XXVIII Congreso Latinoamericano de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Organizado por

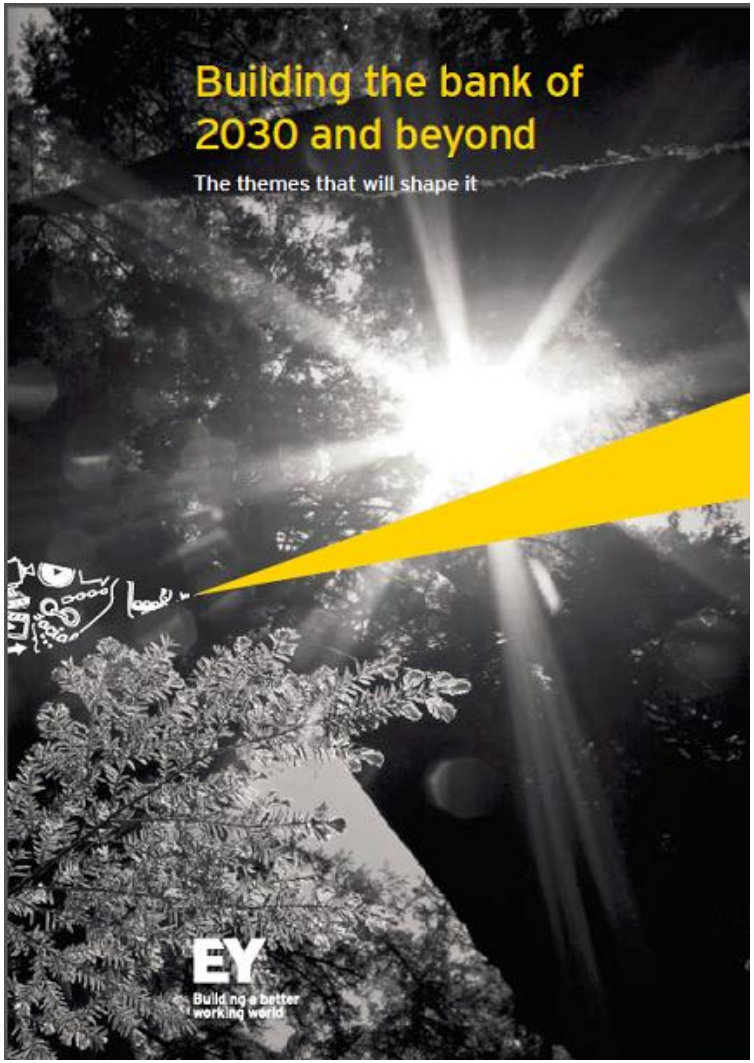
asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Rafael Huamán, CFE
Socio de EY Perú
Nov 2013

“La Prevención del Fraude en la Banca desde la óptica del consultor”

