XXVI Congreso de Seguridad Bancaria
CELAES 2011

Mejores prácticas de seguridad para prevenirlo y controlarlo

Experiencia y perspectivas del fraude informático en Latinoamérica

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

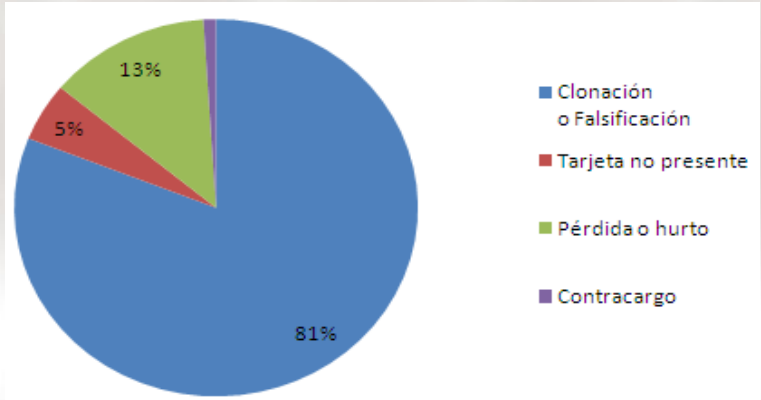
FLORIDA INTERNATIONAL
FIBA
BANKERS ASSOCIATION

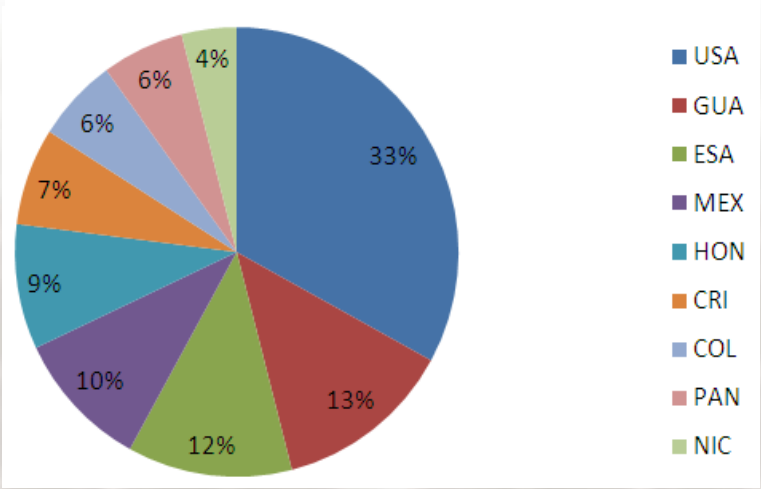
Agenda

1. Experiencia del fraude informático en Latinoamérica
2. Perspectivas del fraude informático en Latinoamérica
3. Mejores prácticas de seguridad en prevención y control del fraude informático

Experiencia y perspectivas

Clonación o falsificación de tarjetas, facilitado principalmente por el uso de programas de código malicioso





Fuente: Informes internos de siniestralidad

Experiencia y perspectivas

Pareto: Pocos vitales, muchos triviales

El 20% de los ataques de seguridad a los sistemas, contribuyen a la generación del 80% de los fraudes informáticos

Clonación o falsificación de tarjetas, facilitado principalmente por el uso de programas de código malicioso

