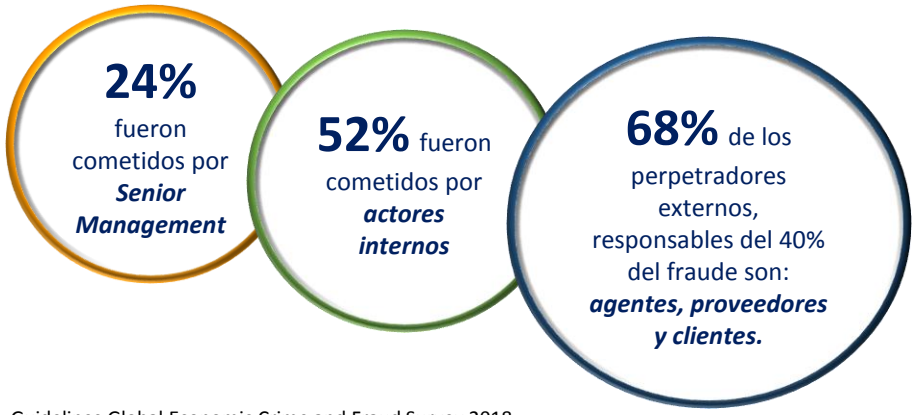
Cuestiones de Ciberseguridad: Desafío Regulatorio para la Robótica

- Limitación o prohibición de la fabricación de uso de robots inteligentes contrarios a la ética
- Seguridad técnica para evitar errores o ataques a los robots
- Seguridad en relación con los datos
- Adecuación de la información del robot
- Seguridad de los sistemas de autocontrol del robot
- Necesidad de interoperabilidad y estándares de normas técnicas internacionales
- Ingeniería inversa y las normas abiertas, garantizar que los robots puedan comunicarse entre sí
- Riesgo ante ciberataques a robots inteligentes interconectados

Fuente: Revista Jurídica de la Universidad de León 2017, "Regulación Legal de la Robótica y la Inteligencia Artificial: Retos del Futuro"

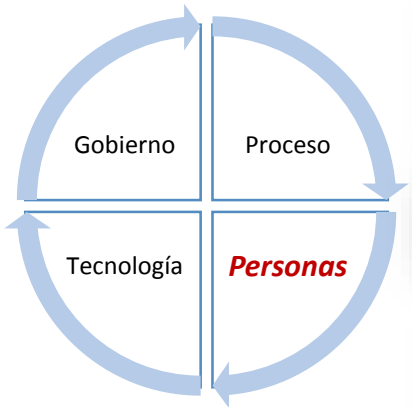
Creando cultura de ciberfraude:
Educación y Concientización al Cliente Interno

¿Quién comete el fraude?



Fuente: PWC - Guidelines Global Economic Crime and Fraud Survey 2018

4 Elementos Claves de la Gestión de Riesgos



54% de usuarios dicen que sus empleadores **no proveen capacitación en ciberseguridad.**

1 de 3 usuarios **prefieren una conexión a internet "rápida" que una conexión "segura"** cuando se les preguntó para escoger entre los 2 tipos.

1 de 5 de usuarios han sido presas de un **ataque de phishing.**

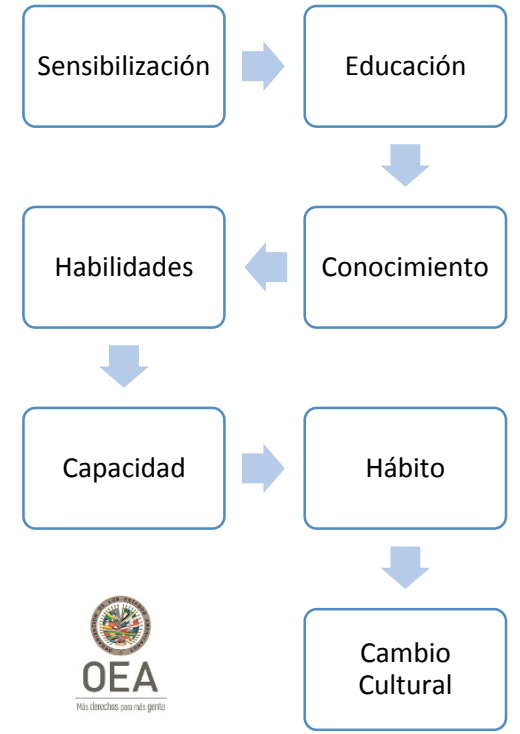
Fuente: ISACA'S 2016 UK CYBERSECURITY PERCEPTIONS STUDY