Construyendo el Banco del 2030 en un entorno dinámico

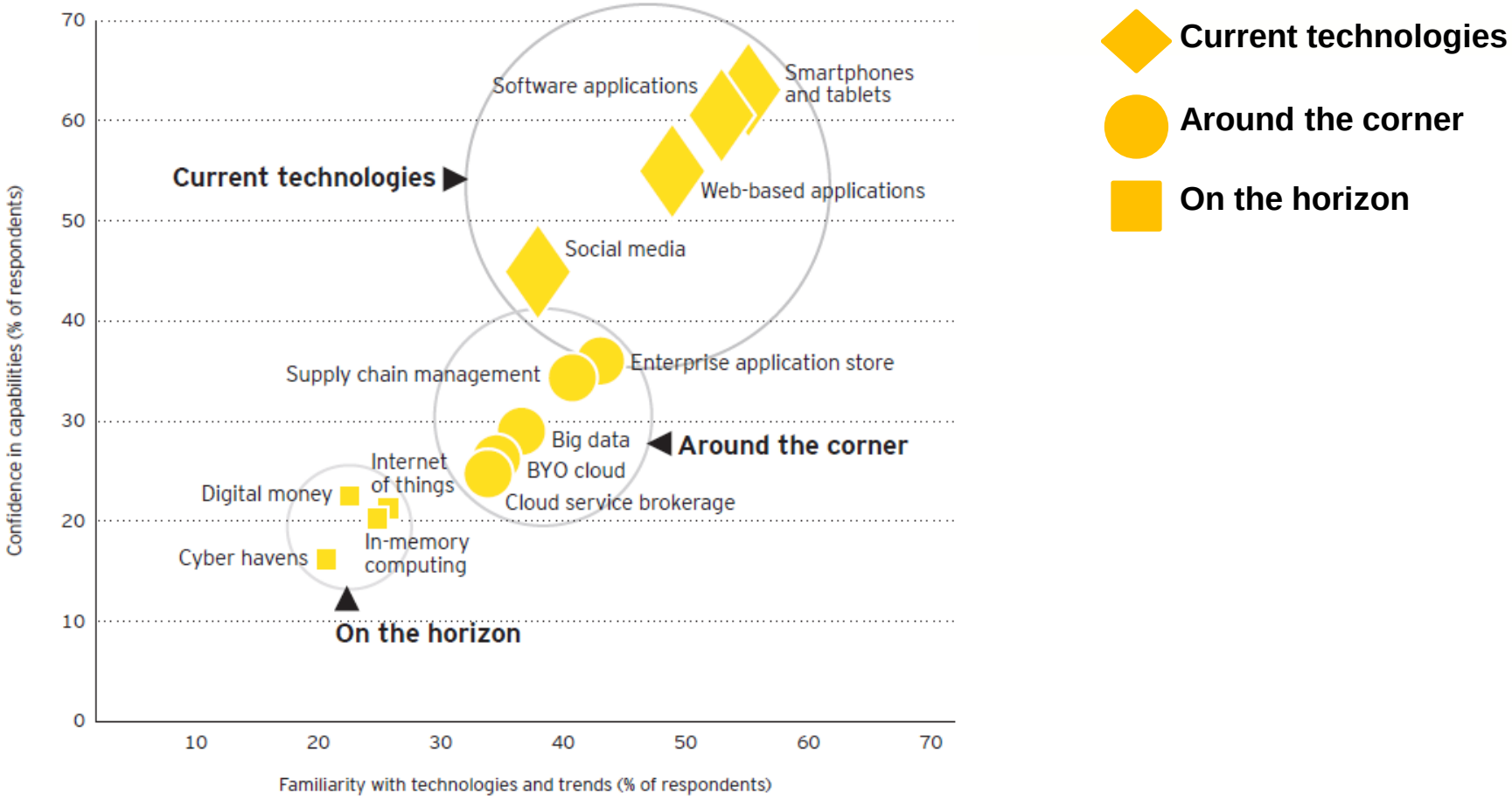


¿… y los riesgos?
¿…y el fraude?

Fuente: Estudio "Building the bank of 2030 and beyond. The themes that will shape it."
EY – Setiembre 2013

Tendencias y tecnologías emergentes

Tendencias y tecnologías emergentes



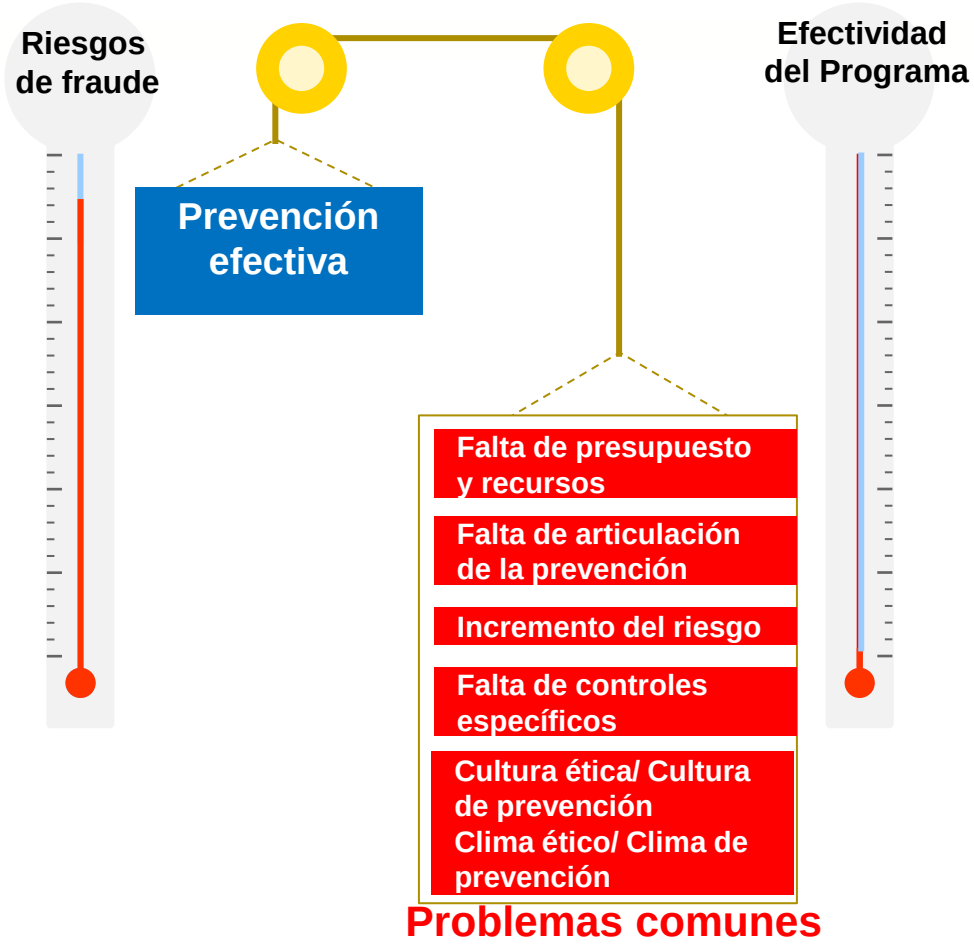
Fuente: Estudio "Under cyber attack. EY´s Global Information Security Survey 2013"
EY – Octubre 2013

Otros puntos a tratar

¿Qué observamos?