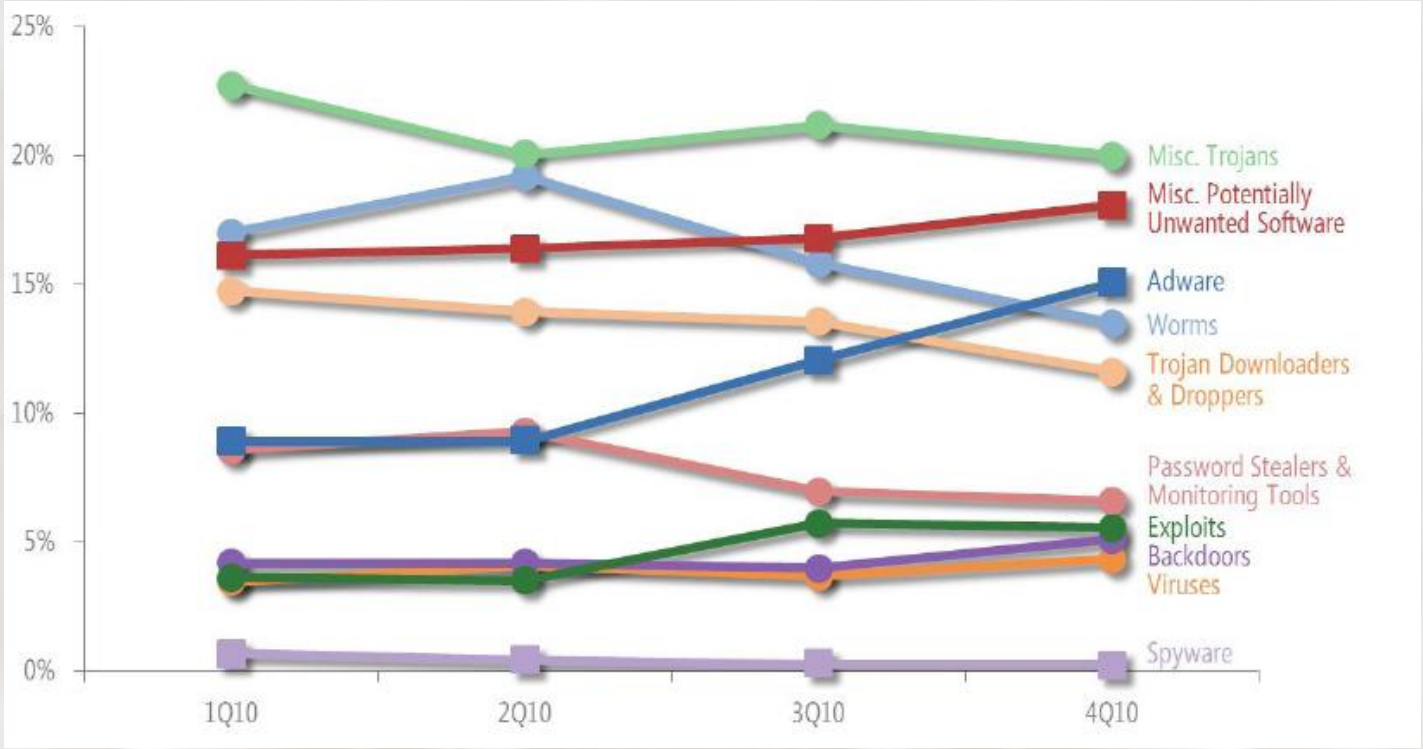
Figura 12. Las ubicaciones con la mayor cantidad de equipos que informan detecciones y eliminaciones por parte de los productos antimalware de escritorio de Microsoft en 2010

	País/Región	1T10	2T10	3T10	4T10	Cambio 3T al 4T	Cambio en 2010
1	Estados Unidos	11.025.811	9.609.215	11.340.751	11.817.437	4,2% ▲	7,2% ▲
2	Brasil	2.026.578	2.354.709	2.985.999	2.922.695	-2,1% ▼	44,2% ▲
3	China	2.168.810	1.943.154	2.059.052	1.882.460	-8,6% ▼	-13,2% ▼
5	Reino Unido	1.490.594	1.285.570	1.563.102	1.857.905	18,9% ▲	24,6% ▲
4	Francia	1.943.841	1.510.857	1.601.786	1.794.953	12,1% ▲	-7,7% ▼
7	Corea	962.624	1.015.173	1.070.163	1.678.368	56,8% ▲	74,4% ▲
6	España	1.358.584	1.348.683	1.588.712	1.526.491	-3,9% ▼	12,4% ▲
9	Rusia	700.685	783.210	928.066	1.311.665	41,3% ▲	87,2% ▲
8	Alemania	949.625	925.332	1.177.414	1.302.406	10,6% ▲	37,1% ▲
10	Italia	836.593	794.099	900.964	998.458	10,8% ▲	19,3% ▲