Desarrollo de un Programa de Concientización y Capacitación sobre Seguridad de TI

*El factor **"persona" es clave** para proporcionar un adecuado y apropiado **nivel de seguridad a la organización.***

Fuente: Guidelines NIST 800-50 "Building and Information Technology Security Awareness and Training Program"

Educar a las personas acerca de la ciberseguridad** es de vital importancia **para la creación de** una cultura de ciberseguridad y **usuarios con inteligencia cibernética.



Fuente: OEA 2015 – Ciberseguridad Kit de Herramientas para la Campaña de Concientización

Creando cultura de ciberfraude:
Educación y Concientización al Cliente Externo

Los Consumidores "Talón de Aquiles de los Sistemas de Seguridad"

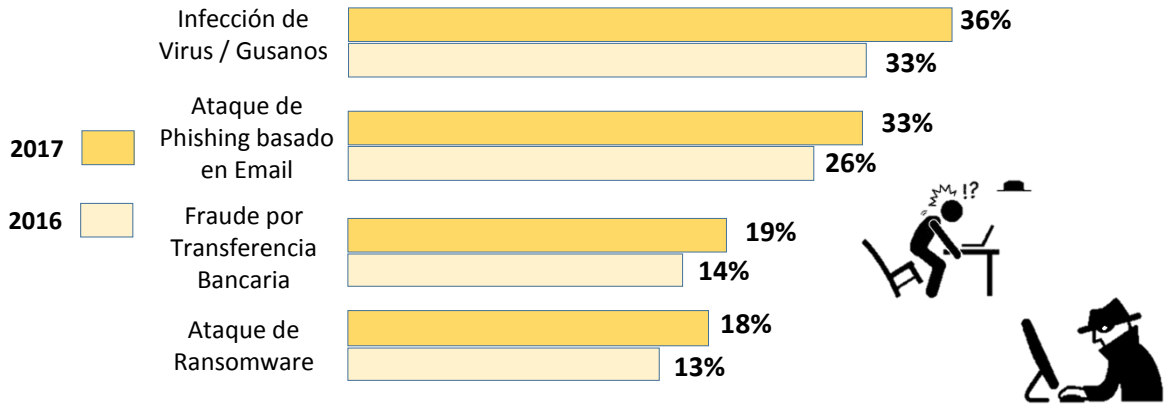
25% de los ***usuarios*** tiene una "comprensión limitada" de los riesgos que enfrentan en internet

43% de los ***usuarios*** afirma que utiliza la misma contraseña para múltiples cuentas online

60% de los ***usuarios*** aseguran que no saben cómo administrar y actualizar su configuración de privacidad en las redes sociales

