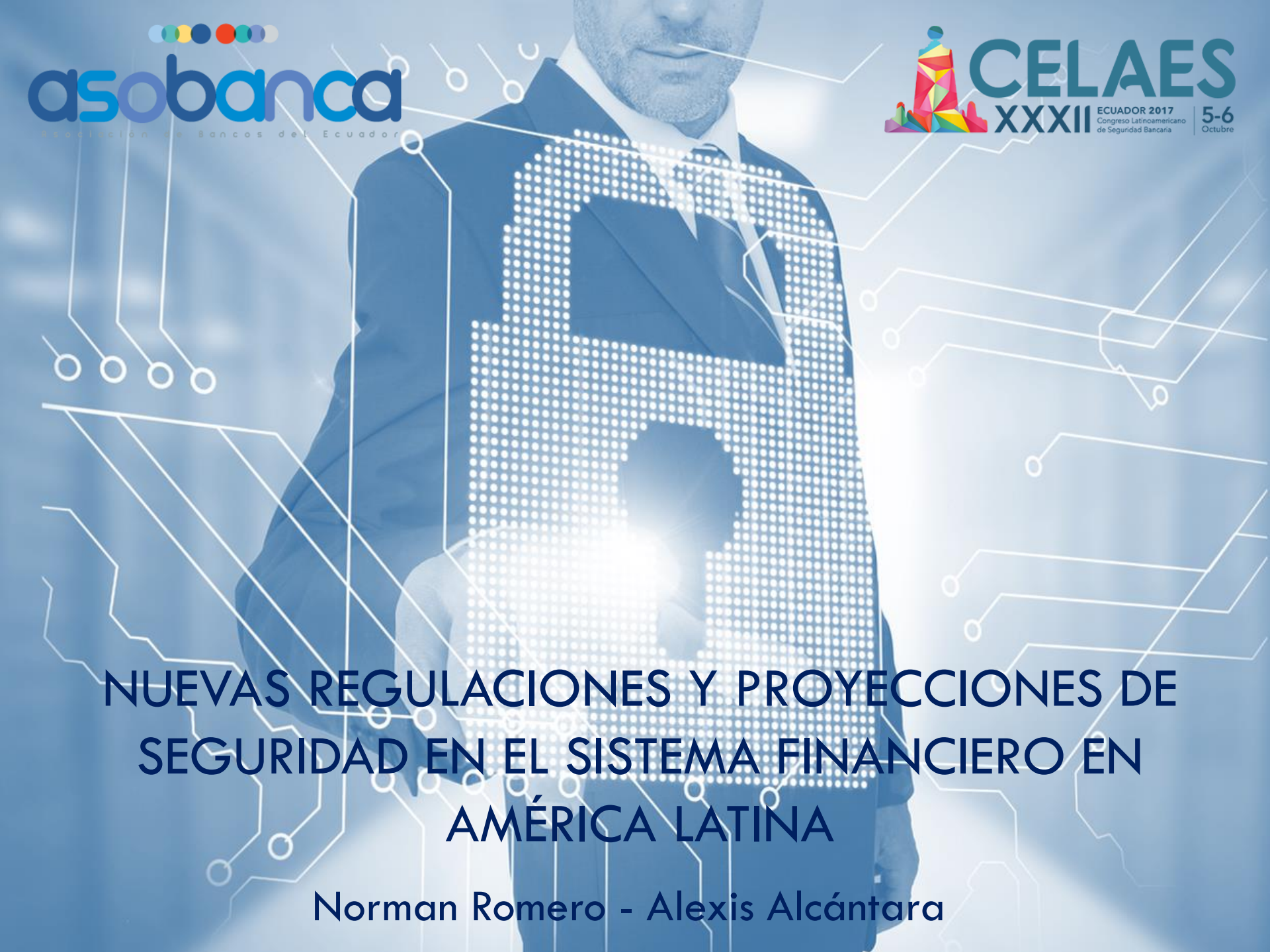


NUEVAS REGULACIONES Y PROYECCIONES DE SEGURIDAD EN EL SISTEMA FINANCIERO EN AMÉRICA LATINA

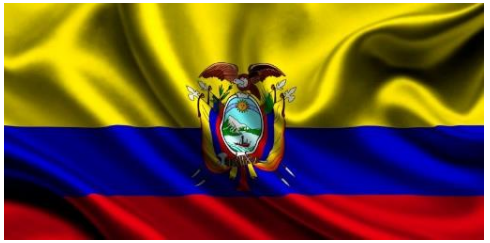
Norman Romero - Alexis Alcántara

PRESENTACIÓN

Alexis Alcántara – República Dominicana

- Licenciaturas en Derecho y en Administración de Empresas.
- Licenciado en Ciencias Navales Egresado de la Academia Naval de La Armada de Republica Dominicana.
- Director de Seguridad del Banco de Servicios Múltiple ADEMI Actualmente, con 20 años de servicios en ese Banco.
- Presidente del Comité de Seguridad Bancaria de Republica Dominicana y 1er Vicepresidente del CELAES.