Fuente: Informe de inteligencia de seguridad de Microsoft, volumen 10

Experiencia y perspectivas

Clonación o falsificación de tarjetas, facilitado principalmente por el uso de programas de código malicioso



Fuente: Informe de inteligencia de seguridad de Microsoft, volumen 10

Experiencia y perspectivas

Cadena de eventos: procesos, tecnología, información, personas

1. Procesos de negocio dinámicos, fuertemente apalancados en tecnología y con oportunidades de mejoramiento en control
2. Gestión del riesgo operativo a nivel alto y medio; con esfuerzos necesarios en integración (tecnológico, de continuidad del negocio, de seguridad de la información) y actualización
3. Tecnología con alto grado de innovación y curva de obsolescencia, vulnerabilidades y fallas de seguridad en los sistemas, retos para actualizar conocimientos sobre su configuración y administración
4. Grandes volúmenes de información, en algunos casos atomizada, con manejo parcial de su ciclo de vida, clasificación incompleta o inexistente y medidas de protección por mejorar
5. “esfuerzos del ser humano por conseguir lo necesario para satisfacer el número siempre mayor y mas variado de sus necesidades, lo cual jamás logrará, pues el hombre es esclavo de necesidades insaciables e infinitas, mientras que la naturaleza es tacaña con sus limitados recursos” (J.M. Ferguson)

Experiencia

Factores externos

1. Procesos amplios y complejos
2. Tecnología al alcance de todos, con “autopistas” para el tránsito de la información, amplias capacidades para el procesamiento electrónico de datos, facilidades para el almacenamiento y transferencia de información
3. Información disponible al instante, en cualquier parte del mundo y con índice alto de volatilidad
4. Personas con fácil acceso para obtener conocimiento especializado
5. En la era de la información y el conocimiento, el talento humano, además del conocimiento individual y colectivo, son un factor clave en la creación o erosión del valor de las organizaciones
6. El poder de las redes sociales
7. La generación del futuro es una generación digital

Experiencia

Factores externos, estrategia del crimen organizado:

1. Conocimiento de los procesos de las organizaciones (vinculación como clientes, uso de “mulas”, ingeniería social)
2. “Inversión” en investigación y desarrollo
3. Mimetización en el espacio virtual y las redes sociales, para afectar la seguridad de los sistemas
4. Ingeniería social y métodos disuasivos o coercitivos para abordar al factor común que:
   - Ejecuta los procesos
   - Crea, accede, modifica y elimina información
   - Administra, opera y proporciona soporte a la tecnología

Perspectivas

1. Masificación de fraudes informáticos orientados a dispositivos inteligentes y Banca Móvil
2. “Mejoramiento continuo” en la combinación de técnicas de ataque, para tener acceso a información confidencial
3. Focalización en información y personal administrados por proveedores y terceros

