CELAES
XXXII Congreso Latinoamericano de Seguridad Bancaria
Oct. 5 y 6, 2017 - Quito

asobanca

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Metodología de Gestión del Fraude

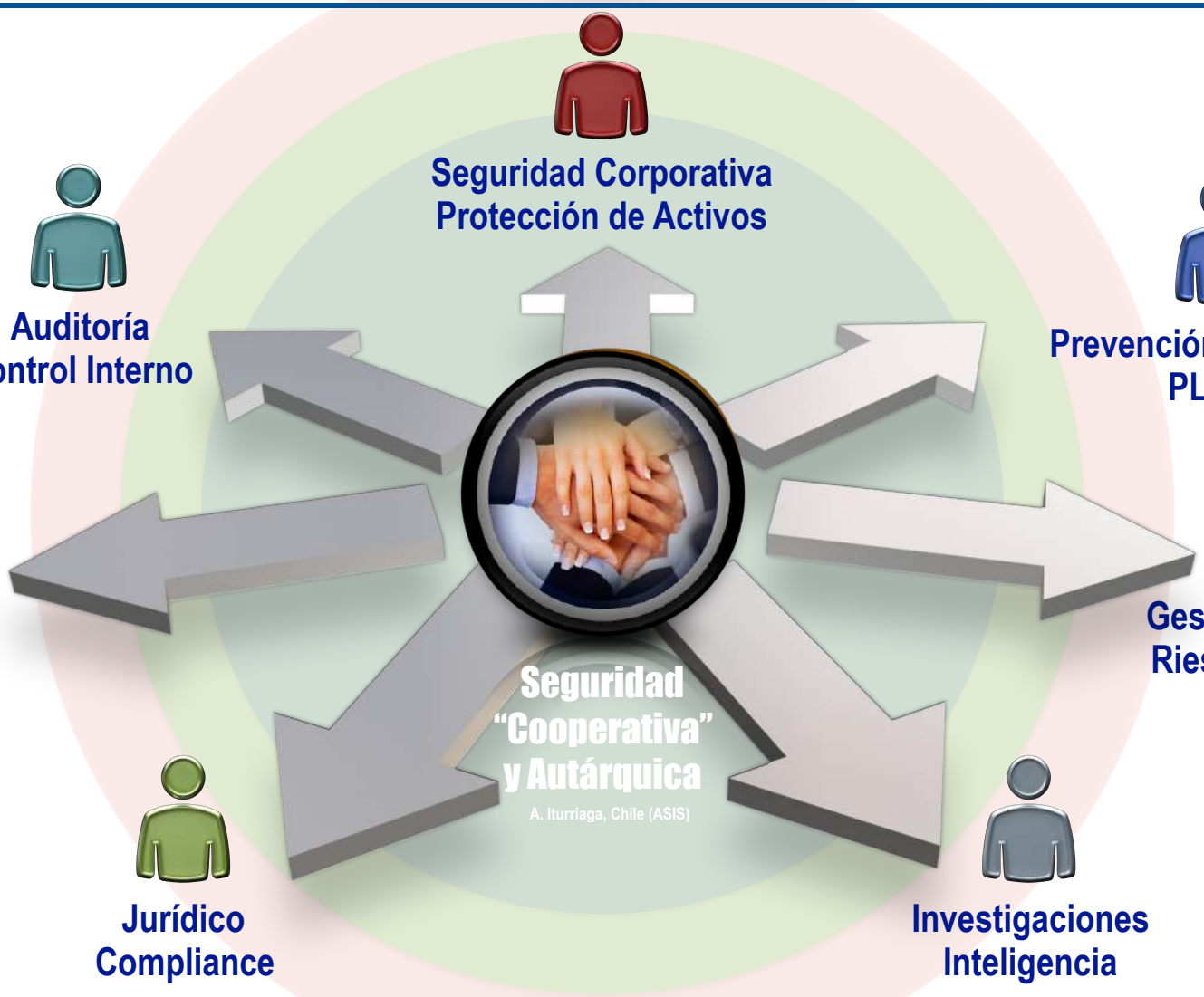
Marco de Referencia

ACFE-COSO

Confianza y Transparencia

Carlos Ramírez, CPP

Comité de Expertos Latinoamericanos en Seguridad Bancaria


Seguridad Corporativa
Protección de Activos
Auditoría
Control Interno
Prevención de Fraudes
PLD/FT
Seguridad de
la Información
Ciberseguridad
Gestión de Riesgos
Riesgo Operacional
Seguridad
"Cooperativa"
y Autárquica
A. Iturriaga, Chile (ASIS)
Jurídico
Compliance
Investigaciones
Inteligencia

Expansión / Septiembre 15, 2017: ACFE; PwC; EY

FRAUDE

Definición práctica

Cualquier **acto intencional** u **omisión** diseñado para **engañar** a otros, **ocasionando pérdidas** a las víctimas y que el **perpetrador** obtenga una **ganancia**.

ACFE

Association of Certified Fraud Examiners

- Surge en **1988** con sede en **Austin**, TX.
- Misión: **reducir** la incidencia de **delitos** de **Cuello Blanco**; prevenir y detectar **FRAUDES**
- Miembros en el mundo: **80,000**

COSO

Committee of Sponsoring Organizations

- Surge en **1987** y resurge en **1992**. EUA
- Misión: **Fortalecer** el Control Interno y la GRE
- Lo integran **5 asociaciones de Auditoria**

Video cápsula

Año 4000 antes de Cristo

En Atenas, un **ciudadano pobre** o un **esclavo** era capacitado y forzado a trabajar como **Contador**.

Los atenienses **preferían** a los **esclavos** como **auditores** porque podían ser **torturados** en el potro de los tormentos y los hombres libres **no**…*

Año 1500 después de Cristo

El matemático italiano **Luca Paccioli** inventó el **cálculo de probabilidades** y mejoró el **método contable de partida doble:**

- No hay **deudor** sin **acreedor**
- Todo el que recibe **debe** a la persona que **da**
- Toda **pérdida** es deudora y toda **ganancia** acreedora

*The Reckoning: Financial Accountability and the Rise and Fall of Nations, Jacob Soll, Basic Books, 2014.

1973

El **Consejo de Estándares de Auditoria** emite la primera **Declaración de un Estándar de Auditoría** (SAS)
"…Un auditor NO tiene responsabilidad respecto de los fraudes…" (¿?)

1977

El **Consejo de Estándares de Auditoria** utiliza el *eufemismo* "**irregularidad**" en lugar de la indeseable palabra "**fraude**" (¿?)

1986

El gobierno norteamericano después de escuchar **muchas quejas** sobre la calidad de los **reportes de auditoria** de firmas independientes, **amenaza** con **eliminarlas** si no mejoran la calidad

1987

Las firmas independientes **reaccionan** y son lideradas por **KPMG** quien emite un reporte con **25 recomendaciones**. Varias siguen siendo vigentes. Ej: **capacitación profesional** en **prevención**

1992

COSO cambia su **enfoque** de **prevención y tratamiento del fraude** por el de precisión en el reporte de la contabilidad financiera y emite el **Marco Integrado de Control Interno** con 5 componentes

1997

El **Consejo de Estándares de Auditoria** emite el estándar SAS 82 donde por **fortuna** llama al "**fraude**" **FRAUDE** en lugar de la confusa palabra "**irregularidades**"

Se reconoce el valor que aportan los "whistleblowers"

2001 y 2002

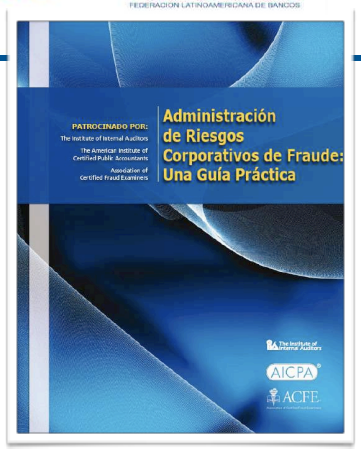
Escándalos por fraude en **ENRON** y **WorldCom** trascienden fronteras y por **malas prácticas de auditoria** desaparece la firma **Arthur Andersen**. El **Congreso** de USA aprueba la **Ley SOX** y se fortalece el marco COSO

2004

COSO emite un **nuevo** Marco de Referencia, ahora de **Gestión del Riesgo Empresarial** (ERM). De 5 componentes ahora emite 8, pero **NINGUNO** con énfasis en la prevención del **FRAUDE** (¿?)

2007

Un equipo especial de trabajo patrocinado por **ACFE** y las firmas Auditoras publican **"Gestión de Riesgos Corporativos de Fraude. - Una Guía Práctica"**, estableciendo **"criterios comprobables"**



2013

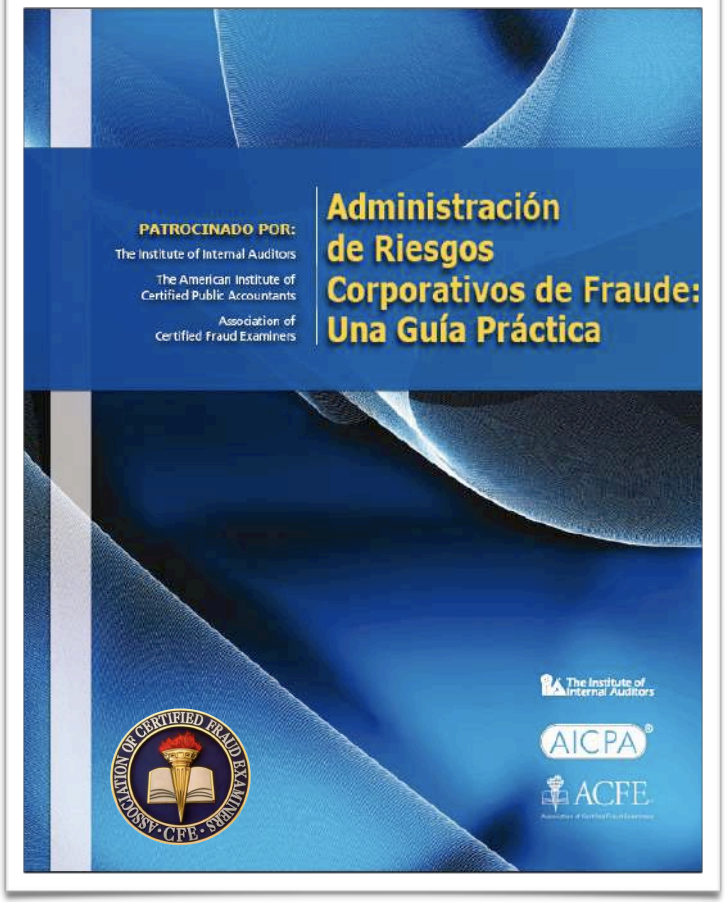
COSO **actualiza** su Marco de Referencia e incluye 17 "principios". El **PRINCIPIO 8** adquiere mucha atención en el **mundo financiero**: **La organización debe considerar la posibilidad de fraude en la evaluación de riesgos para lograr sus objetivos**

2016

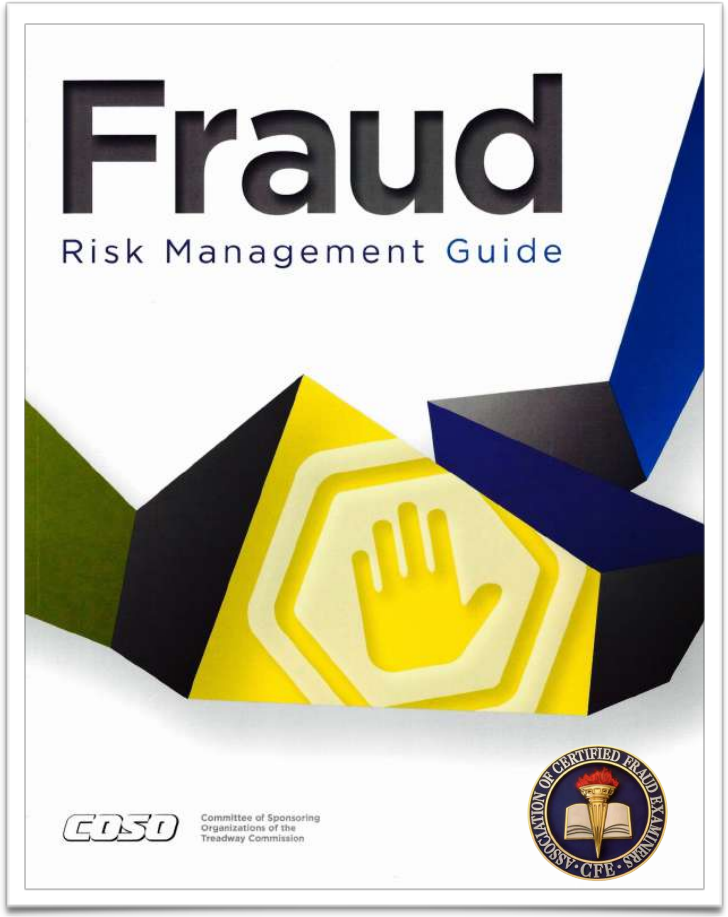
ACFE y COSO **integran** un equipo especial de trabajo para guiar la preparación y **desarrollo metodológico** de la **evaluación de riesgos de fraude.**
Publican: **The ACFE-COSO Fraud Risk Management Guide en Septiembre 2016**