- Problemas comunes
- Buenas prácticas… y no tan buenas
- Replicando modelos
- Delineando la ruta a la prevención (Fraude interno/externo - articulación)
- Espacios para soluciones conjuntas
- Tendencias
- Ejemplo de monitoreo de riesgos específicos: “Know your Trader”

Algunos problemas comunes



Existe consciencia …

<u>pasar a la acción es el reto.</u>

Buenas prácticas… y no tan buenas

Existencia de áreas de prevención….. que no cuentan con Programas de Prevención

Líneas de denuncias

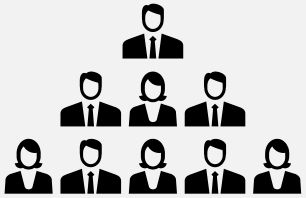
Líneas de reclamos

Se detecta
Se investiga
PERO NO SE DENUNCIA

Códigos de ética y conducta

Guías y políticas conceptualmente buenas pero no aterrizadas a la realidad de la organización

Entrenamiento:
Líneas de defensa



Riesgos específicos de fraude
VS.
Controles específicos

Carencia de protocolos de respuesta al fraude

Monitoreo…¿sobre qué?

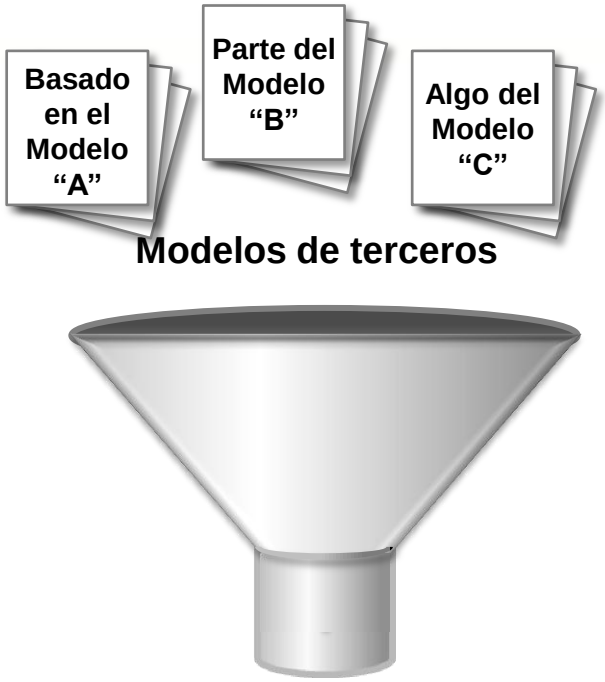
Replicando modelos

¿Cuál es el CRITERIO?

"Identificar modelos referentes, seleccionar alguno(s) de sus componentes, consolidarlos y diseñar el Modelo de Prevención de la Compañía" = Riesgo

Esta práctica asume que las características (p.e. cultura, procesos, canales, etc), variables y riesgos (entre otros aspectos) a los que se enfrentan las distintas Compañías son similares (cuando no siempre es así).

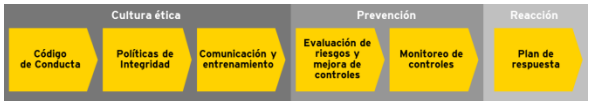
Un Modelo de Prevención de Fraude debe ser diseñado considerando los riesgos a los que se enfrenta la compañía, en el contexto de sus características propias (cultura, organización, estrategia, procesos, canales, soporte tecnológico, productos, clientes, etc).



Replicando modelos (continuación)

ACTIVIDADES CLAVE A CONSIDERAR

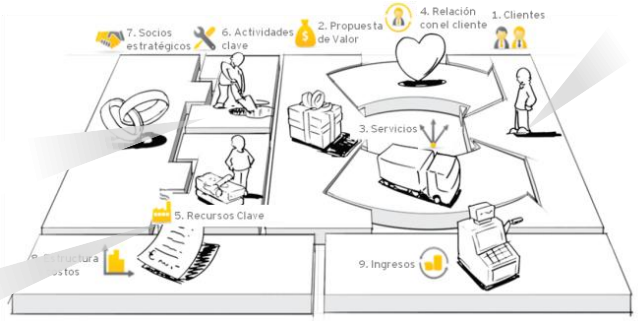
A **Tomar programas referentes y autoevaluarse en función a éstos**



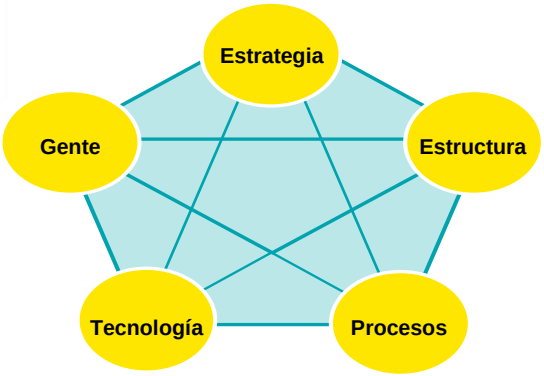
Procesos críticos

Recursos y herramientas

B **Diseñar un modelo *ad hoc***



Demanda de nuestros clientes Internos y Externos. (Naturaleza de riesgos a ser cubiertos por el modelo)