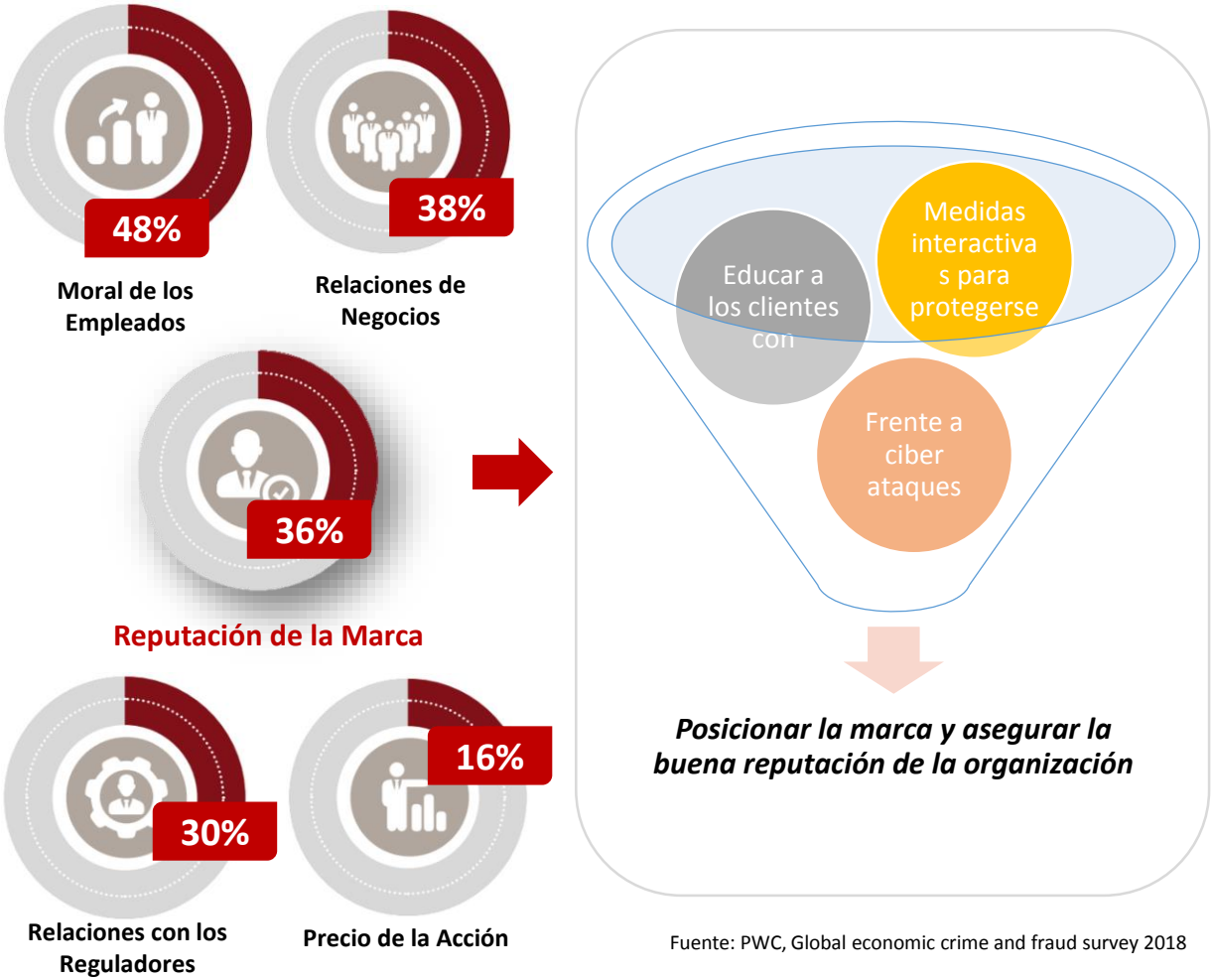
Fuente: Encuesta Get Safe Online (Iniciativa que promueve la seguridad en el Reino Unido)