2017

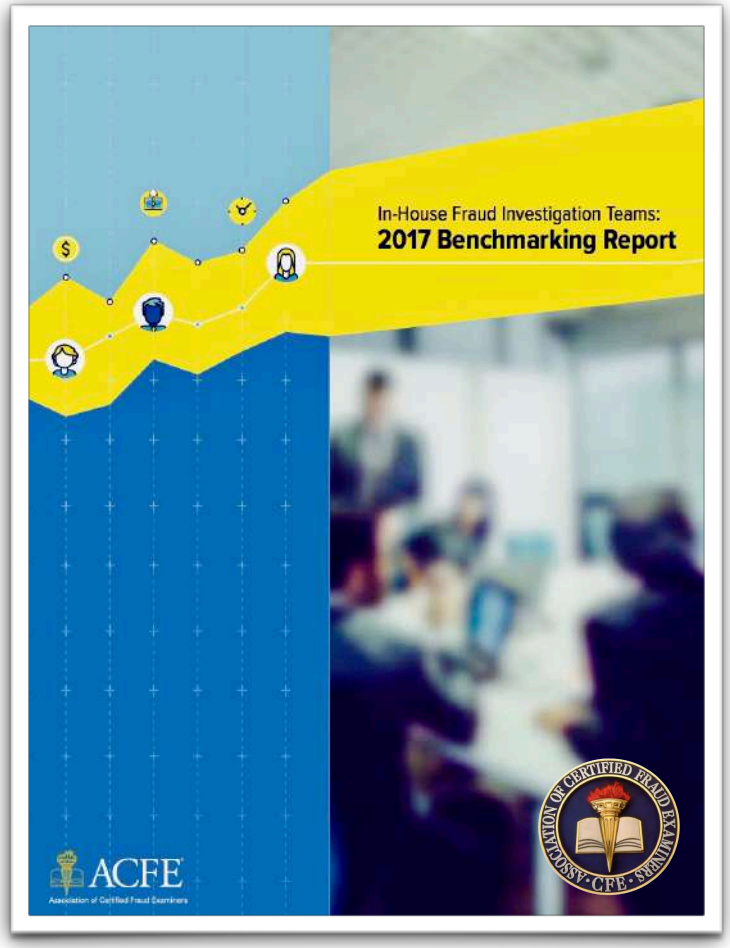
Comienza una **campaña global** para difundir en los sectores **financieros** y empresariales, la **necesidad** y la **importancia** de que las organizaciones realicen **Evaluaciones del Riesgo de Fraude**


PATROCINADO POR:
The Institute of Internal Auditors
The American Institute of Certified Public Accountants
Association of Certified Fraud Examiners
Administración de Riesgos Corporativos de Fraude: Una Guía Práctica
The Institute of Internal Auditors
AICPA
ACFE

2007


Fraud
Risk Management Guide
COSO
Committee of Sponsoring Organizations of the Treadway Commission

2016



2017 Benchmarking / Equipos
INVESTIGACIÓN DE FRAUDES

1485 Respondientes
104 países y 22 industrias
386 Bancos = 26%
207 Sector Público = 14%
148 Aseguradoras = 10%

Bancos +10 mil empleados
59 Investigadores Corporativos

Bancos 1,000 a 9,999 empl.
10 Investigadores Corporativos

Área de Reporte
Auditoría……..25%
Compliance….10%
Legal……..08%
Seguridad…….07%
Riesgos…….06%

51% de Investigadores
< 5 casos en promedio

60% de Investigadores
cierran casos en 30 días Ⓟ

64% de U. Investigación
No tercerizan investigaciones

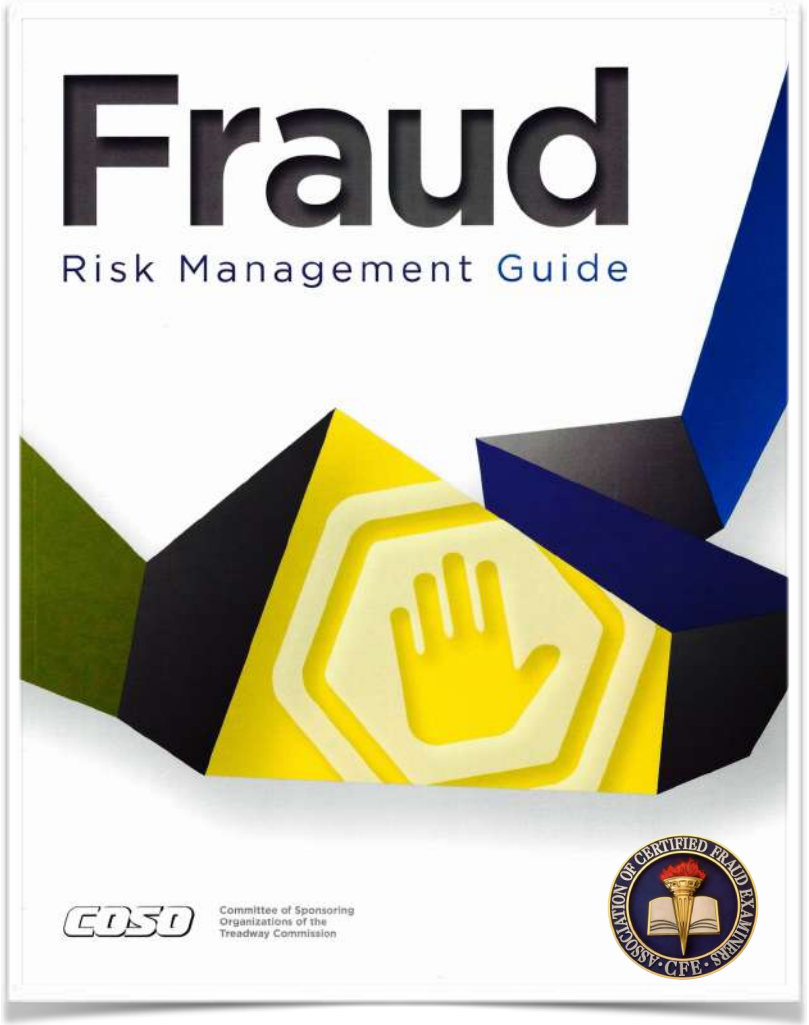
38% de U. Investigación
Usan SW Gestión de Casos

47% de U. Investigación
Usan SW Data Analytics

25% o menos de Bancos
Recuperan pérdidas x Fraude

Top 3 cualidades UI
1 Certificaciones profesionales
2 Experiencia previa
3 Grados académicos

La palabra "Fraude" aparece 2,862 veces en esta obra de 128 páginas



Edición de Septiembre 2016

Proceso de asimilación implantación y consolidación Septiembre 2017

Marco de referencia COSO

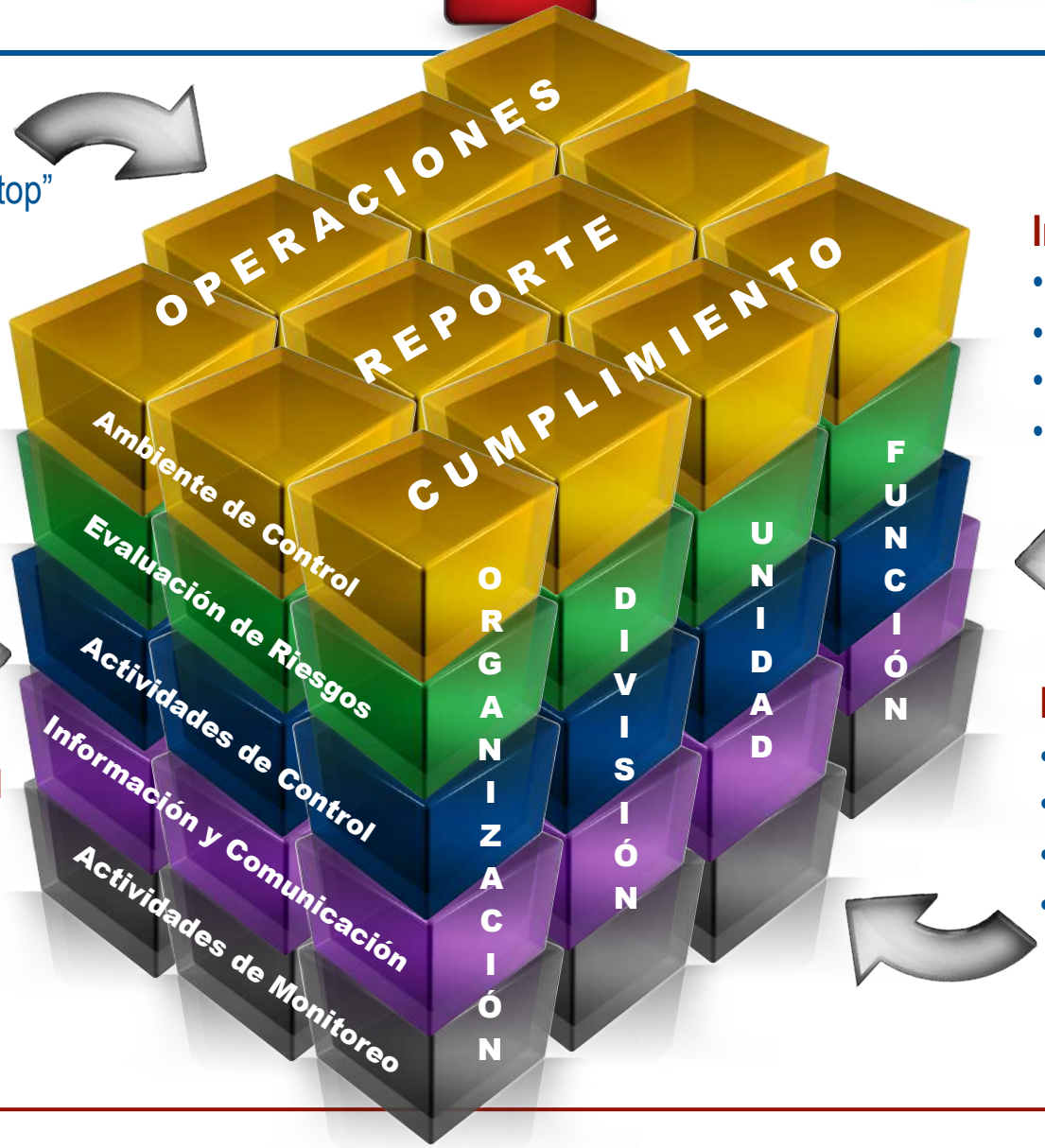
Después de enfocarse en los errores "no intencionales" y en las inexactitudes por más de 20 años, AHORA se les ha señalado a los usuarios que DEBEN fijar su atención en las "inexactitudes intencionales", así como en la malversación y desvío deliberado de activos: FRAUDE.

Cubo COSO

Ambiente de Control
- Filosofía "Tone at the top"
- Infraestructura ética
- Accountability

Evaluar Riesgos
- Identificación
- Análisis
- Mitigación
- Tratamiento

Actividades de Control
- Políticas
- Procedimientos
- Segregación
- Seguridad



Info. y Comunicación
- Correcta
- Completa
- Segura
- Oportuna

Monitoreo
- Supervisión
- Seguimiento
- Auditabilidad
- Trazabilidad

La Guía de Gestión del Riesgo de Fraude señala que…

Los grandes fraudes…

- han llevado a la **caída** de organizaciones enteras
- pérdidas **masivas** de activos y de inversión
- costos **legales** significativos
- **encarcelamiento** de personas clave
- **erosión** de la **CONFIANZA**
  - en los mercados de capitales
  - el gobierno
  - las entidades sin fines de lucro

La Gestión del Riesgo de Fraude…

Es un **componente integral** del **GOBIERNO CORPORATIVO**, del ambiente de **control interno** y de la **SEGURIDAD INSTITUCIONAL**.

Enfatiza que la gestión del riesgo de fraude es una cuestión tanto para los **consejos de administración** como para la **alta dirección**.

Recomienda que cada organización establezca un **programa integral** de gestión del **RIESGO DE FRAUDE**

La guía incluye herramientas y recursos para realizar una evaluación de riesgos de fraude, redactar una política antifraude y cómo establecer un programa integral anti-fraude

Fraude: conducta ilícita patrimonial no violenta (delito de cuello blanco)

La Guía Anti-fraude expande las categorías

Reportes financieros fraudulentos

Cualquier declaración equivocada **intencional**

Reportes no financieros fraudulentos

Informes falsos o dudosa calidad de la seguridad o de **métricas** operacionales **alteradas**.