Mejores prácticas de seguridad

Modelo de Convergencia para Combatir Eficazmente el Fraude

Planes estratégicos

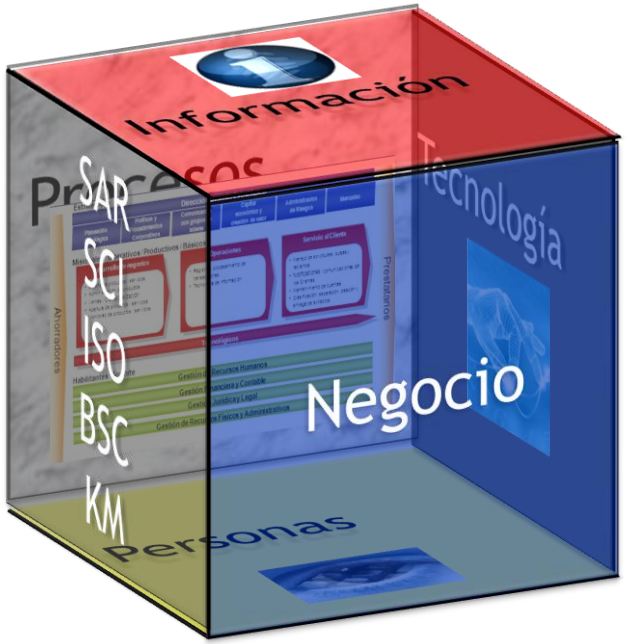
- ***" Conoce al enemigo*** **y conócete a ti mismo; nunca te encontrarás en peligro en cien batallas. Cuando no sabes nada del enemigo pero te conoces a ti mismo, tienes igual probabilidad de ganar o perder. Si no conoces al enemigo ni a ti mismo, puedes estar seguro de estar en peligro en todo combate"**

- **"El excelente general pondera la situación antes de moverse...toma riesgos calculados pero nunca innecesarios"**

- **"Tal vez algunos elementos de su ejército están insuficientemente entrenados, insatisfechos, cobarde o torpemente dirigidos...estas condiciones constituyen vacios y proveen oportunidades para que un general imaginativo diseñe un ventajoso curso de acción"**

Fuente: Libro El Arte de la Guerra de Sun Tzu; traducción de Jaime Barrera, editorial Panamericana.

Modelo del Negocio para la Seguridad



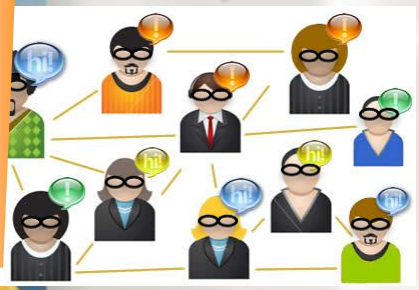
Estrategia antifraude
Visión Helicóptero