Incidentes cibernéticos sufridos en los pasados 12 meses



Fuente: Global Fraud Risk Report 2017-18

Impacto del crimen cibernético en la organización

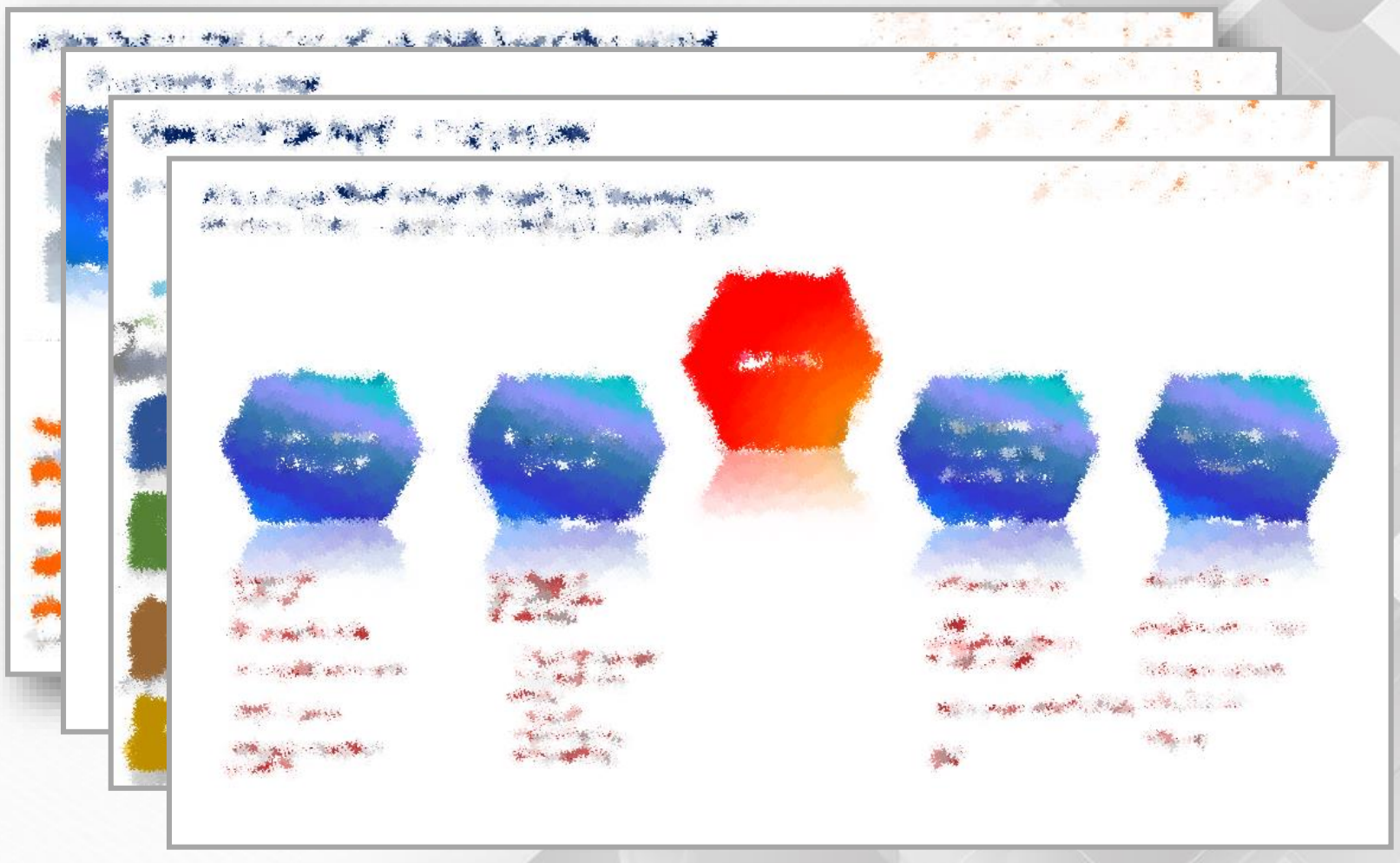


Fuente: PWC, Global economic crime and fraud survey 2018

De la visión estratégica a la práctica (caso en banca):

Roadmap, Planificación y manejo de las capacidades internas, externas, sinergias y resultados

Plan Seguridad Integral para los Negocios BCP (2018 – 2021)



Reflexiones finales

1. Principales consideraciones para una estrategia de Prevención y gestionar el fraude en los procesos tecnológicos :
   a) El modelo debe comprender las etapas Gobierno, Prevención, Detección, Respuesta y Recuperación.
   b) Estrategia de Gestión por Riesgos. Considerar de manera esencial cumplir con el Principio No.8 del COSO 2013.
   c) Formación de talento especializado en la Prevención y Gestión del riesgo de ciberseguridad y Crimen cibernético y Auditoria con este perfil, complementariamente a los equipos de Seguridad de la Informática/CISO de la organización.
   d) Incorporar en la gestión por Riesgos los escenarios vinculados al proceso de transformación digital y desarrollos bajo esquemas de metodologías ágiles e impulsadas por esquemas de co-creación. Ver con especial atención el cambio generacional y la evolución tecnológica.

2. En los roles de 2LD y 3LD considerar esquemas de control que considere la evolución de los procesos tecnológicos de cara al IoT y IoE. Además de un especial control sobre la obsolescencia tecnológica y brechas de seguridad. En este tipo de Riesgos, repensar los Ethical Hacking como principal mecanismo de validación en determinadas industrias.

CLAIN 2018
XXII Congreso Latinoamericano
de Auditoría Interna y Evaluación
de Riesgos PANAMA, 17-18 de Mayo 2018

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Cómo Prevenir y Gestionar el Fraude en los Procesos Tecnológicos

Dr. José Marangunich R.
Gerente del Área Seguridad Integral para los Negocios
Banco de Crédito del Perú

Presidente del Comité Estratégico de Seguridad Integral
Asociación de Bancos del Perú - ASBANC
Mayo, 2018