Aprovechamiento indebido de activos

Por **empleados**, **clientes**, **proveedores**; **organizaciones criminales**: **Robo Interno; Facturas Falsas de Proveedores; Reclamaciones Falsas de Clientes; CIBER ATAQUES.**

Corrupción y otros comportamientos ilícitos

Violación de leyes y regulaciones gubernamentales de impacto directo o indirectos en reportes financieros. Sobornos, abuso de confianza, uso ilegal de información o de secretos comerciales.

Principio 8 de Control Interno (2013)

La organización DEBE considerar la POSIBILIDAD DE FRAUDE en la EVALUACIÓN DE RIESGOS para el logro de sus objetivos

Ambiente de Control	Evaluación de Riesgos	Actividades de Control	Información y Comunicación	Actividades de Monitoreo
1. **Demostrar compromiso con la integridad y valores éticos**.	6. Especificar objetivos apropiados.	10. Seleccionar y desarrollar un control de actividades.	13. **Utilizar información relevante y de calidad.**	**16. Conducir evaluaciones de supervisión en el transcurso de las operaciones**.
2. Ejercer responsabilidad de supervisión.	**7. Identificar y analizar riesgos.**	**11. Seleccionar y desarrollar controles generales sobre la tecnología.**	14. Mantener comunicación interna.	**17. Evaluar y comunicar las deficiencias.**
3. Establecer una estructura, autoridad y responsabilidad.	**8. Evaluar el riesgo de fraude.**	12. Desplegar políticas y procedimientos.	15. Mantener comunicación externa.	
4. Demostrar competenc	9. Identificar y analizar cambios significativos.			
5. Fortalecer la transparencia rendición de cu				

Principio 8: La organización debe considerar la posibilidad de fraude en la evaluación de riesgos para el logro de sus objetivos

La Guía de Gestión del Riesgo de Fraude se enfoca en 5 aspectos principales para diseñar e implementar un Programa Integral

1 AMBIENTE DE CONTROL
Establecer un Política de Gestión del Riesgo de Fraude, como parte del Gobierno Organizacional

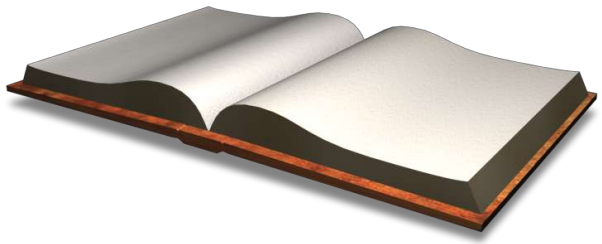
2 EVALUACIÓN DEL RIESGO
Llevar a cabo en toda la organización una evaluación del riesgo de fraude

3 ACTIVIDADES DE CONTROL
Seleccionar, desarrollar y desplegar actividades del control del fraude, preventivas y detectivas

4 INFORMACIÓN Y COMUNICACIÓN
Establecer un proceso de reporte del fraude, así como un enfoque coordinado de acciones de investigación y corrección

5 ACTIVIDADES DE MONITOREO
Monitorear el proceso de gestión del riesgo de fraude, reportar los resultados y mejorar el proceso

1. Establecer una Política de Gestión del Riesgo de Fraude como parte del Gobierno Corporativo



Cuando una organización cae víctima del fraude, los miembros de la Junta del Consejo, casi siempre absorben mucho o la mayoría de la culpa. El compromiso para implementar el proceso de gestión del riesgo de fraude necesita venir del nivel más alto de la organización, idealmente del Gobierno Corporativo. La política sobre la gobernanza del riesgo de fraude:

- Est… …esgo de fraude
- Define pr…
- Establece las condicio…
- Define las políticas de conflicto de int…
- Determina los procedimientos de investigación par…
- Establece una estrategia de auditoria interna
- Explica la revisión, monitoreo y retroalimentación del proceso

2. Realizar en toda la organización una evaluación del riesgo de fraude

Este es el paso más importante de la gestión del riesgo de fraude porque establece las bases para que los siguientes pasos resulten exitosos.

- Seleccionar e inte... equipo de trabajo directivo y ejecutivo para la eval... ...dos de las
- Lo... objetivo de ide... pueden ocurrir los fraudes e...

3. Seleccionar, diseñar y desplegar actividades de control del fraude preventivas y detectivas

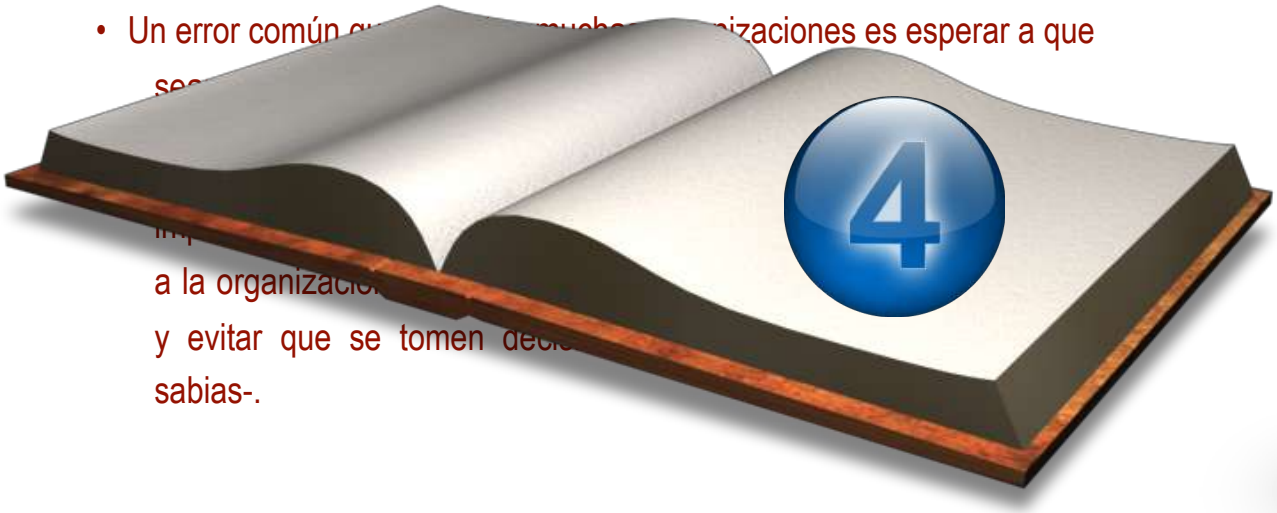
Este paso se enfoca tanto en la prevención como en la detección del fraude respecto al nivel de exposición identificado por el equipo de trabajo ejecutivo que realiza las evaluaciones de riesgo.

- Los procedimi… …ntrol son diseñados para …
  como …

4. Establecer un proceso de reporte del fraude, así como un enfoque coordinado de acciones de investigación y de corrección

Se necesita saber con anticipación qué puede pasar y cómo actuar si el perpetrador de un fraude supera con éxito las barreras preventivas y detectivas que se tienen establecidas en la organización.

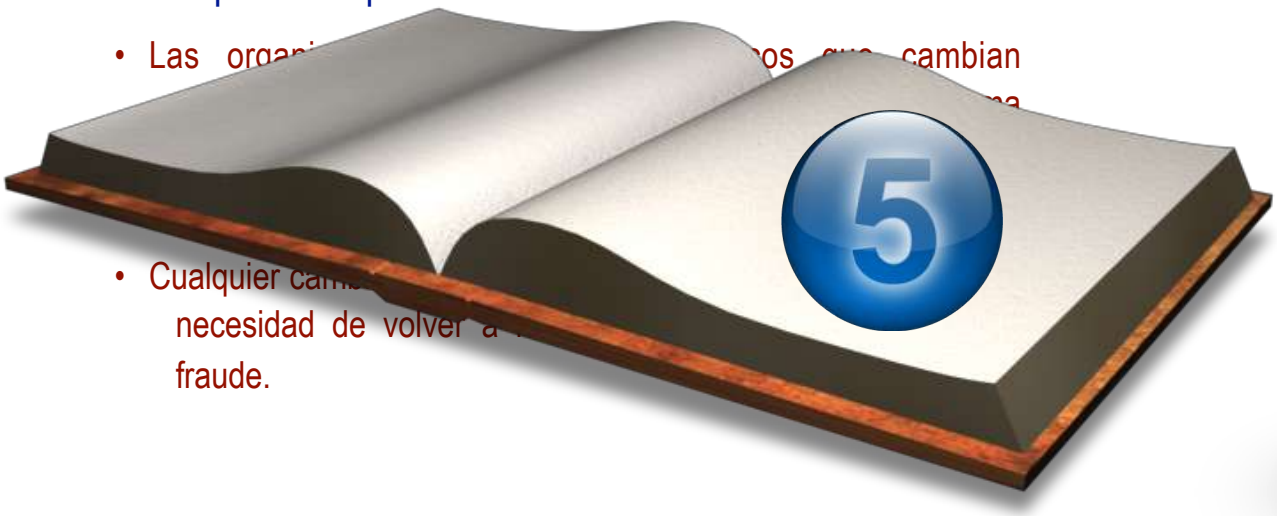
- Un error común q… …izaciones es esperar a que se… …
  …
  …
  a la organizaci… …
  y evitar que se tomen deci…
  sabias-.



5. Monitorear el proceso de gestión del riesgo de fraude, reportar resultados y mejorar el proceso

Tan pronto se realizan e implementan los cambios en los procesos para gestionar el riesgo de fraude en la organización, se debe instaurar un monitoreo continuo de todo lo que esté operando.

- Las organi… …os que cambian …



- Cualquier cam… necesidad de volver a … fraude.

De la Evaluación del Riesgo de Fraude a la GESTIÓN DEL RIESGO DE FRAUDE

Marco de referencia ACFE-COSO

1	2	3	4	5	6
Identificación del riesgo de fraude	Evaluación del riesgo	Tolerancia al riesgo	Fortalecimiento de controles	Plan de respuesta al fraude	Programa Anti-Fraude

Visión

A De la evaluación del riesgo de fraude a la gestión del riesgo de fraude **B** → **C** → **D**

Gestión del Riesgo

Evaluar	Prevenir			Detectar		Responder
Riesgos inherentes de fraude	Riesgos residuales y tolerancia al riesgo	Conocimiento de políticas y capacitación	Cultura "Tone at the Top" y Rendición de cuentas	Procedimientos y controles	Monitoreo y análisis	Reporte confidencial	Investigación Remediación Mejora continua

Código de conducta - cumplimiento y programa de ética

Gestión del desempeño (métricas)

Integración con la gestión de riesgos del negocio

Excelencia operacional

Gobierno de Seguridad


REPORTE A LAS NACIONES
SOBRE EL ABUSO Y EL FRAUDE OCUPACIONAL
Estudio Mundial de Fraude - 2014
2014

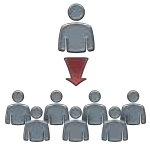

REPORT TO THE NATIONS
ON OCCUPATIONAL FRAUD AND ABUSE
2016 GLOBAL FRAUD STUDY
2016
ACFE

Sistema de clasificación del abuso y fraude ocupacional

El árbol del fraude

- **Corrupción**
  - Conflictos de interés
    - Esquemas de compra
    - Esquemas de venta
  - Soborno
    - Comisiones ilegales
    - Licitaciones manipuladas
  - Agradecimientos ilegales
  - Extorsión económica
- **Apropiación Ilegal de Activos**
  - **Dinero en efectivo**
    - Robo de dinero en efectivo disponible
    - Robo de dinero cobrado
      - Hurto antes de su registro
        - Ventas
          - Sin registrar
          - Sub estimadas
        - Cuentas por cobrar
          - Esquemas cancelación
          - Esquemas traslapo
          - No disimuladas
        - Reembolsos y otros
      - Hurto después de su registro
    - Desembolsos fraudulentos
      - Esquemas de facturación
        - Compañía fantasma
        - Proveedor no cómplice
        - Compras personales
      - Esquemas de nómina
        - Empleados fantasma
        - Salarios falsificados
        - Esquemas de comisión
      - Esquemas de reembolso de gastos
        - Clasificación fraud gastos
        - Gastos inflados
        - Gastos ficticios
        - Reembolsos múltiples
      - Hurto después de su registro
        - Emisor falsificado
        - Endoso falsificado
        - Beneficiario falsificado
        - Emisor autorizado
      - Hurto después de su registro
        - Facturas falsas
        - Reembolsos falsos
  - **Inventario y otros activos**
    - Uso indebido
    - Hurto después de su registro
      - Confiscación y transferencia de activos
      - Ventas y envíos falsos
      - Comprar y recibir con dolo
      - Hurto no disimulado
- **Fraude en Estados Financieros**
  - Sobreestimación de activos / ingresos
    - Diferencias en tiempo
    - Ingresos ficticios
    - Pasivos y gastos ocultos
    - Valuación indebida de activos
    - Revelaciones indebidas
  - Subestimación de activos / ingresos
    - Diferencias en tiempo
    - Ingresos subestimados
    - Pasivos y gastos subestimados
    - Valuación indebida de activos