C **Una vez definido el modelo se debe pensar en cómo atender éste**

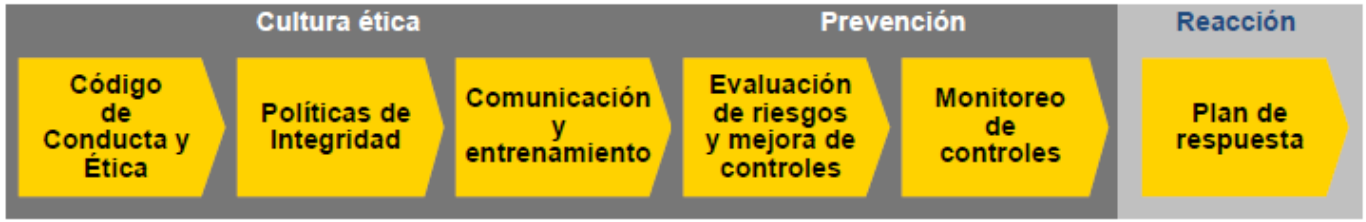
Fuente: EY, Componentes de un Programa de prevención
Fuente: Business Model Canvas

¿Factor CRÍTICO? ➡ **EQUILIBRIO**

- ✓ **Costo**
- ✓ **Riesgo**
- ✓ **Valor**

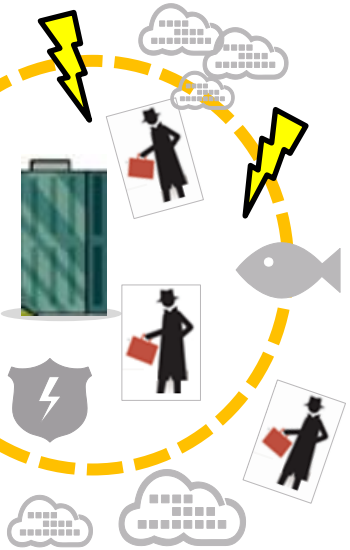
Delineando la ruta a la prevención

¿Fraude Interno?



Delineando la ruta a la prevención (continuación)

¿Fraude Externo?



Universo de riesgos

Ejemplos:

- Robo de información
- Ciber ataques
- Fraudes con tarjetas
- Canales móviles
- Canales electrónicos
- Suplantación
- Lavado de activos
- Proyectos
- Terceros/ Empleados de Proveedores de tecnología

…

Evaluación de Riesgos

Riesgos	Controles	Monitoreo
Bajos	Deben ser cubiertos por los controles generales	Supervisión y control de las líneas de defensa
Moderados	Requieren controles preventivos robustos	Exigen pruebas de efectividad frecuentes (data analitycs/ inteligencia artificial)
Altos	Demandan controles "detectivos" específicos (en adición a los preventivos)	Exigen monitoreo permanente (24 * 7 – 365) Factor crítico: TECNOLOGÍA

Detección de incidentes

Respuesta

- Gestión de contingencias
- Investigación (y enforcement)
- Remediación

Asignación de recursos inmediata

Sistemas/ mecanismos de inteligencia para detección de amenazas

Sistemas de gestión de reclamos

Programa de identificación de vulnerabilidades

Sistemas de denuncias internas

CULTURA DE PREVENCIÓN

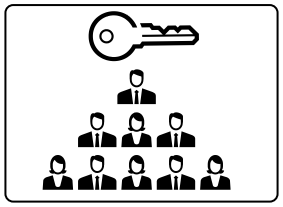
EDUCACIÓN A USUARIOS - CLIENTES

TECNOLOGÍA – HABILIDADES TÉCNICAS - PRESUPUESTO

Tendencias

- **Fraude interno**

Característica general se mantiene:



Abuso de la posición de confianza mediante la explotación de vulnerabilidades identificadas como consecuencia de la ejecución de la propia función.

Variable nueva:

"surgimiento de súper usuarios"

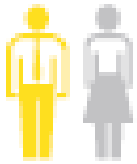
¿Inmigrantes digitales controlando a nativos digitales?

Inmigrantes digitales vs. Nativos digitales

Tendencias

➢ Fraude interno

- Menor número de casos
- El monto promedio es alto (depende del nivel ejecutivo involucrado)
- Existe un grupo importante de casos que no son detectados o se detectan en promedio 31 meses (*) después de iniciados.



38% (de casos de fraude interno) los empleados actuaron en **colusión con terceros**

33% (de casos) los defraudadores ocupaban cargos de Gerencia **(76% de nivel de supervisión)**

19% (Casos 2013) La pérdida económica directa en promedio está en el rango entre US$50K y US$100K. **(19% más de US$100K)**

56% de casos los defraudadores tenían entre 1 y 5 años en la compañía **(35 % más de 5 años)**

83% indican que no confían en los controles anti-fraude de sus organizaciones **(42% confía parcialmente.; 15% se siente muy seguro)**

63% señala que los casos se produjeron debido a la falta de controles o su inoperancia (mal diseñados)

Fuente: Estudio de Fraude en el Perú EY 2013

Fuente:
(*) Insider Threat Study: Illicit Cyber Activity. Involving Fraud in the U.S. Financial Services Sector
Carnegie Mellon University

Tendencias (continuación)

- **Fraude externo**

Antes: se presentaban de manera itinerante.
Ahora: pueden ocurrir simultáneamente en diferentes mercados o áreas geográficas.