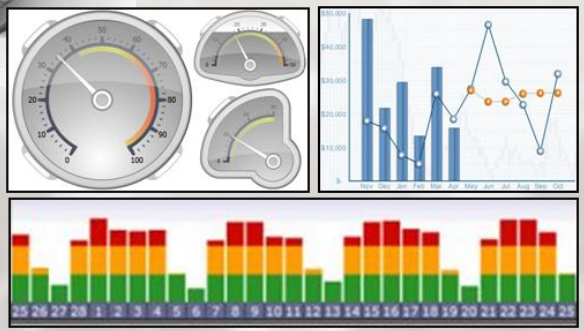
Ahorradores

ZONAS GEOGRÁFICAS

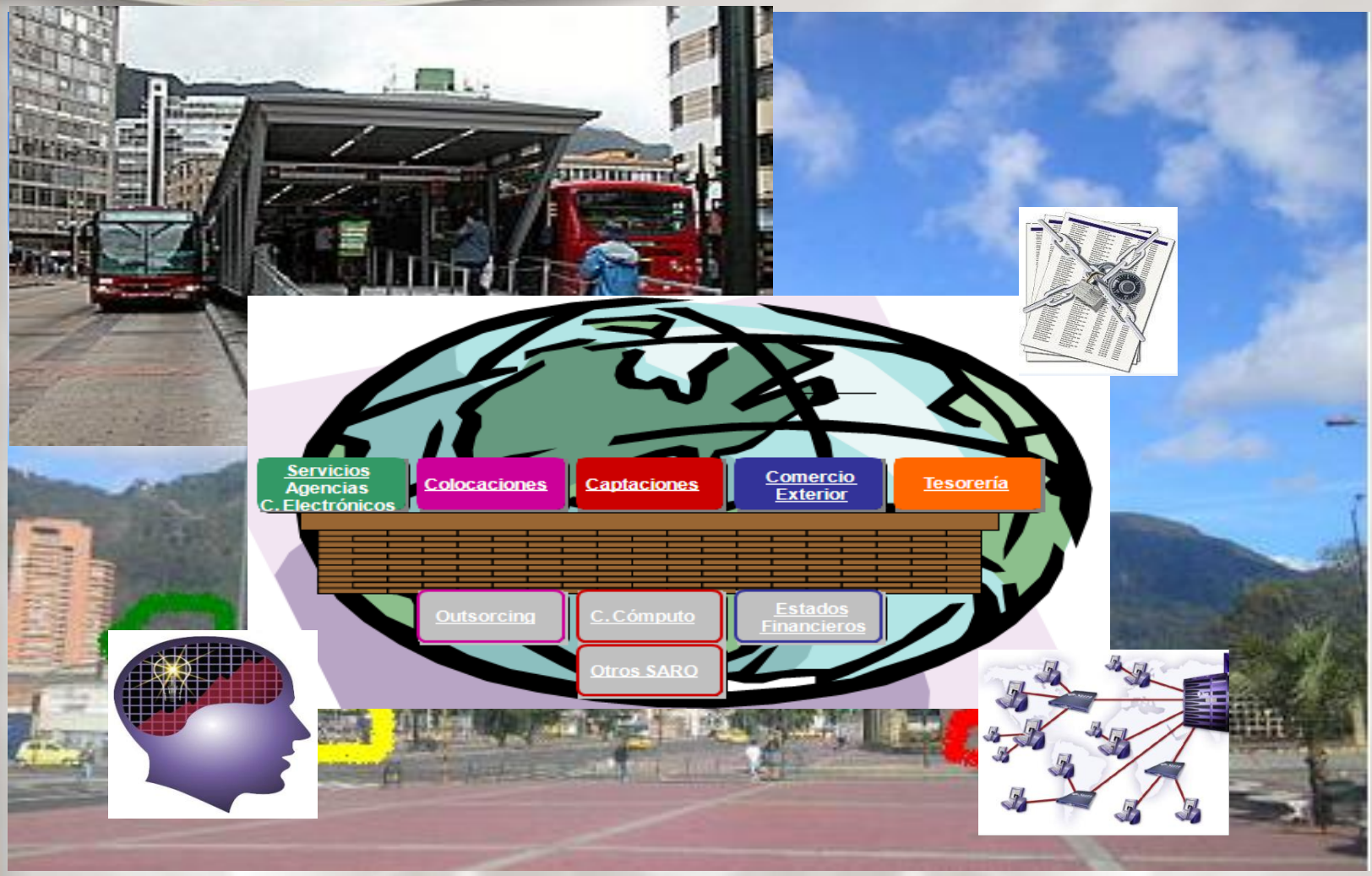
PROCESOS

DEPENDENCIAS

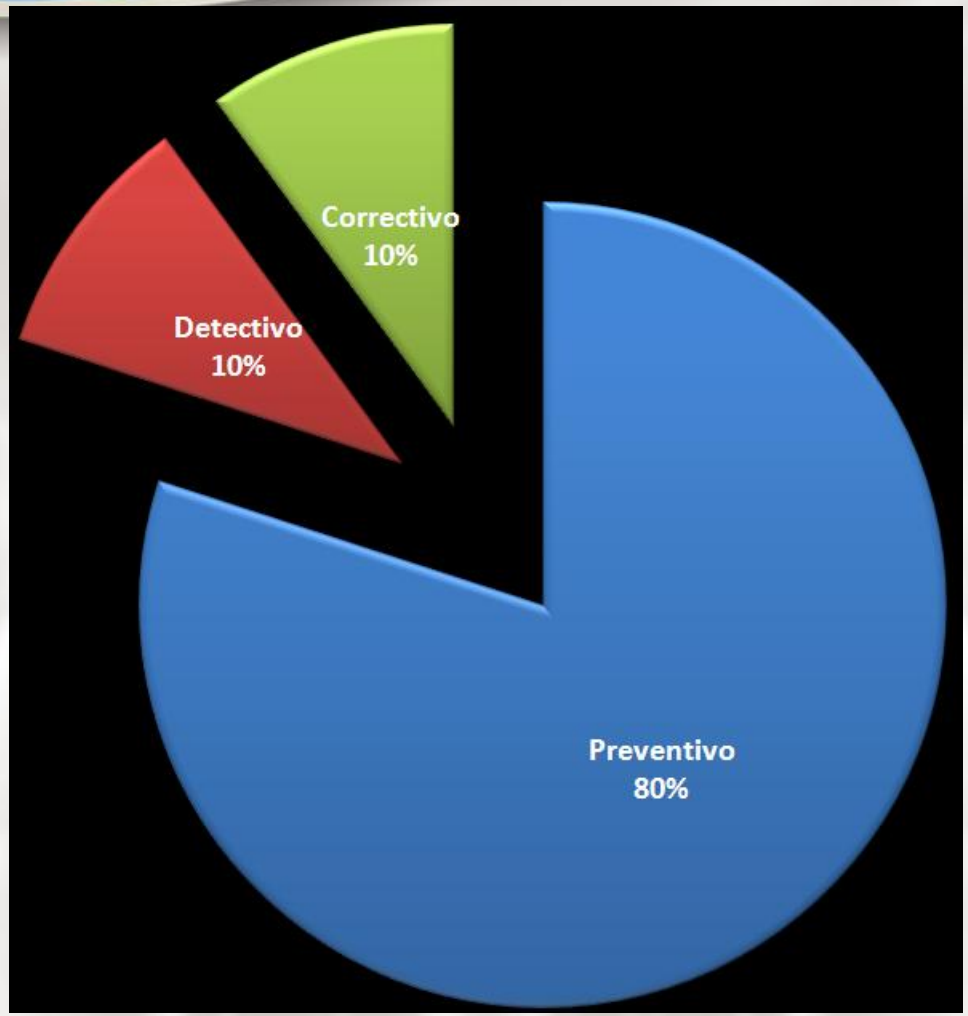




Estrategia antifraude
Dominar el terreno



Estrategia antifraude
Pareto y focalización



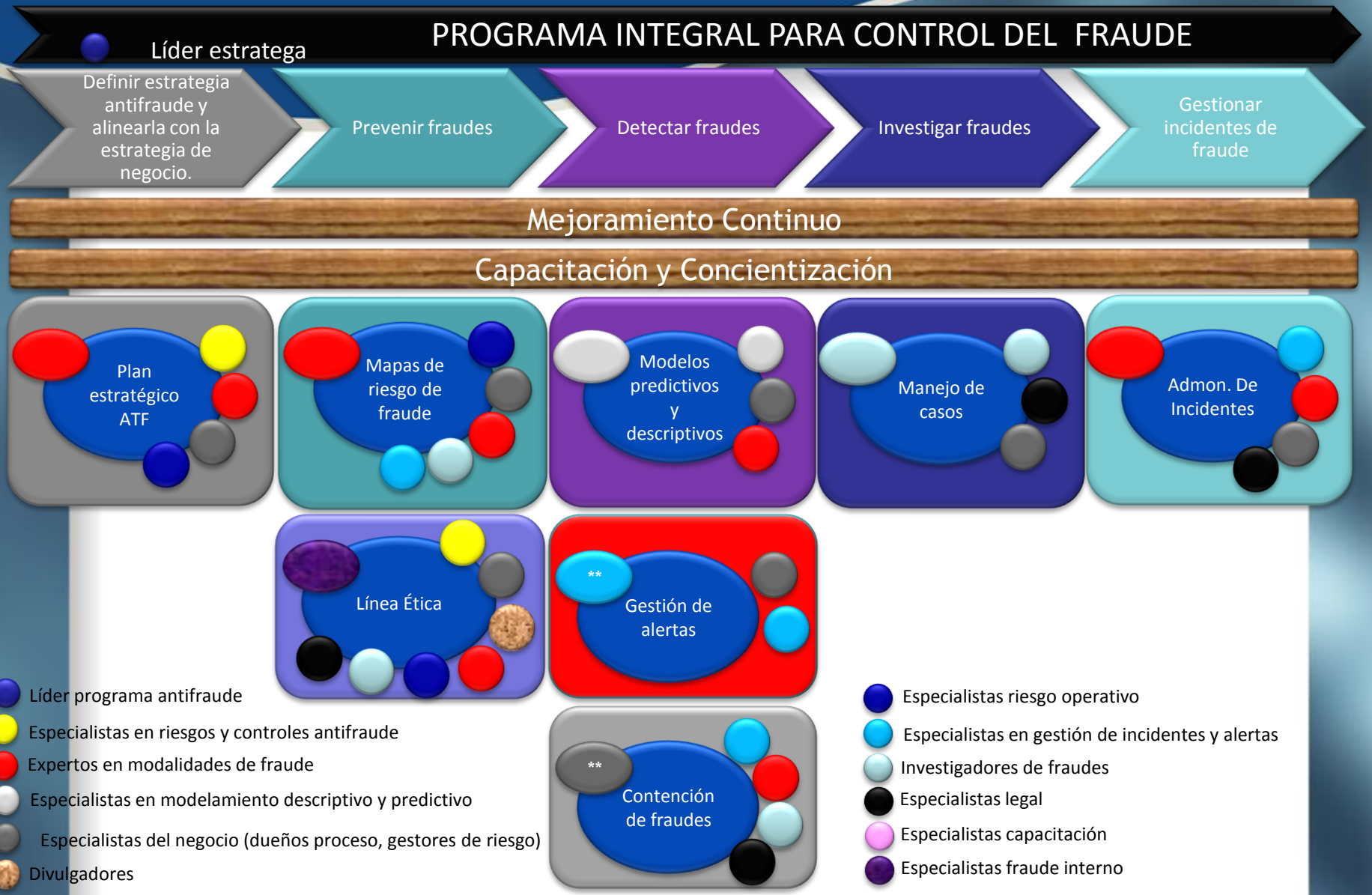
Modelo Lean

Protección de Activos

- Modelo Operativo
- Administración e Infraestructura
- Mentalidad y Comportamiento

Roles y responsabilidades	Inteligencia del fraude
Refuerzo SCI – Labor conjunta	Conocimiento del empleado
Registro y documentación	Medición de resultados
Conocimiento del Cliente	Control de calidad y calibración
Capacitación, entrenamiento, concientización	

Gestión por procesos



** Nombrados por áreas gestoras de alertas

5. Ciclo Control Integral del Fraude

Definición de estrategia

Alinear con la estrategia de negocio.

Análisis de riegos (bajo nivel)