10 FACTORES DE FRAUDE OBSERVADOS EN LAS PERSONAS	10 FACTORES DE FRAUDE EN EL CLIMA ORGANIZACIONAL
1. Vivir más allá de sus posibilidades	1. Otorgar demasiada confianza a personas clave
2. Un enorme deseo de beneficio personal	2. Falta de proceds. adecuados p/autorizar operaciones
3. Altas deudas personales	3. Divulgaciones inadecuadas de inversiones/ingresos
4. Una relación o asociación inusual cercana con clientes	4. Falta de separación en procesos de autorización
5. Sentir que el sueldo no va de acuerdo con la responsabilidad	5. Falta de controles independientes de rendimiento
6. Actitudes ventajosas personales (“chapucero”)	6. Inadecuada atención a los detalles
7. Actitud desafiante para romper el sistema	7. Falta de separación de la custodia de activos
8. Hábitos excesivos al juego	8. Falta de separación de deberes/funciones contables
9. Presión de grupo o tener otra familia	9. Falta clara de línea de autoridad y responsabilidad
10. No sentirse reconocido en el trabajo	10. Oficinas que no son visitadas por auditoria



Pruebas de cumplimiento y capacitación

Programas de Prevención

Implementación de controles

Incidentes

Publicación

Reporte de incidentes

Análisis

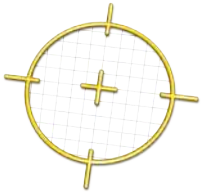
Investigación

ASIS INTERNATIONAL
Advancing Security Worldwide

Modelo Integral de Prevención de Robo y Fraude, Investigación y Programa de Prueba

Resolución

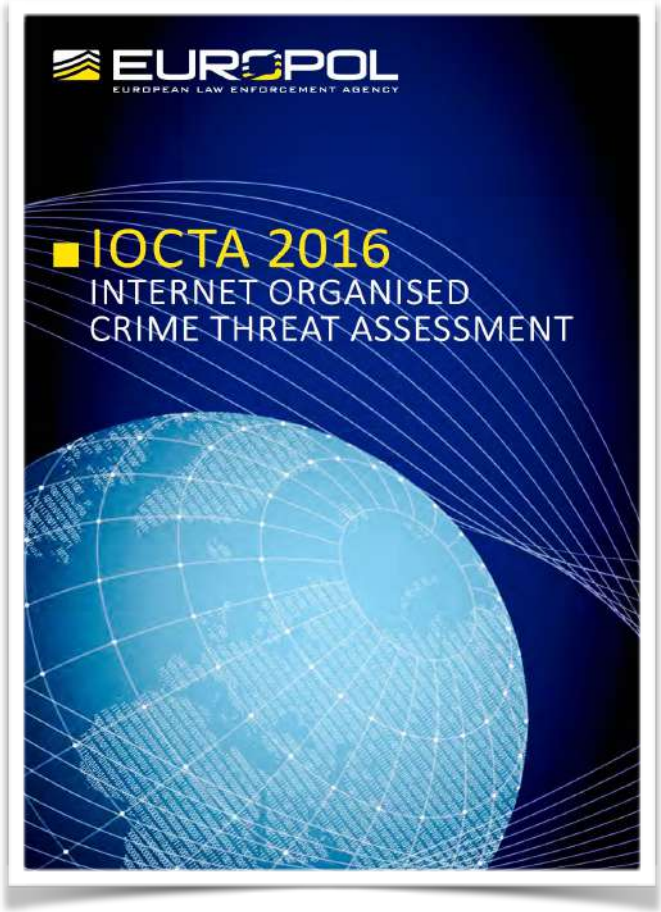
Acción



Certified Protection Professional
Board Certified in Security Management

Video cápsula

Evaluación de amenazas del crimen organizado a la red internet
Centro Europeo vs el ciber crimen EC3



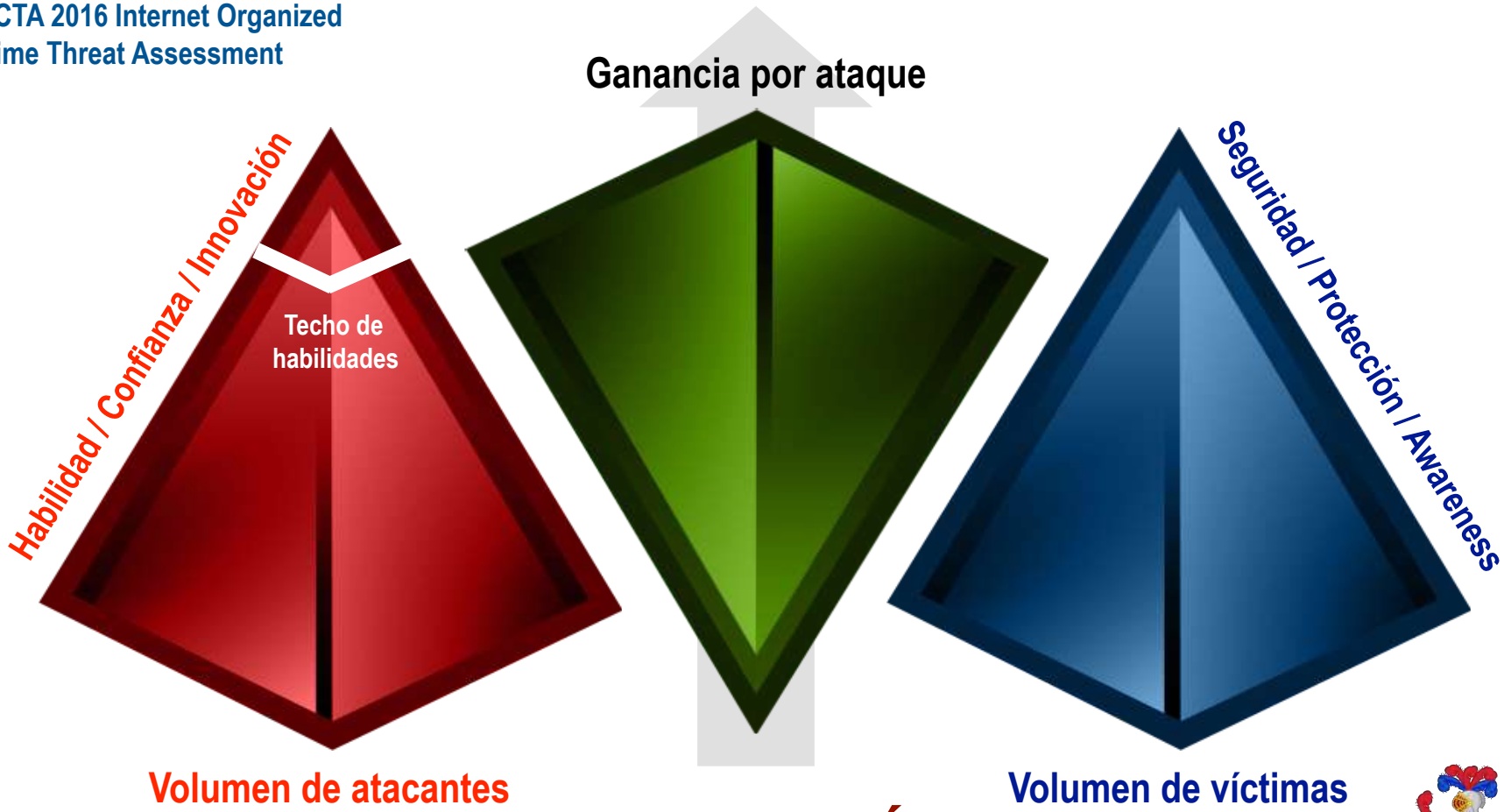
- **2016 Reporte anual en la Unión Europea**
  - Confirma que el ciber crimen es una real amenaza significativa.
  - Riesgos asimétricos *ciber crimen vs víctimas*
    - Crime-as-a-Service
    - Advance Persistent Threat (APT)
    - Darknet
    - Ransonware
    - ATMs malware; Fraud card-not-present (CNP)
    - DDos attacks growing / Attacks agains SWIFT
    - Cryptocurrencies (Bitcoin) remains-cybercrime
    - Growing misuse of anonymity & encryption
- **Tricotomía del ciber crimen:**
  - Awareness - Prevention - Investigation

Tricotomía del Cibercrimen

IOCTA 2016 Internet Organized Crime Threat Assessment

INVESTIGACIÓN

Visión del ciber crimen
Law Enforcement Focus



PREVENCIÓN

Estructuras criminales del ciber crimen

Capacidad económica
Enlaces internacionales

Profesional en derecho
Representa jurídicamente
a los integrantes

Desarrollador
Mercenario informático

Traficante de datos
Enlace con capturistas
Define los objetivos
Enlace lavadores

Lanzan ataques phishing
Instalan malware
Accesos remotos

Enlace con reclutadores
Busca perfiles
Confianza segundo nivel
Comprueba ganancias

Captación de dineros
Reclutamiento de personal

Mulas

Insider (banco)
Filtro de datos

Jefe (s)
Nivel Asesor
Nivel técnico
Nivel operativo
Nivel básico

La Cadena de Compromiso es un modelo que se centra en el usuario para ilustrar como los ciber ataques combinan diferentes técnicas y recursos para comprometer dispositivos y redes

4. Invasión

Fase donde un malware descargable persiste más allá de la infección inicial, a menudo escalando las consecuencias del ataque

I. Incepción

Fase donde un sistema o dispositivo queda expuesto a una amenaza potencial

3. Infección

Fase donde el atacante instala exitosamente un malware descargable

2. Intrusión

Fase donde un atacante gana exitosamente acceso al sistema

Web superficial: 4 %

Nivel 1

Aquí se ubican las páginas más comunes: Google, Bing, Wikipedia

Web Profunda – 90%

Nivel 2

En este nivel se encuentran páginas para descarga de material pirata y fotos con material explícito

Nivel 3

Los “torrents” y descargas masivas son parte de este nivel.

Nivel 4

En este nivel se necesita TOR. Aquí reside la Hidden Wiki y directorios con libros y material de descarga

Nivel 5

Foros Onion Chan, portales con material pornográfico infantil, hackers a sueldo, venta de objetos robados y drogas

Nivel 6

El nivel más clasificado y restringido: “Fosa de las Marianas”. Aquí están redes de gobierno secretas (EUA)

Web obscura: 6 %

Sitios encriptados TOR / Otros

Carlos Ramírez

Video cápsula

Usuarios de Internet en el mundo (Junio 2017)

INTERNET USERS AND 2017 POPULATION STATS FOR THE AMERICAS						
REGIONS	Population (2017 Est.)	% Pop. America	Internet Users Latest	% Population (Penetration)	% Users America	Facebook 30-June-2017
North America	363,224,006	35.9 %	**320,059,368**	88.1 %	44.2 %	263,081,200
South America	426,548,298	42.2 %	**278,596,721**	65.3 %	38.5 %	257,242,500
Central America	177,249,493	17.5 %	**105,771,952**	59.7 %	14.6 %	102,760,000
The Caribbean	43,806,854	4.3 %	**19,900,490**	45.4 %	2.7 %	10,972,840
TOTAL THE AMERICAS	**1,010,828,651**	**100.0 %**	**724,328,531**	**71.7 %**	**100.0 %**	**634,056,540**
Rest of the World	6,508,200,319	86.6 %	**3,161,239,088**	48.6 %	81.4 %	1,345,646,990
TOTAL WORLD	**7,519,028,970**	**100**	**3,885,567,619**	**51.7 %**	**100.0 %**	**1,979,703,530**

WORLD INTERNET USAGE AND POPULATION STATISTICS
JUNE 30, 2017 - Update

World Regions	Population (2017 Est.)	Population % of World	Internet Users 30 June 2017	Penetration Rate (% Pop.)	Growth 2000-2017	Internet Users %
Africa	1,246,504,865	16.6 %	388,376,491	31.2 %	8,503.1%	10.0 %
Asia	4,148,177,672	55.2 %	1,938,075,631	46.7 %	1,595.5%	49.7 %
Europe	822,710,362	10.9 %	659,634,487	80.2 %	527.6%	17.0 %
Latin America / Caribbean	647,604,645	8.6 %	404,269,163	62.4 %	2,137.4%	10.4 %
Middle East	250,327,574	3.[illegible] %	146,972,123	58.7 %	4,374.3%	3.8 %
North America	363,224,006	[illegible] %	320,059,368	88.1 %	196.1%	8.2 %
Oceania / Australia	40,479,846	0.5 %	28,18[illegible]56	69.6 %	269.8%	0.7 %
WORLD TOTAL	7,519,028,970	100.0 %	3,885,[illegible]67,619	51.7 %	976.4%	100.0 %

NOTES: (1) Internet Usage and World Population Statistics updated as of June 30, 2017. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations Population Division. (4) Internet usage information comes from data published by Nielsen Online, by ITU, the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide. (6) Information from this site may be cited, giving the due credit and placing a link back to www.internetworldstats.com.