Mecanismos de inteligencia para la identificación de amenazas

Programas para la detección de vulnerabilidades

Monitoreo de riesgos específicos

Análisis de nuevos productos

Empleo de nuestras líneas de defensa

ciber ataques

Tendencias: Percepción acerca de los ciber ataques

- **Directorios y C- level (conformados por inmigrantes digitales): La competencia por el mercado y un bajo entendimiento de las amenazas desplazan la discusión a un tercer plano. Las razones varían por organización, pero en términos generales tienen origen en los siguientes obstáculos:**

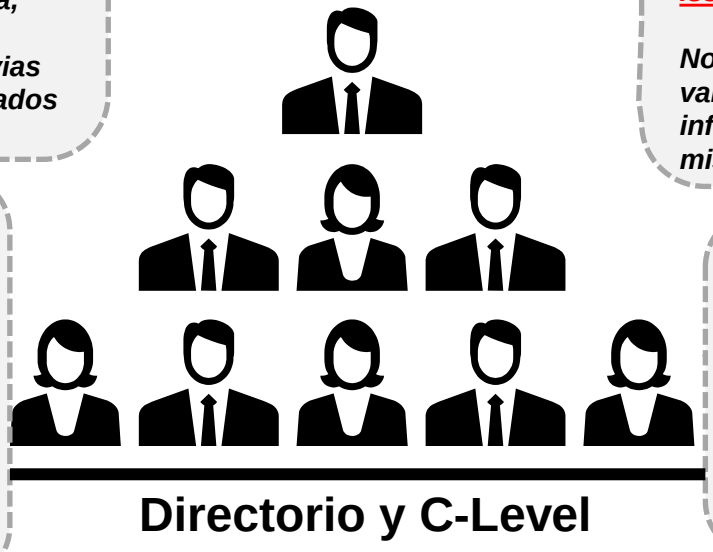
Retorno Invisible (no percibido)
En tiempos como los actuales, es difícil para el management destinar presupuesto, gente y tiempo en este tema, existiendo otras demandas más obvias que generan resultados concretos.

Agenda Recargada:
En tiempos de volatilidad económica, la agenda tiene "otras prioridades".

Es un tema de TI:
Tradicionalmente se considera que la seguridad de la información es un issue de TI,

No se considera el valor estratégico de la información en si misma.

Dificultad para estimar el impacto
Este tipo de amenazas son difíciles de predecir (y evaluar el impacto). El análisis costo beneficio requiere de un enfoque diferente.



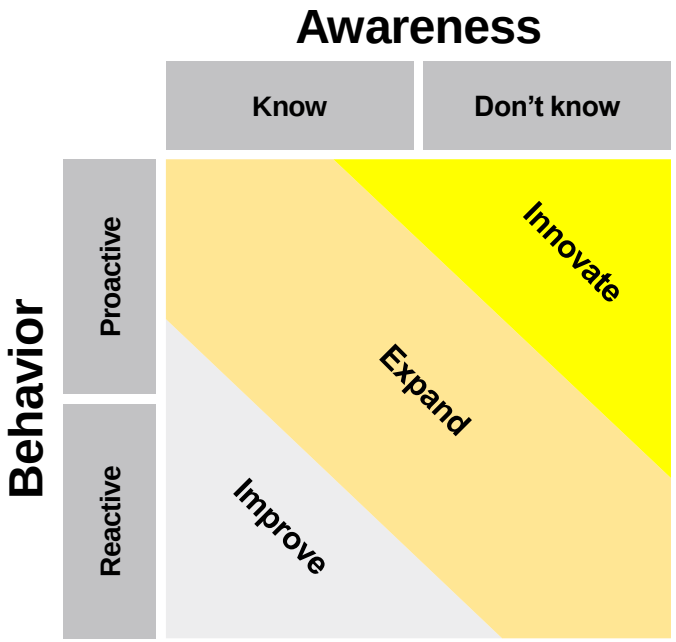
No es nuestro tema
No necesariamente se asocia el hecho que el negocio está basado en data digital para operar y competir.

Fuente: Estudio "Beating cybercrime. Security Program Management from the board´s perspective."
EY – Octubre 2013

Tendencias: “Bajo el Ciber ataque”

“Under cyber attack: EY´s Global Information Security Survey 2013”

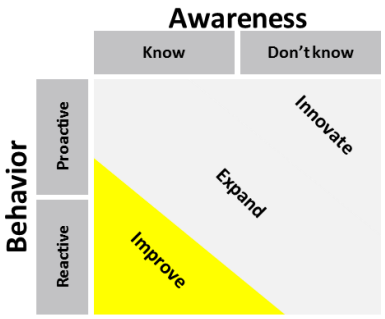
La encuesta explora 3 niveles de respuestas frente al riesgo de **ciber ataques**, en un entorno donde éstos son **numerosos, constantes y cada vez más complejos**:



Fuente: Estudio “Under cyber attack. EY´s Global Information Security Survey 2013”
EY – Octubre 2013

Tendencias: “Bajo el Ciber ataque”

“Under cyber attack: EY´s Global Information Security Survey 2013” – Desagregado para Banking and Capital Markets



Improve

80% de los encuestados considera que la función de seguridad de la información cubre parcialmente las necesidades (4% no cubre, 16% cubre totalmente).