Actualización mapas riesgo de fraude

Validación con todos los actores

Modelos para predecir y detectar

Datos

Extracción, comprensión y preparación de datos

Aplicación de Algoritmos Segmentación / Predicción

Interpretación de resultados

Combinación de reglas

Generación de alertas

Puesta en producción

Control de calidad

Gestión de alertas de fraude

Retro-alimentación y reporte de fraudes

Gestión de incidentes de fraude

Actualización base de conocimiento

Recepción e investigación de fraudes

Actualización base de conocimiento

Seguimiento indicadores de gestión PATF

Capacitación y entrenamiento

Mentalidad y comportamiento

Propuesta de aplicación o mejora de controles

Areas de control

Areas gestoras de riesgo

Dueños de los procesos

Mercadeo

Canales de distribución

Fuerza comercial

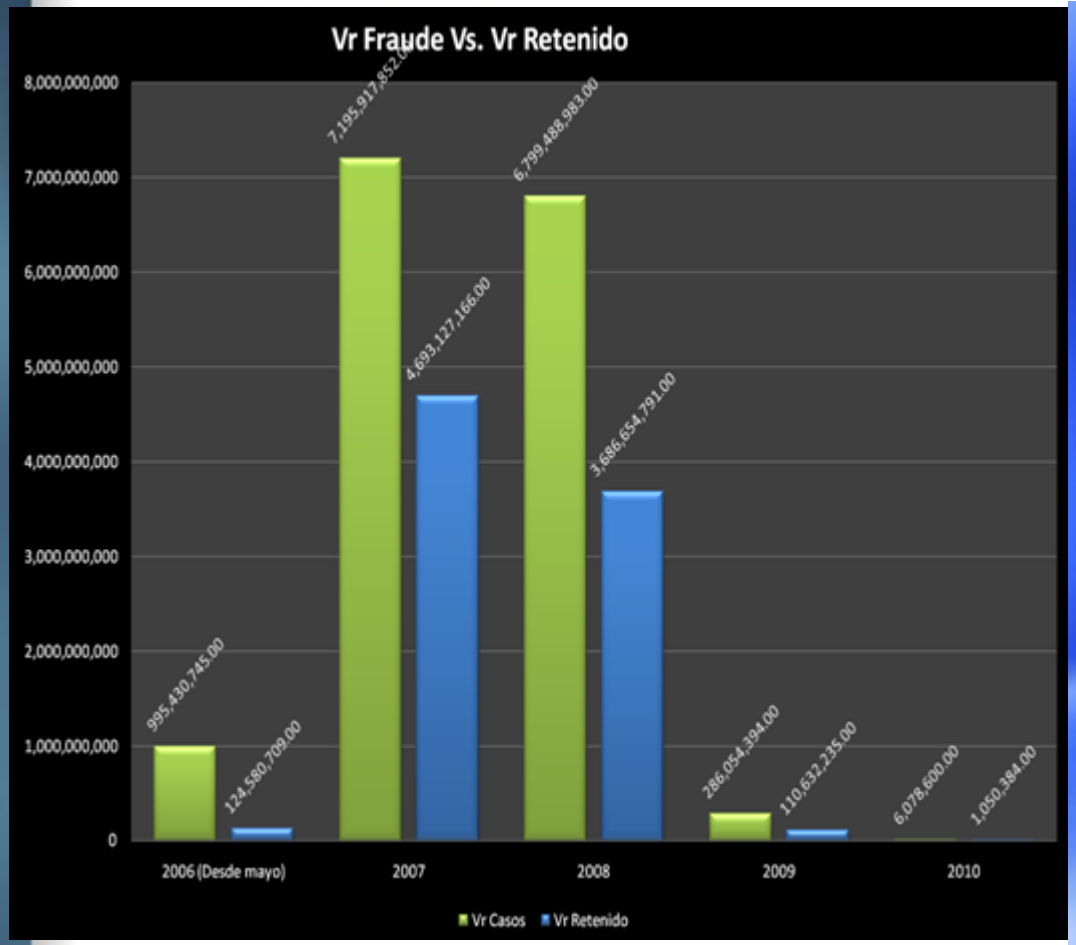
Areas de apoyo

...

CONOCIMIENTO

"La sociedad futura será una sociedad del conocimiento y los trabajadores del conocimiento serán el grupo dominante de su población activa"
Peter F. Drucker, La Gerencia en la Sociedad Futura

Medición de resultados



Lecciones aprendidas

Importante trabajar en:

1. Ejecución de acciones conjuntas y coordinadas entre las áreas de control, la administración, la fuerza comercial y áreas de apoyo
2. Estudio de la naturaleza y evolución de los defraudadores, para actuar con un nivel de conocimiento que permita mejorar la efectividad en la reducción de la siniestralidad
3. Empleo eficaz de los recursos, apoyados en las mejores prácticas y tecnología de punta
4. Acciones concretas e inmediatas, a partir del conocimiento obtenido y los resultados de los indicadores
5. Cultura de personal disciplinado, afianzado en los principios y valores éticos; comprometido con una sociedad mejor
6. Creación de redes de apoyo e inteligencia del delito con autoridades, entidades del sector financiero, sector seguros y demás organizaciones gremiales
7. Principio de especialización, división de tareas, trabajo de equipos multidisciplinarios

Gracias