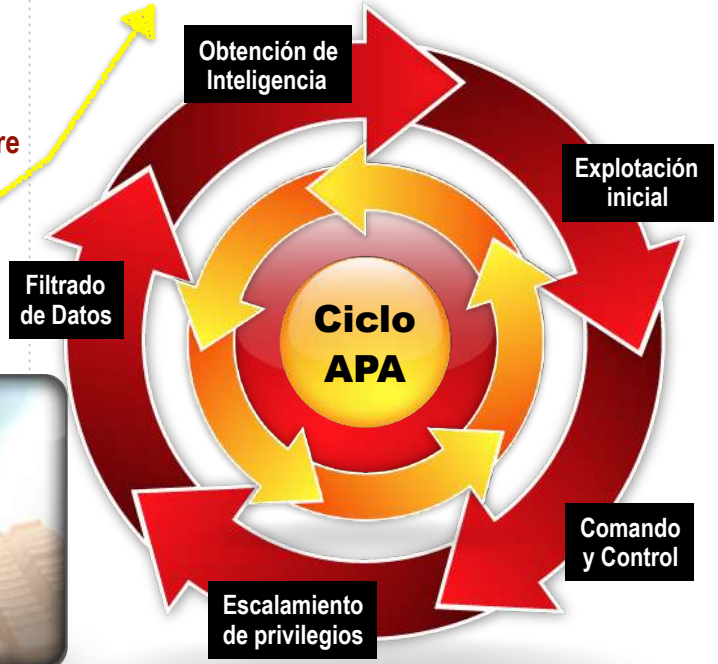
Usuarios de Internet en LATAM y el Caribe (Junio 2017)

Internet Usage and Population Statistics for South America
June 30, 2017

SOUTH AMERICA	Population (2017 Est.)	% Pop. Table	Internet Usage, 30-Jun-2017	% Population (Penetration)	% Users Table	Facebook 30-June-2016
Argentina	44,272,125	10.4 %	34,785,206	78.6 %	12.5 %	29,000,000
Bolivia	11,052,864	2.6 %	4,871,000	44.1 %	1.7 %	4,600,000
Brazil	211,243,220	49.5 %	139,111,185	65.9 %	49.9 %	111,000,000
Chile	18,313,495	4.3 %	14,108,392	77.0 %	5.1 %	12,000,000
Colombia	49,067,981	11.5 %	28,528,124	58.1 %	10.2 %	26,000,000
Ecuador	16,625,776	3.9 %	13,471,736	81.0 %	4.8 %	9,700,000
Falkland Islands	2,919	0.0 %	2,900	99.3 %	0.0 %	2,500
French Guiana	282,761	0	100,000	35.4 %	0.0 %	100,000
Guyana	774,407	.2 %	305	39.4 %	0.1 %	280,000
Paraguay	6,811,58	1.6 %	7,748	51.4 %	1.3 %	2,900,000
Peru	32,166,473	7.5 %	18,000,000	56.0 %	6.5 %	18,000,000
Suriname	552,112	0.1 %	260,000	47.1 %	0.1 %	260,000
Uruguay	3,456,877	0.8 %	2,400,000	69.4 %	0.9 %	2,400,000
Venezuela	31,925,705	7.5 %	19,155,423	60.0 %	6.9 %	13,000,000
TOTAL SOUTH AMERICA	416,548,298	100.0 %	278,596,721	65.3 %	100.0 %	229,242,

Usuarios de Internet en Ecuador (Junio 2017)

Riesgos	Atacantes poco sofisticados	Atacantes sofisticados	Espionaje corporativo	Crimen organizado	Amenazas Persistentes Avanzadas (Ataques patrocinados por Estados)
Ataques muy sofisticados					• Espionaje patrocinado por Gobiernos • Manipulación del Mercado • Ventaja competitiva • Objetivos politicos y/o militares
Bandas del crimen organizado				• Dinero • Robo de Identidad • Ramsomware	
"Insiders" maliciosos			• Venganza • Beneficio pers. • Manipular el Mercado		
Hackers		• Dinero • Difamar • Causas políticas • Causas sociales			
Inexpertos "Script kiddies"	• Diversión • Experimentar • Molestar • Notoriedad				



Recursos de los atacantes y su sofisticación

Adaptación gráfica de C. Ramírez
Fuente: EY Cybercrime 2014.

CELAES XXXII Congreso Latinoamericano de Seguridad Bancaria
Oct. 5 y 6, 2017 - Quito

asobanca

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Aquí está la clave

CIBER INTELIGENCIA

Punto de detección potencial con **INTELIGENCIA** robusta contra amenazas

Aceleración de la detección del ataque

Punto donde la mayoría de los objetivos son notificados del ataque. Generalmente por terceras partes

¿Como se realiza un ataque dirigido?

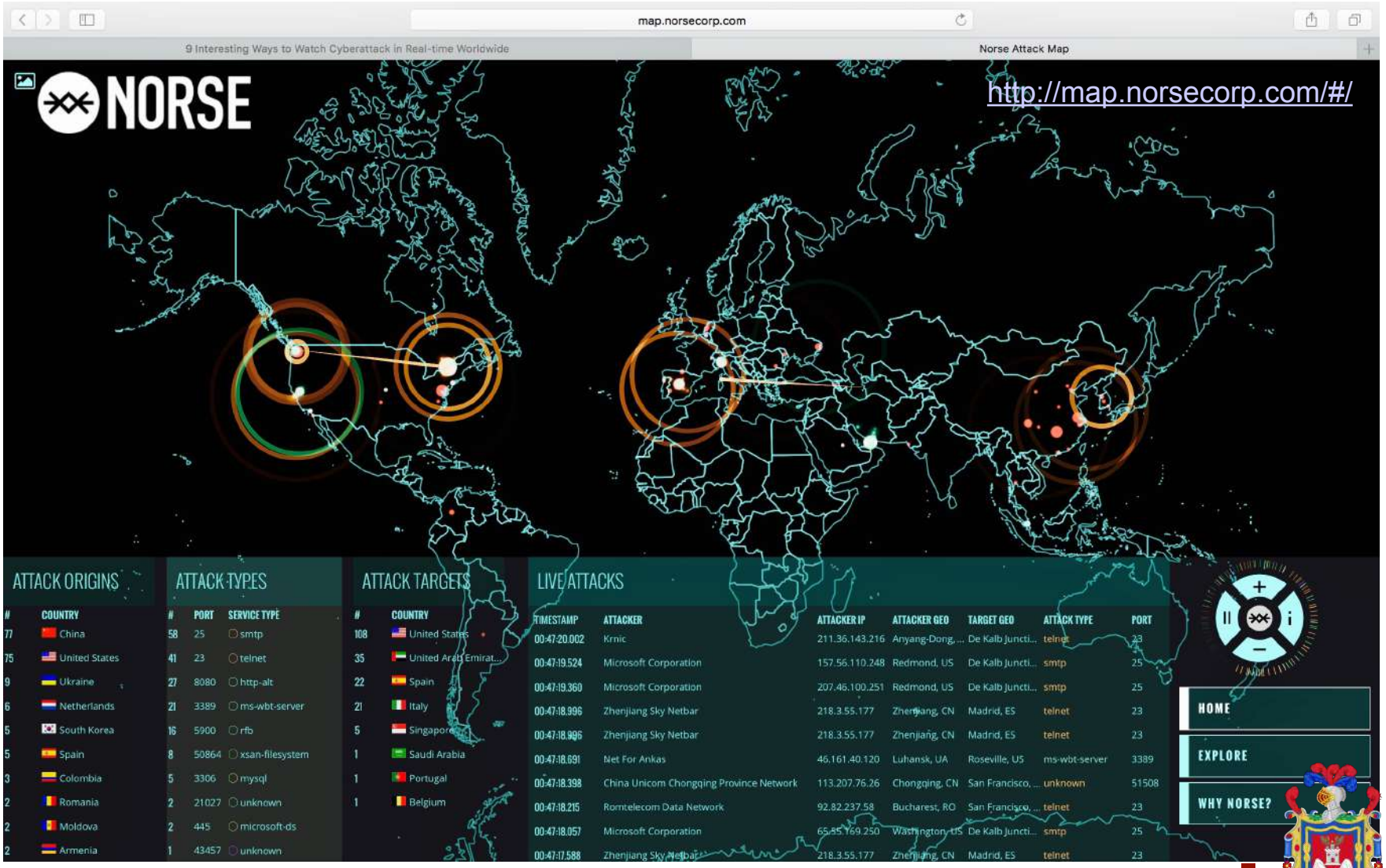
Obtención de Inteligencia	Explotación inicial	Comando y control	Privilegios de escalamiento	Extracción de Datos
Revisión y análisis de antecedentes	Ejecución de ataque inicial	Colocación de punto de apoyo	Habilitar persistencia	Realizar un reconocimiento profundo de la empresa	Moverse lateralmente a nuevos sistemas	Escalar privilegios	Obtener y encriptar datos de interés	Extraer datos de los sistemas de la víctima	Mantener presencia persistente

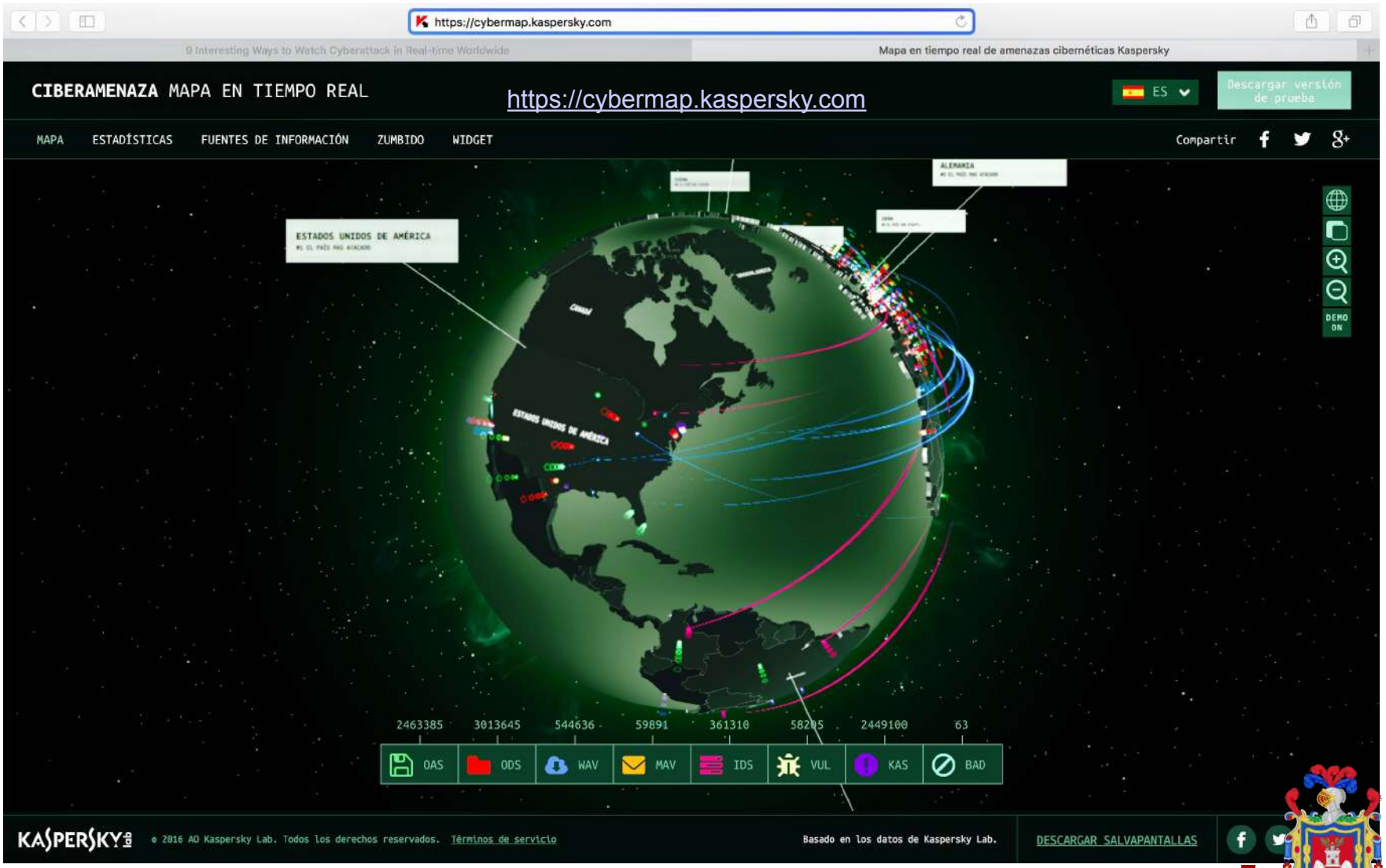
Degradación de la seguridad durante el progreso del ataque