53% indica que la estrategia de seguridad de la información está alineada a su estrategia de negocio (57% a la estrategia de IT)

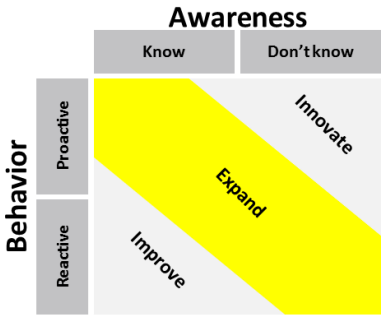
67% señala que el principal obstáculo es la restricción presupuestaria

63% de organizaciones indicaron que la continuidad del negocio y la recuperación ante desastres son sus 2 principales prioridades

“La toma de consciencia acerca de las ciber amenazas es el detonante que debe impulsar la mejora”

Tendencias: “Bajo el Ciber ataque”

“Under cyber attack: EY´s Global Information Security Survey 2013” – Desagregado para Banking and Capital Markets



Expand

Nivel de madurez de 6 áreas claves del Programa de Seguridad de Información

	Innovador	Líder	Promedio	Debajo del promedio	Pobre
Capacidad de identificación de vulnerabilidades	9%	27%	32%	22%	10%
Programa de detección	13%	29%	28%	25%	5%
Programa de identificación y administración inteligente de amenazas	7%	15%	28%	31%	19%
Programa de manejo de identificación y accesos	14%	31%	36%	13%	6%
Programa de protección de datos	23%	40%	21%	13%	3%
Capacidad de respuesta ante incidentes de seguridad de información	6%	71%		17%	6%

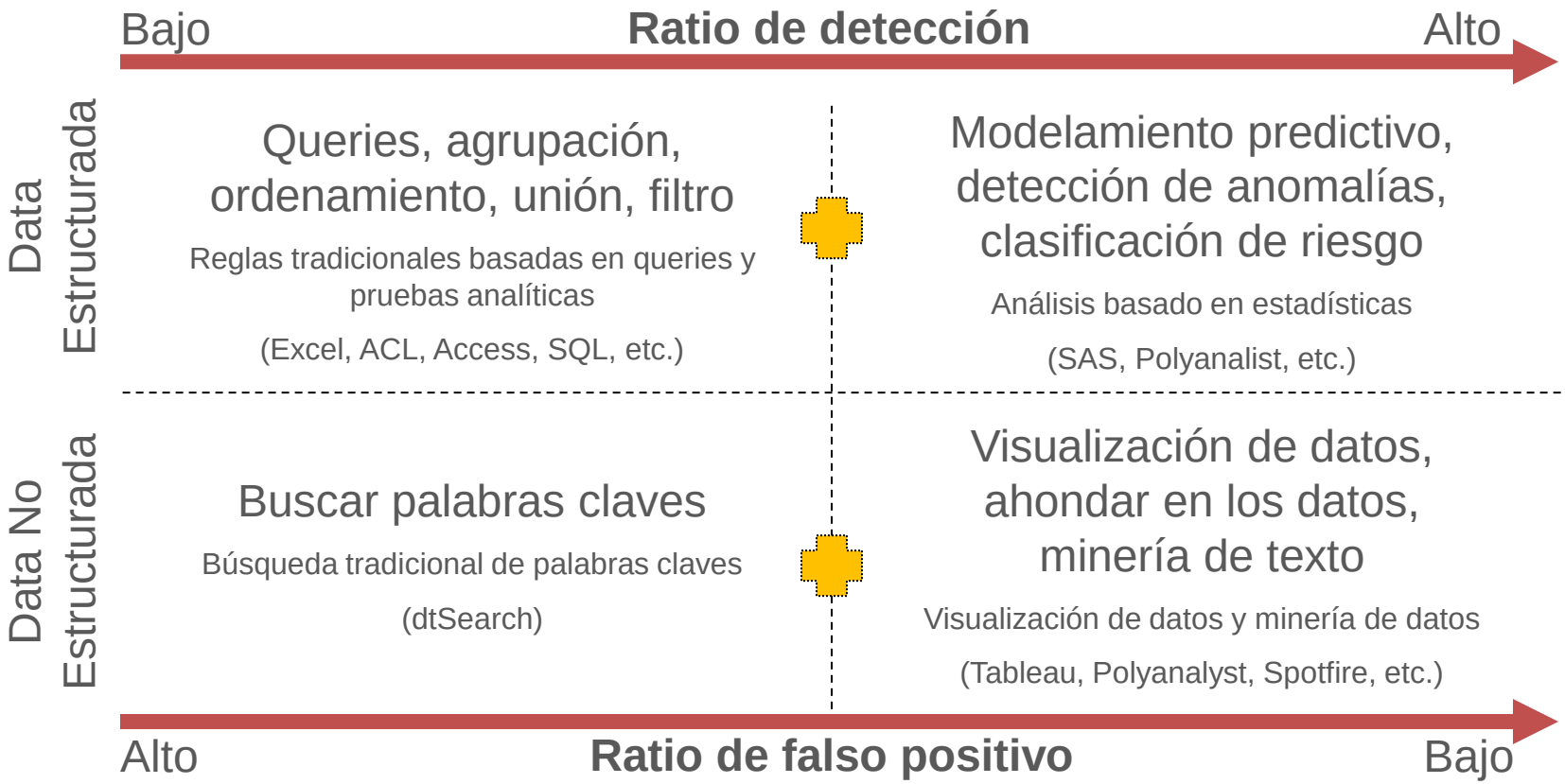
“Cada persona y cada organización es un objetivo. En este momento, su organización puede estar siendo víctima de ciber ataques”