El objetivo primario del ataque:

- **NO es una computadora**
- **ES un usuario humano**

Adaptación gráfica de C. Ramírez
Fuente: EY Cybercrime 2014.


map.norsecorp.com
9 Interesting Ways to Watch Cyberattack in Real-time Worldwide
Norse Attack Map
NORSE
http://map.norsecorp.com/#/
ATTACK ORIGINS
COUNTRY
77 China
75 United States
9 Ukraine
6 Netherlands
5 South Korea
5 Spain
3 Colombia
2 Romania
2 Moldova
2 Armenia
ATTACK TYPES
PORT SERVICE TYPE
58 25 smtp
41 23 telnet
27 8080 http-alt
21 3389 ms-wbt-server
16 5900 rfb
8 50864 xsan-filesystem
5 3306 mysql
2 21027 unknown
2 445 microsoft-ds
1 43457 unknown
ATTACK TARGETS
COUNTRY
108 United States
35 United Arab Emirat...
22 Spain
21 Italy
5 Singapore
1 Saudi Arabia
1 Portugal
1 Belgium
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
00:47:20.002 Krnic 211.36.143.216 Anyang-Dong, ... De Kalb Juncti... telnet 23
00:47:19.524 Microsoft Corporation 157.56.110.248 Redmond, US De Kalb Juncti... smtp 25
00:47:19.360 Microsoft Corporation 207.46.100.251 Redmond, US De Kalb Juncti... smtp 25
00:47:18.996 Zhenjiang Sky Netbar 218.3.55.177 Zhenjiang, CN Madrid, ES telnet 23
00:47:18.996 Zhenjiang Sky Netbar 218.3.55.177 Zhenjiang, CN Madrid, ES telnet 23
00:47:18.691 Net For Ankas 46.161.40.120 Luhansk, UA Roseville, US ms-wbt-server 3389
00:47:18.398 China Unicom Chongqing Province Network 113.207.76.26 Chongqing, CN San Francisco, ... unknown 51508
00:47:18.215 Romtelecom Data Network 92.82.237.58 Bucharest, RO San Francisco, ... telnet 23
00:47:18.057 Microsoft Corporation 65.55.169.250 Washington, US De Kalb Juncti... smtp 25
00:47:17.588 Zhenjiang Sky Netbar 218.3.55.177 Zhenjiang, CN Madrid, ES telnet 23
HOME
EXPLORE
WHY NORSE?


https://cybermap.kaspersky.com
Mapa en tiempo real de amenazas cibernéticas Kaspersky
CIBERAMENAZA MAPA EN TIEMPO REAL
https://cybermap.kaspersky.com
ES
Descargar versión de prueba
MAPA
ESTADÍSTICAS
FUENTES DE INFORMACIÓN
ZUMBIDO
WIDGET
Compartir
ESTADOS UNIDOS DE AMÉRICA
ALEMANIA
DEMO ON
2463385
3013645
544636
59891
361310
58205
2449100
63
OAS
ODS
WAV
MAV
IDS
VUL
KAS
BAD
KASPERSKY
© 2016 AO Kaspersky Lab. Todos los derechos reservados. Términos de servicio
Basado en los datos de Kaspersky Lab.
DESCARGAR SALVAPANTALLAS

Piratas rusos se infiltraron en el Partido Demócrata estadounidense

El FBI y Homeland Security describen cómo operaron dos unidades rusas: APT28 y APT29

El ataque APT28

Llevaba a sus objetivos a cambiar sus contraseñas en un sitio web falso, para luego robar información

Infraestructura operacional

1

Piratas informáticos crearon una infraestructura operacional para ocultar su origen

9 **Publicación**

2

Envío de un email

Incitando al destinatario a cambiar su contraseña

5 **El sitio transmite** la nueva identificación

http:// "malware" ok

6

8 **Reenvío** de datos

3

El destinatario

accede a un vínculo contenido en el email

4 **Ingresa nuevo PW** en un sitio que parece legítimo

Las Id obtenidas son usadas para acceder a organizaciones específicas

7 **Instalación** de virus

John Podesta
Jefe de campaña H. Clinton

Comité Nacional Demócrata

Objetivos

divulgados por los medios de EU

APT Advanced Persistent Threat
Software malicioso sofisticado que explota vulnerabilidades en los sistemas

Carlos Ramírez, CPP
ALAPSI México 2017

Piratas rusos se infiltraron en el Partido Demócrata estadounidense

El FBI y Homeland Security describen cómo operaron dos unidades rusas: APT28 y APT29

Trump rechazó versiones de sus cuerpos de Inteligencia quienes señalaron a Rusia por ciber ataques (APT) para favorecer su campaña


Video cápsula

Ver **"Computer Security Incident Handling Guide"** Section 1 Special Publication 800-61

Ver **"Guide to Integrating Forensic Techniques into Incident Response"** Section 2 Special Publication 800-86

RECOMENDACIONES DEL
National Institute of Standards and Technology
Guidance Software, Inc

TRADUCIDAS AL ESPAÑOL

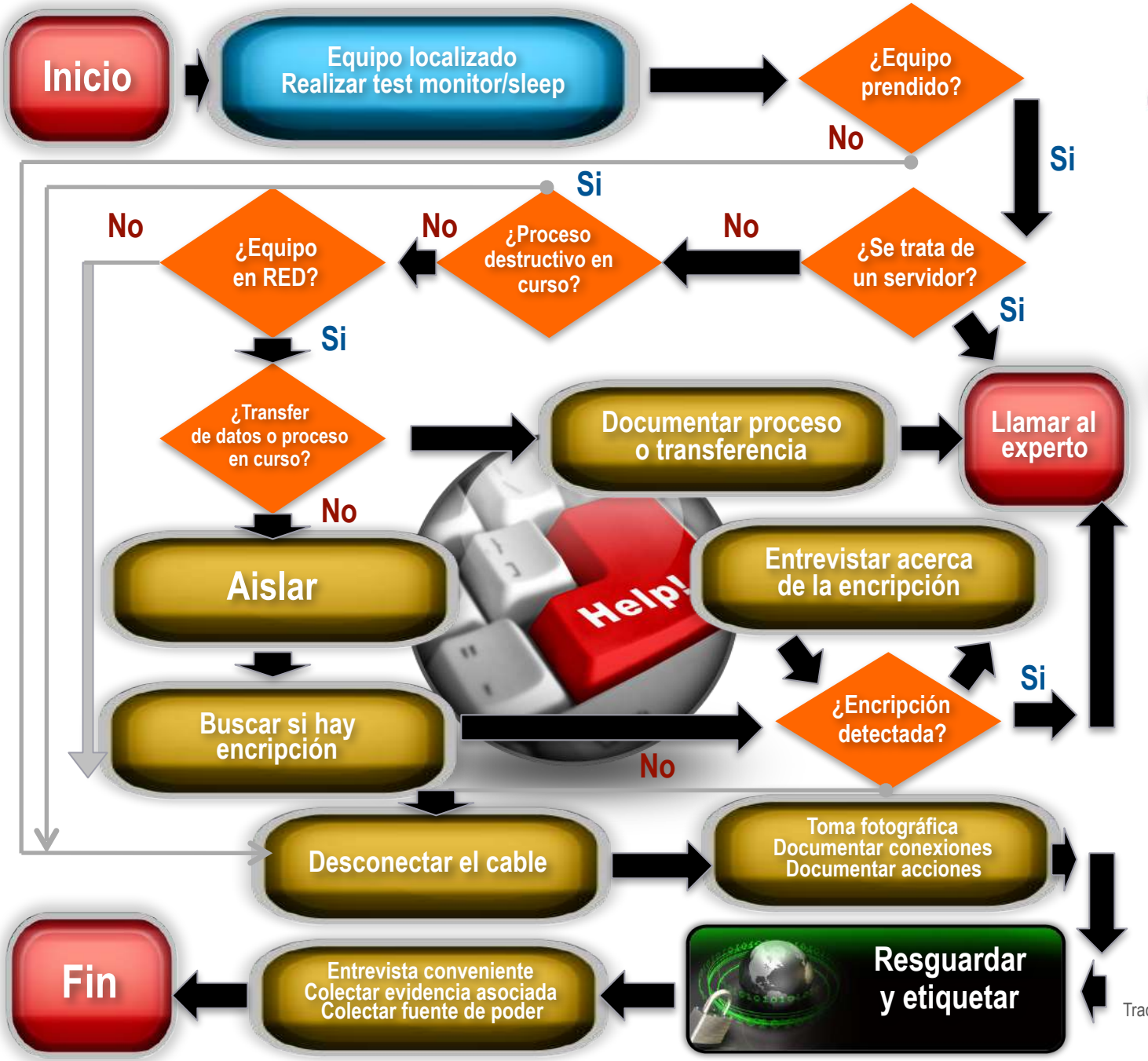
CICLO DE VIDA DE RESPUESTA A INCIDENTES

PREPARACIÓN → DETECCIÓN Y ANÁLISIS → CONTENCIÓN ERRADICACIÓN Y RECUPERACIÓN → ACCIONES DESPUÉS DEL INCIDENTE

PROCESO FORENSE COMPUTACIONAL

RECOLECCIÓN → EXAMINACIÓN → ANÁLISIS → REPORTE

Medio → Datos → Información → Evidencia



CELAES
XXXII Congreso Latinoamericano de Seguridad Bancaria

Primero en responder al llamado

(First Responder)

Flujograma para el aseguramiento de la evidencia física y digital

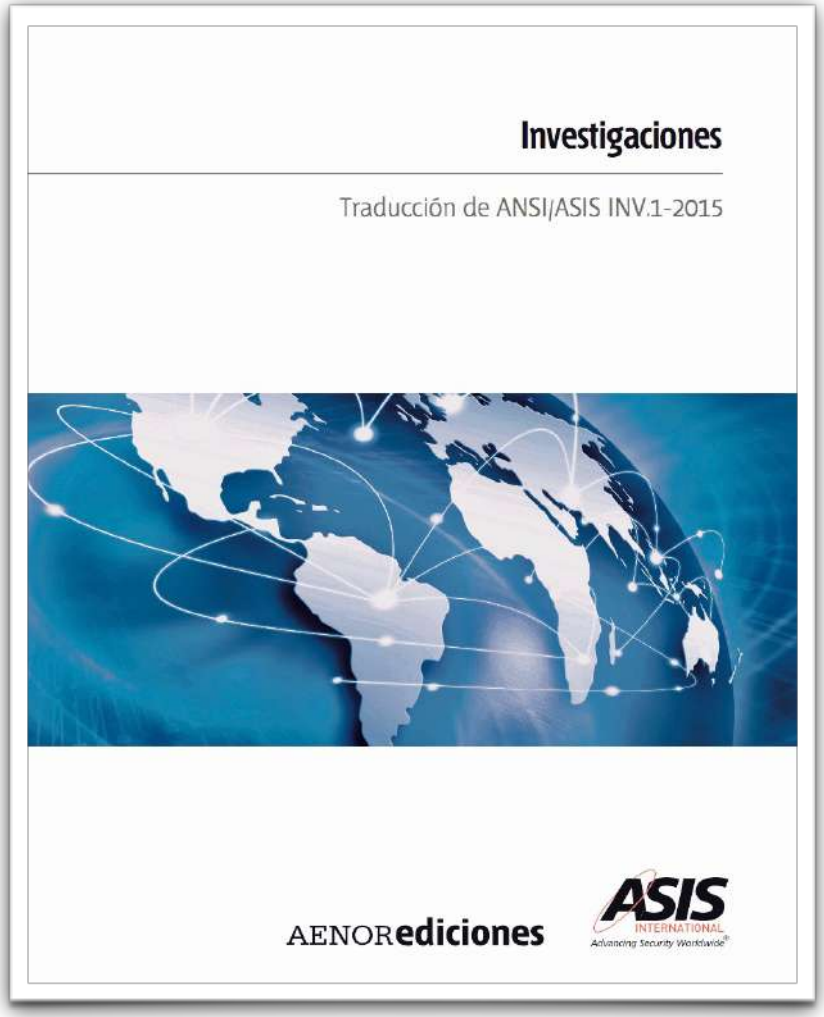
International Association of Computer Investigative Specialists (IACIS). 2011