Ejemplo de monitoreo específico: KYT /Know Your Trader – Área de Trading)

"I need a miracle…" (Necesito un milagro)

Ejemplo de monitoreo específico: Área de Trading

De la data estructurada a la no estructurada



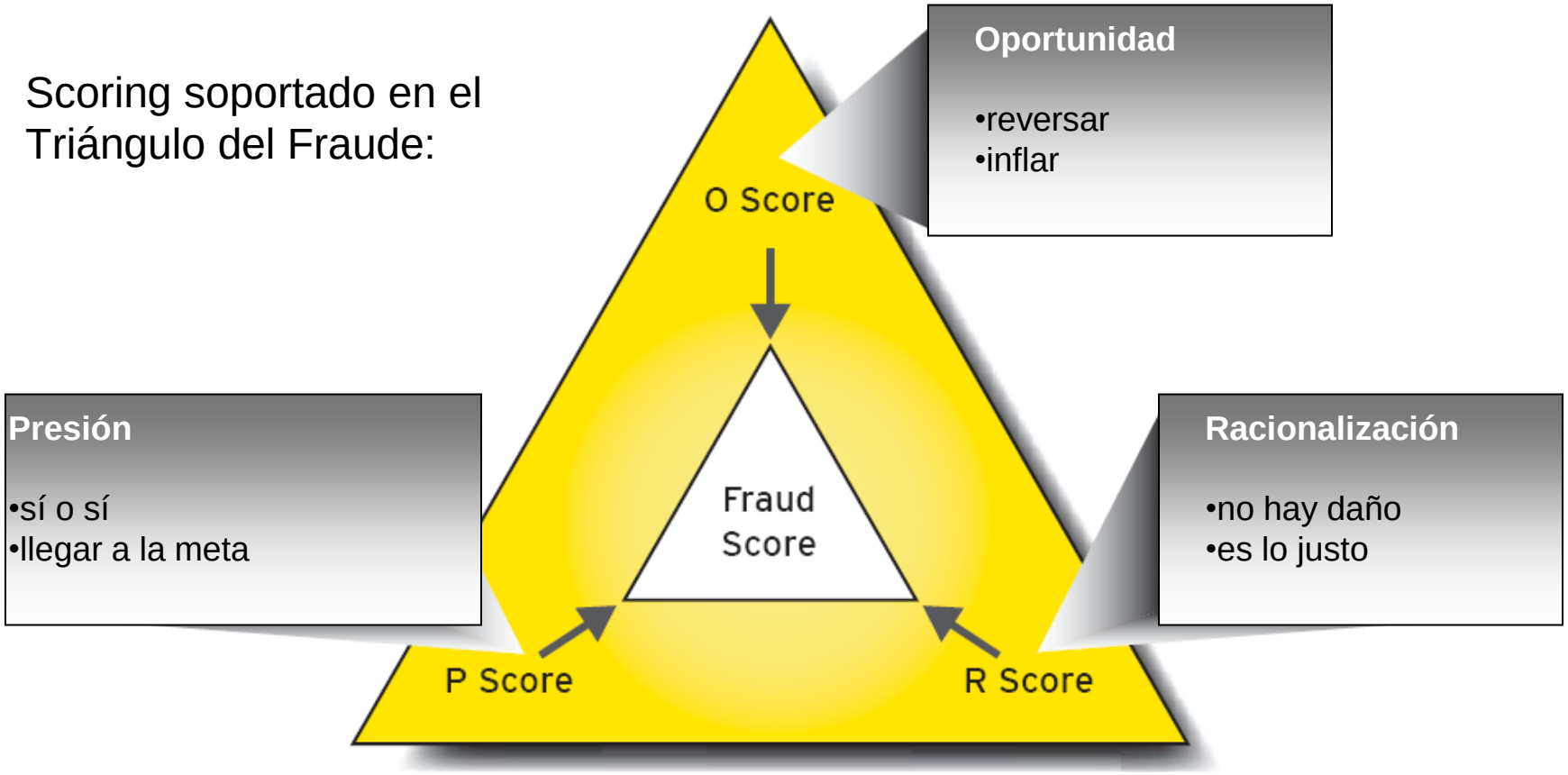
Fuente: Forensic Technology & Discovery Services – Ernst & Young

Ejemplo de monitoreo específico: Área de Trading

Ejemplo de monitoreo específico: Área de Trading

Ejemplo de monitoreo específico: Área de Trading

Scoring soportado en el Triángulo del Fraude:



1. *Donald R. Cressey's "Fraud Triangle" ; Incentive/Pressure, Opportunity and Rationalization are present when fraud exists.*

Ejemplo de monitoreo específico: Área de Trading

de palabras sensibles identificadas producto del análisis de la data no estructurada:

Racionalización

…no se notará

…**por ahora**

…todos

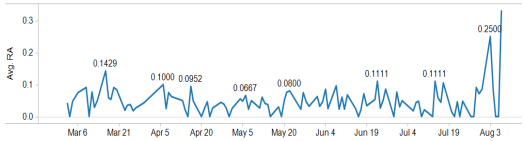
…es temporal

…no hay daño

…no es raro

…es lo justo

…zona



 # de palabras relacionadas como % del total de emails

Incentivo/ Presión

… Sí o Sí

… entre nosotros

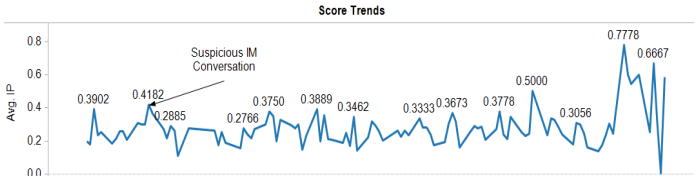
…no me siento cómodo

…no se cómo

…no quiero

…no es correcto

…necesito un milagro



 # de palabras relacionadas como % del total de emails

Oportunidad

…**inflar**

…por fuera

…reversar

…lo mio /

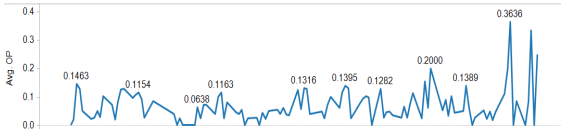
…pedido verbal

…dar en el blanco

…**disminuir**

…arreglar

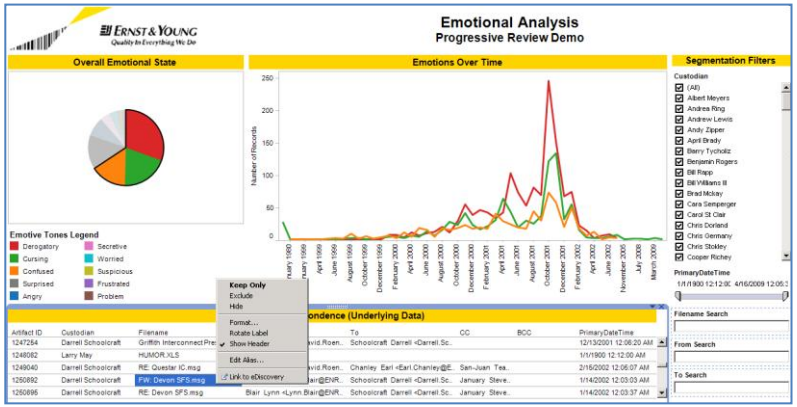
…**aumentar**



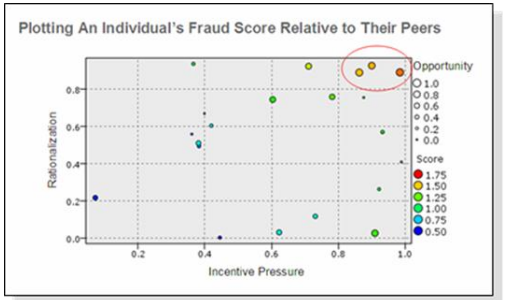
 # de palabras relacionadas como % del total de emails

Ejemplo de monitoreo específico: Área de Trading

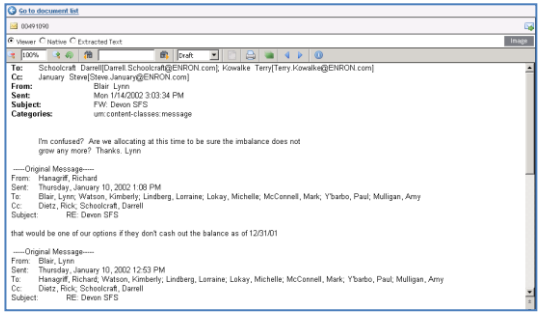
La data es organizada por factores de riesgo asociado para su análisis.
Se establece un modelo de relaciones entre personas, documentos y eventos.



Análisis de la frecuencia de uso de términos sensibles



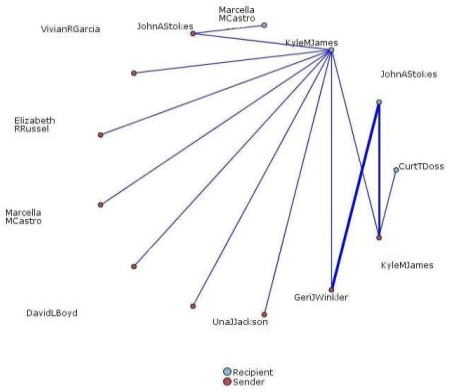
Scoring soportado en el triángulo del Fraude



Análisis de Palabras clave

- ***Identificación de Riesgos***
- ***Clasificación de traders por factores de riesgo***
- ***Conductas anómalas o de riesgo***
- ***Fuga de información***
- ***Documentos (evidencia)***
- ***……***

¿Qué? ¿Quién con quién?
¿En que periodo?



Para tener en cuenta…

"Ausencia de evidencia de casos de fraude no es evidencia de ausencia de fraude"

"La pregunta ya no es "¿si existen?" sino ***"¿Dónde están sucediendo?*** *o* ***¿cuándo sucederán?"***

Contacto: rafael.huaman@pe.ey.com
+ 51 1 411 4443

“La Prevención del Fraude en la Banca desde la óptica del consultor”