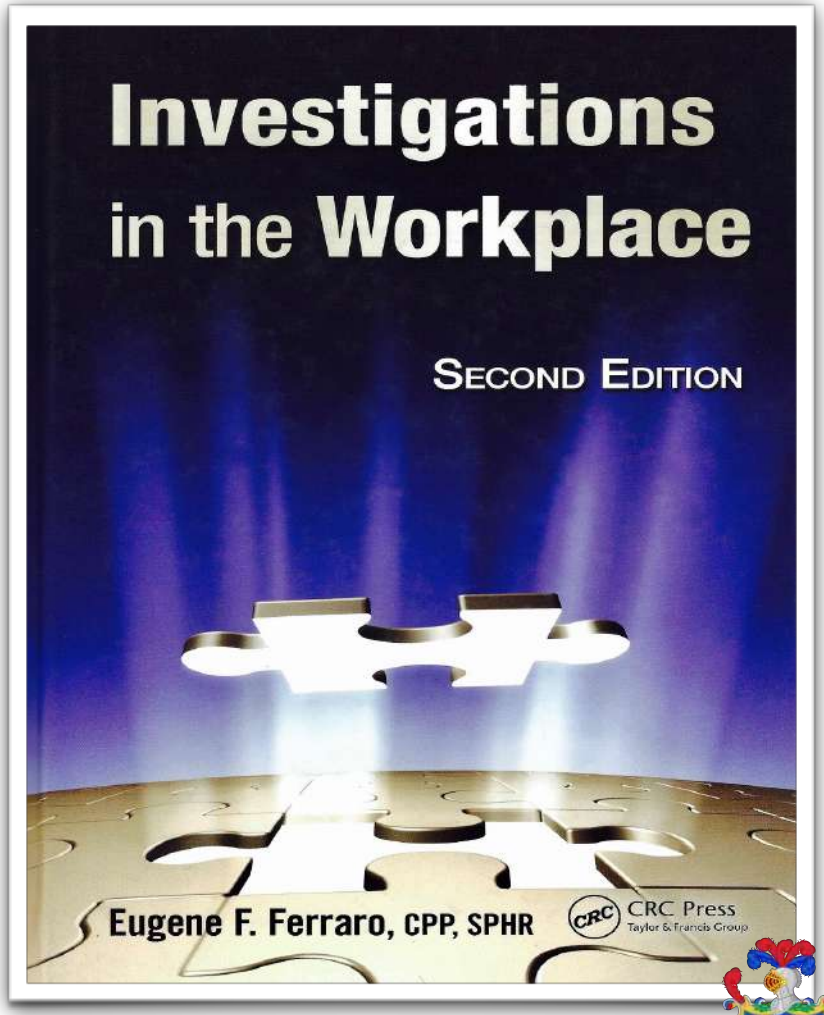
IACIS
The International Association of Computer Investigative Specialists

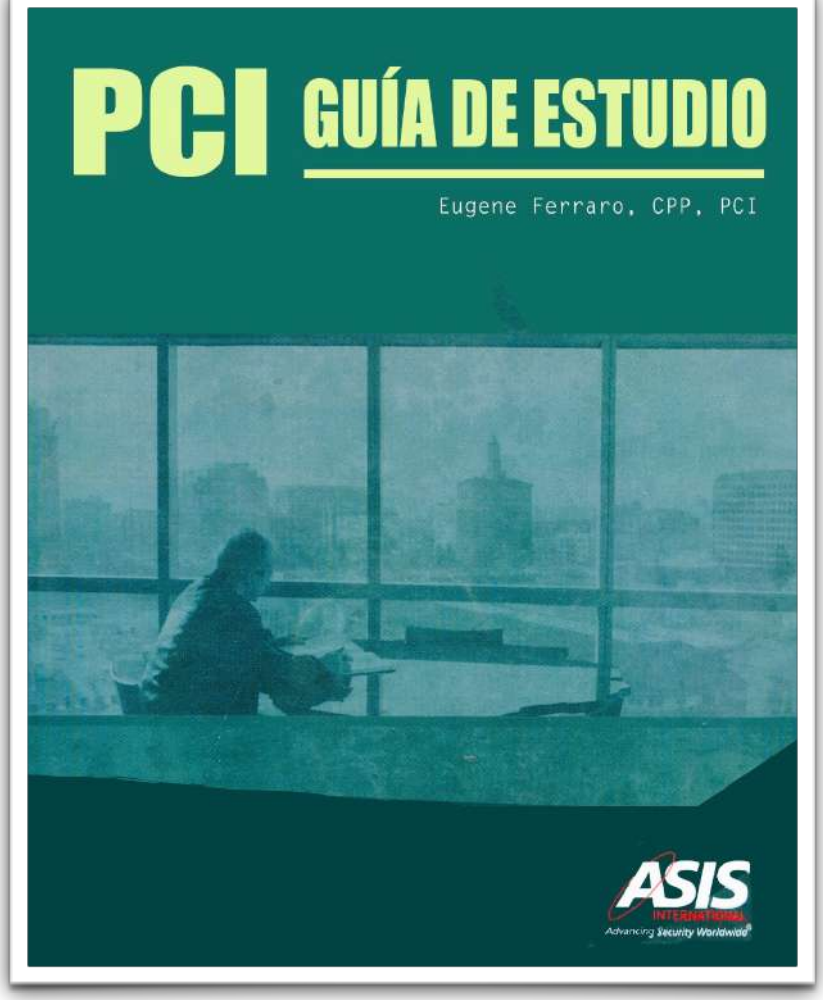
Traducido y adaptado por C. Ramírez

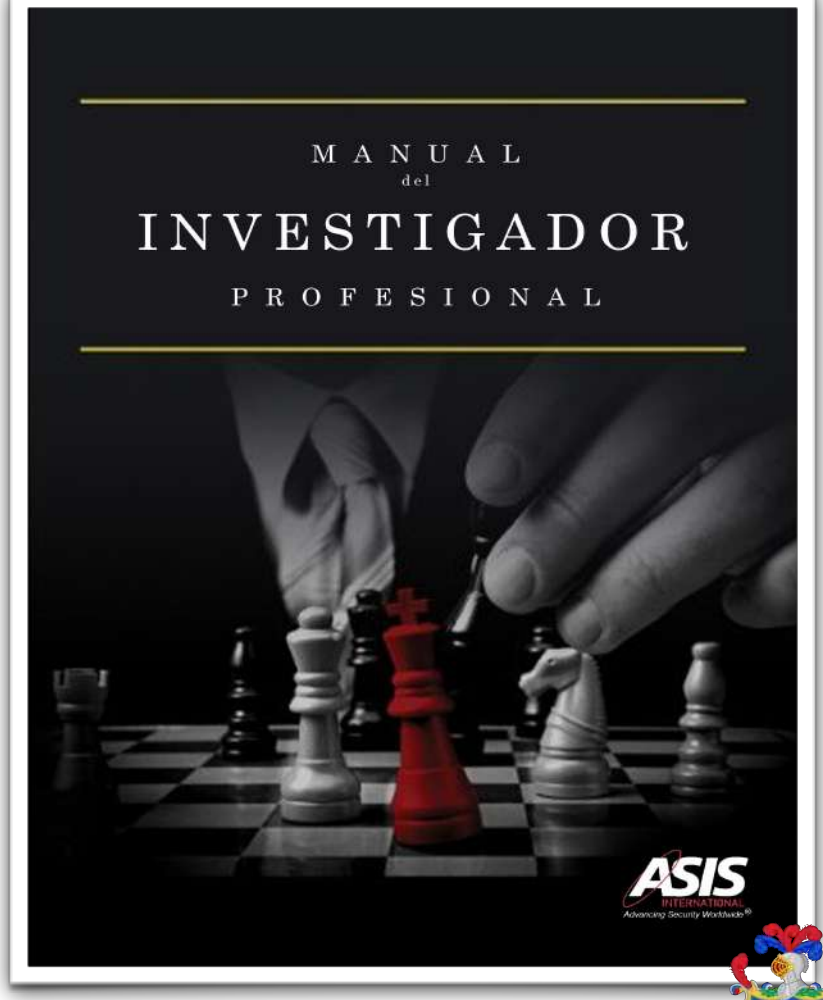
Las cinco "D"

1
Disuadir
Firewalls
PW
Encryption
2
Detectar
IDS
Alertas
Alarmas
3
Demorar
Capas
Honynets
Honypots
4
Defender
Pen-Test
CIRTs
Bloqueadores
5
Destruir
Atacar
Borrar
CMC
Pensamiento Crítico en la CIBERSEGURIDAD


Investigaciones
Traducción de ANSI/ASIS INV.1-2015
AENORediciones
ASIS INTERNATIONAL


Investigations in the Workplace
SECOND EDITION
Eugene F. Ferraro, CPP, SPHR
CRC Press
Taylor & Francis Group


PCI GUÍA DE ESTUDIO
Eugene Ferraro, CPP, PCI
ASIS INTERNATIONAL
Advancing Security Worldwide


MANUAL
del
INVESTIGADOR
PROFESIONAL
ASIS INTERNATIONAL
Advancing Security Worldwide

10 Consejos prácticos para Investigar fraudes

1. Sé agradable. Sonríe a menudo

Los mejores investigadores son los más agradables
Sonríen bastante, aún frente a los pillos. Eso los desarma

2. Primero, haz tu trabajo

Si tienes un juicio de fraude, no entrevistes
al sospechoso antes de que hagas la tarea

3. Desarrolla una teoría del fraude

Para el éxito de un caso, es vital tener
una teoría. Cada caso tiene signos únicos

4. No compliques un caso

La mayoría de fraudes son cometidos por una
persona. El pillo siempre busca lo más fácil

5. Si no sabes qué sigue, detente

Si llegas a un punto donde no sabes qué hacer,
busca a colegas y asesoría legal

6. No sobreestimes tu autoridad

No hagas nada ilegal para atrapar un pillo.
Cada pieza de evidencia así obtenida se caerá

7. Siempre busca más pistas

Tu trabajo NO es investigar sino buscar pistas: personas,
lugares y cosas por vincular

8. Sé muy cuidadoso con lo que opines

El código de ética de nuestra profesión, prohibe
opinar sobre la culpa o inocencia de alguien

9. Las personas son quienes defraudan

No son los registros ni las computadoras, sino la
gente quien defrauda. Busca evidencia y testigos

10. Comprende el espíritu de la Ley

Haz tu trabajo y hazlo bien. Juega las reglas del juego
para que merezcas ganar

CONCLUSIÓN

RÍTMICOS

CÍCLICOS

PREDECIBLES

Fraudes

Prevenibles

OPORTUNIDAD

NECESIDAD

Triángulo del Fraude

RACIONALIZACIÓN

RED FLAGS

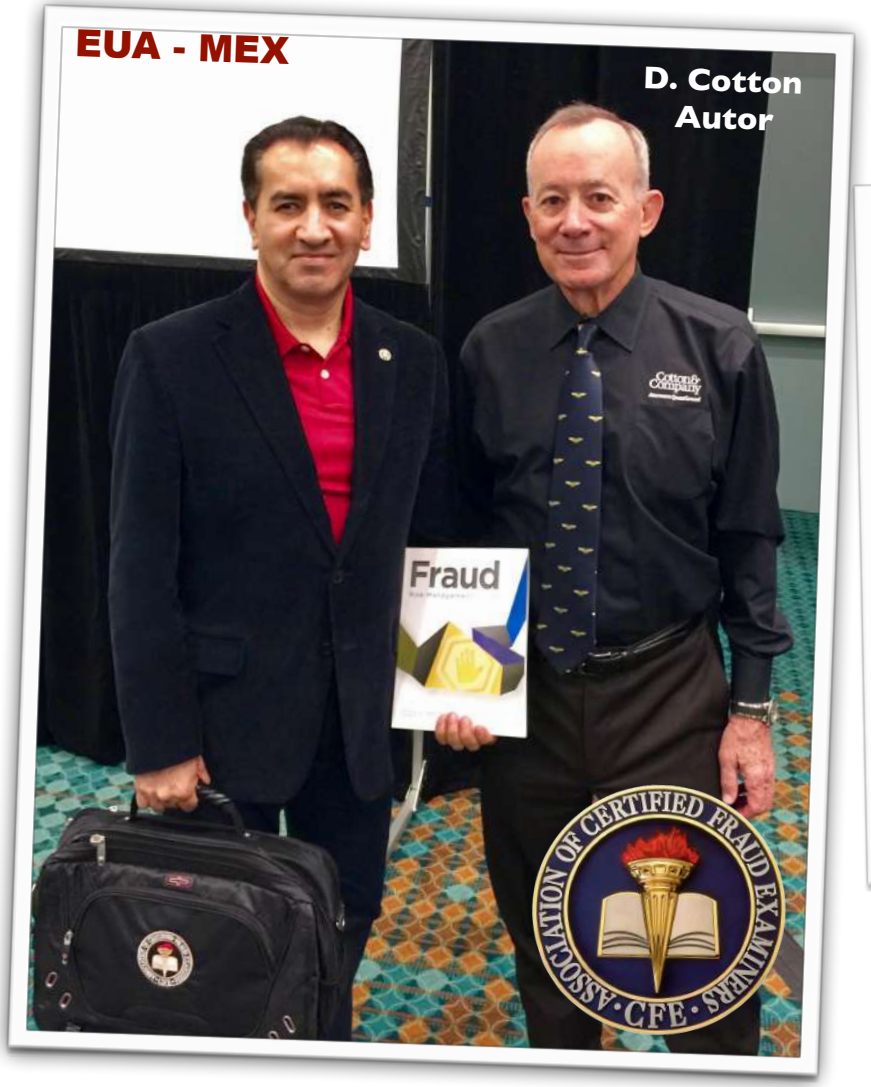
PREVENCIÓN

DETECCIÓN

Triángulo de la Seguridad

RESPUESTA

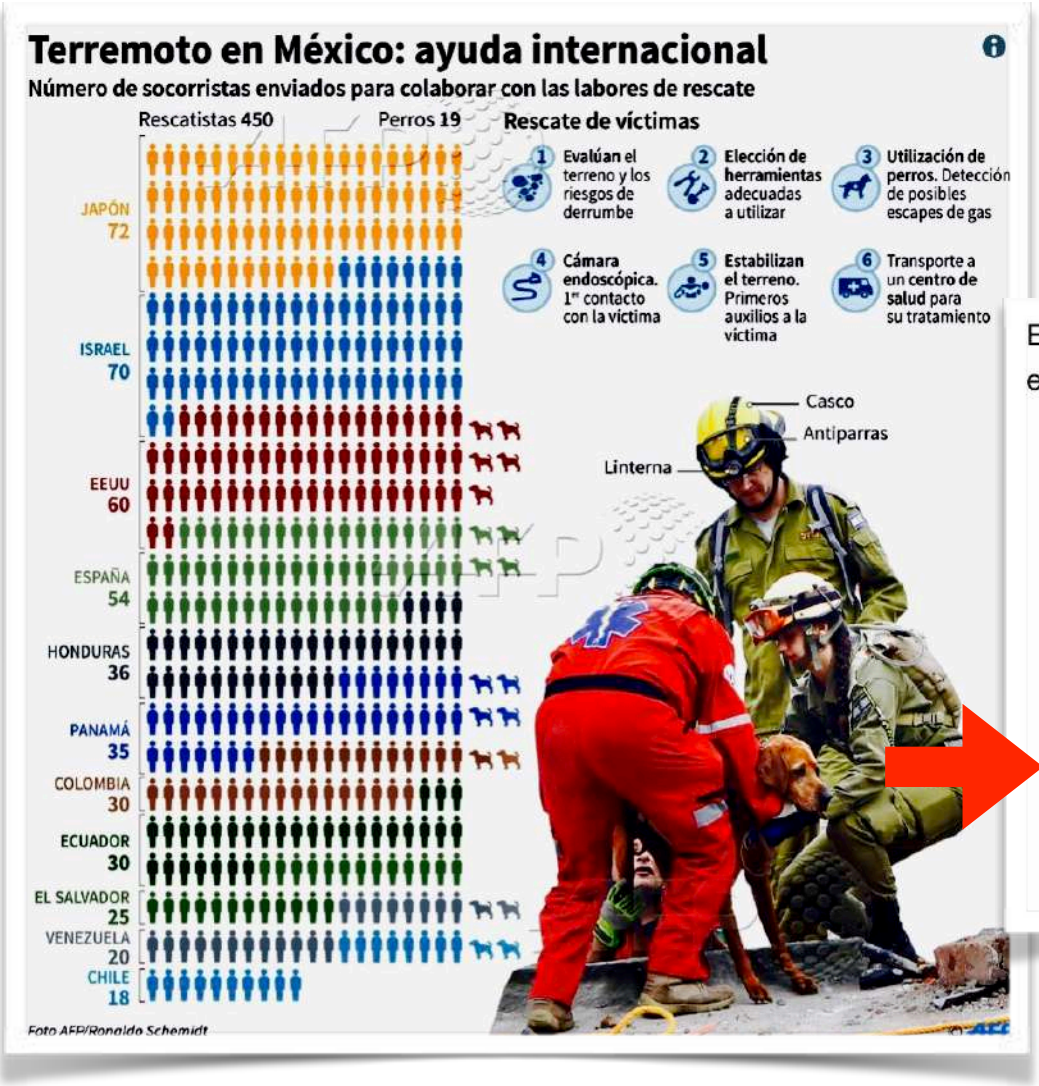
Guía de Gestión del Riesgo de Fraude ACFE-COSO



MÉXICO - NIGERIA - SUDÁFRICA -COREA - JAPÓN

Gracias Ecuador por los Rescatistas que enviaron a México


AFP
13
Ronaldo Sc
AFP
AFP

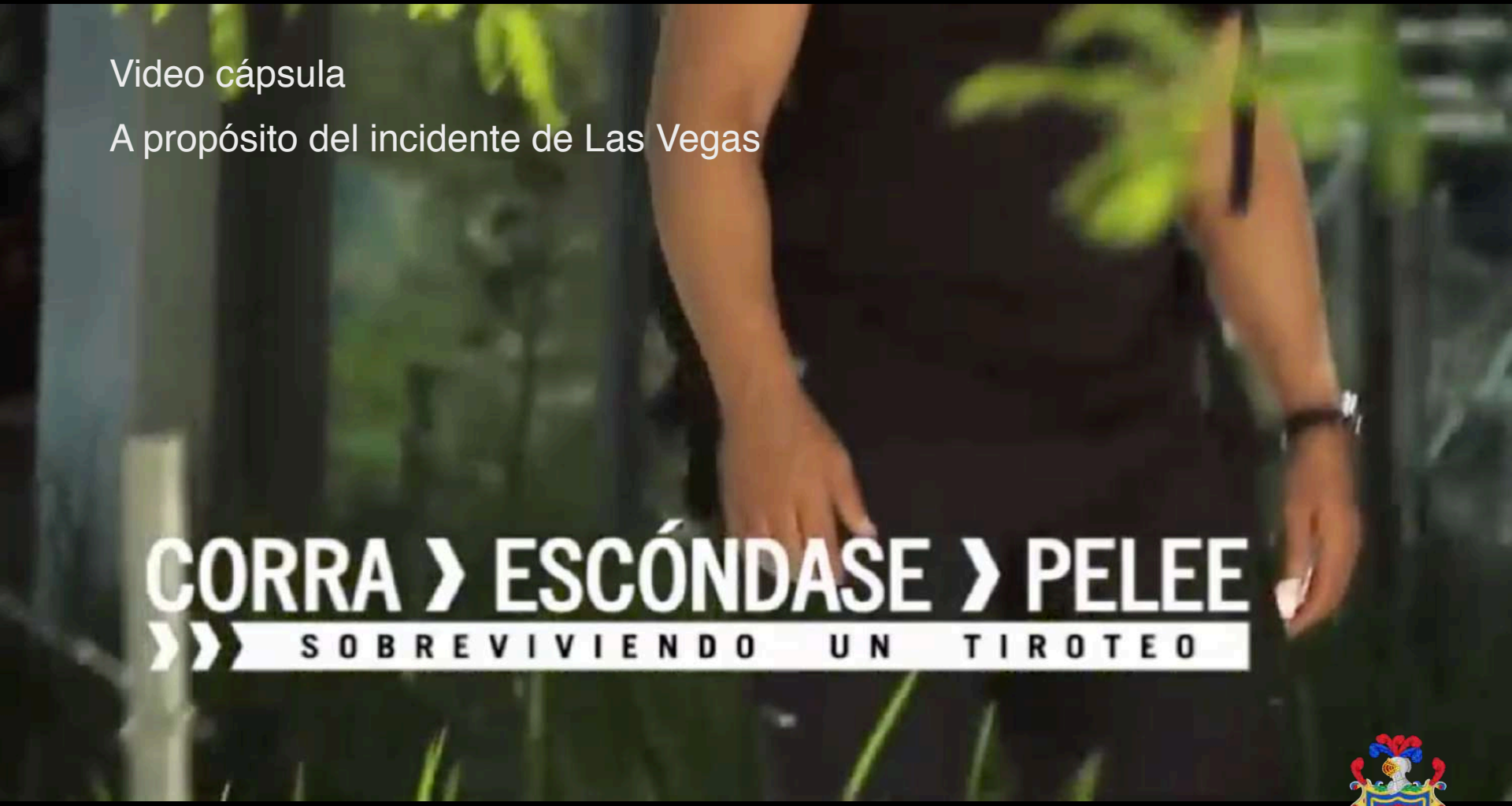


Esta es la lista completa de brigadistas extranjeros que se encuentran en México colaborando en las labores de rescate:

- Japón: 72 brigadistas y perros de rescate
- Israel: 70 brigadistas
- Estados Unidos: 60 brigadistas y cinco perros de rescate
- España: 54 brigadistas y cuatro perros de rescate
- Honduras: 36 brigadistas
- Panamá: 35 brigadistas y cuatro perros de rescate
- Colombia: 30 brigadistas y dos perros de rescate
- Ecuador: 30 brigadistas
- El Salvador: 25 brigadistas
- Venezuela: 20 brigadistas y dos perros de rescate
- Chile: 18 brigadistas y dos perros de rescate

Video cápsula

A propósito del incidente de Las Vegas



CELAES
XXXII Congreso Latinoamericano de Seguridad Bancaria
Oct. 5 y 6, 2017 - Quito

asobanca

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Hasta pronto

Carlos Ramírez, CPP

Comité de Expertos Latinoamericanos en Seguridad Bancaria

Congresos CELAES

	#	CONGRESO	FECHAS	AÑO	LUGAR
I	1	CELAES		1986	
II	2	CELAES		1987	
III	3	CELAES		1988	
IV	4	CELAES		1989	PUEBLA, MÉXICO
V	5	CELAES	29 AL 31 DE OCTUBRE	1990	QUITO, ECUADOR
VI	6	CELAES	23 AL 25 DE OCTUBRE	1991	BOGOTÁ, COLOMBIA
VII	7	CELAES	23 AL 25 DE SEPTIEMBRE	1992	GUATEMALA, GUATEMALA
VIII	8	CELAES	8 AL 10 DE NOVIEMBRE	1993	LIMA, PERÚ
IX	9	CELAES	29 Y 30 DE SEPTIEMBRE	1994	MIAMI FL, USA
X	10	CELAES	9 Y 10 DE NOVIEMBRE	1995	PANAMÁ, PANAMÁ
XI	11	CELAES	14 AL 16 DE OCTUBRE	1996	MONTEVIDEO, URUGUAY
XII	12	CELAES	22 AL 24 DE OCTUBRE	1997	BÁVARO, REP. DOMINICANA
XIII	13	CELAES	28, 29 DE OCTUBRE	1998	SAN SALVADOR, EL SALVADOR
XIV	14	CELAES	20, 21 DE OCTUBRE	1999	LIMA, PERÚ
XV	15	CELAES	03 AL 05 DE JULIO	2000	LA HABANA, CUBA
XVI	16	CELAES	21 AL 23 DE NOVIEMBRE	2001	GUATEMALA, GUATEMALA
XVII	17	CELAES	04 Y 05 DE AGOSTO	2002	SAN JOSÉ, COSTA RICA
XVIII	18	CELAES	08 AL 11 DE OCTUBRE	2003	LA ROMANA, REP. DOMINICANA
XIV	19	CELAES		2004	LIMA, PERÚ
XX	20	CELAES	10, 12 DE AGOSTO	2005	GUATEMALA, GUATEMALA
XXI	21	CELAES	01, 03 DE OCTUBRE	2006	PANAMÁ, PANAMÁ
XXII	22	CELAES	23, 25 DE SEPTIEMBRE	2007	TEGUCIGALPA, HONDURAS
XXIII	23	CELAES	31 AGOSTO AL 2 DE SEPTIEMBRE	2008	MÉXICO, MÉXICO
XXIV	24	CELAES	27 AL 29 DE SEPTIEMBRE	2009	PANAMÁ, PANAMÁ
XXV	25	CELAES	30 DE SEPTIEMBRE AL 1 DE OCTUBRE	2010	MIAMI FL, USA
XXVI	26	CELAES	16 AL 16 DE SEPTIEMBRE	2011	MIAMI FL, USA
XXVII	27	CELAES	20 AL 21 DE SEPTIEMBRE	2012	MIAMI FL, USA
XXVIII	28	CELAES	25 AL 26 DE NOVIEMBRE	2013	LIMA, PERÚ
XXIX	29	CELAES	22 AL 23 DE SEPTIEMBRE	2014	MIAMI FL, USA
XXX	30	CELAES	15 AL 16 DE OCTUBRE	2015	PANAMÁ, PANAMÁ
XXXI	31	CELAES	03 AL 04 DE OCTUBRE	2016	MIAMI FL, USA
XXXII	32	CELAES	05 AL 06 DE OCTUBRE	2017	QUITO, ECUADOR