Norman Romero – Ecuador



- Licenciado Ciencias Militares, Diplomado en Gestión de Riesgo y Administración de Seguridad Bancaria.
- 30 años en trabajos de prevención de pérdidas.
- 18 años responsable de la Dirección de Prevención de Fraudes y Seguridad de Banco Internacional.
- 17 años miembro del Comité de Seguridad Bancaria del Ecuador
- Ex Oficial de Inteligencia de las FFAA.

asobanca
Asociación de Bancos del Ecuador

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre


ESTRUCTURA

ESTRUCTURA

Contexto

- 20 minutos por cada panelista.

Conclusiones

- 5 minutos.

Preguntas

- Se receptarán y se contestarán a través de la APP del evento.

Norman Romero

CONTEXTO

La sociedad del riesgo.

"Fase de desarrollo de la sociedad moderna donde los riesgos sociales, políticos, económicos e industriales tienden cada vez más a escapar a las instituciones de control y protección de la sociedad industrial". (Beck: 2007)

asobanca
Asociación de Bancos del Ecuador

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre

La sociedad del riesgo.

Likelihood

1. Extreme weather events
2. Large-scale involuntary migration
3. Natural disasters
4. Terrorist attacks
5. Data fraud or theft
6. Cyberattacks
7. Illicit trade
8. Man-made environmental disasters
9. Interstate conflict
10. Failure of national governance

Impact

1. Weapons of mass destruction
2. Extreme weather events
3. Water crises
4. Natural disasters
5. Failure of climate-change mitigation and adaptation
6. Large-scale involuntary migration
7. Food crises
8. Terrorist attacks
9. Interstate conflict
10. Unemployment or underemployment

Categories

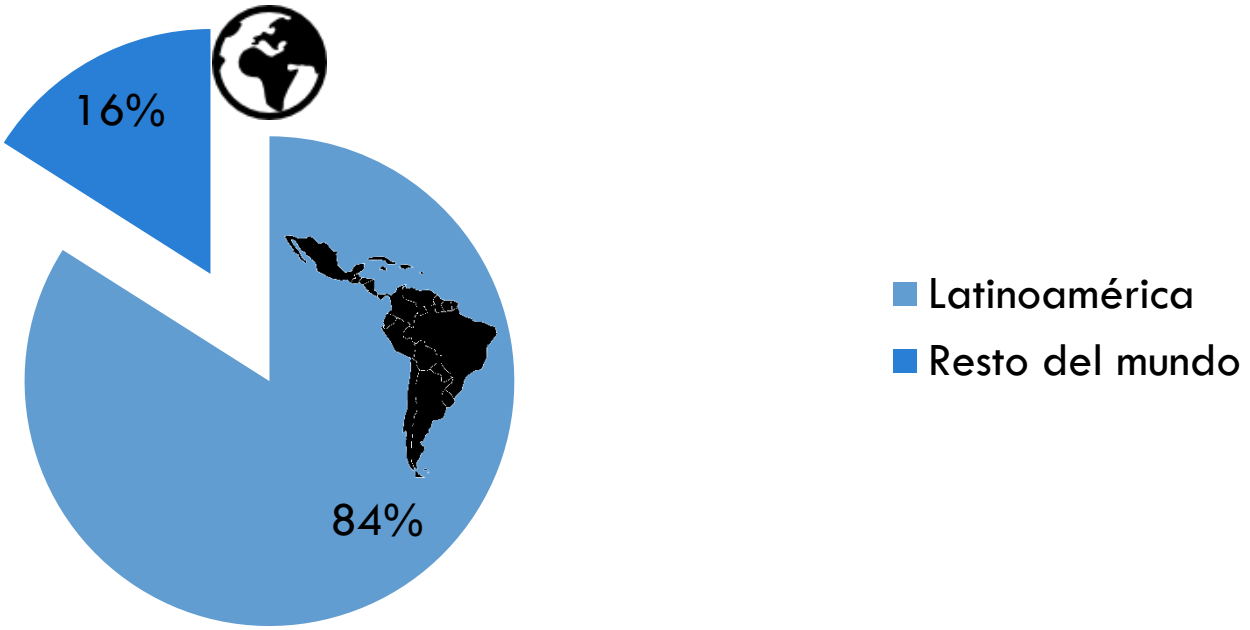
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

asobanca
Asociación de Bancos del Ecuador

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre

Situación en América Latina

Ciudades más violentas del mundo



Fuente: Consejo Ciudadano para la Seguridad Pública y Justicia Penal, en México.

10 ciudades más violentas del mundo

-Caracas
-Maturín
-Ciudad Guayana
-Valencia

-Acapulco
-Victoria

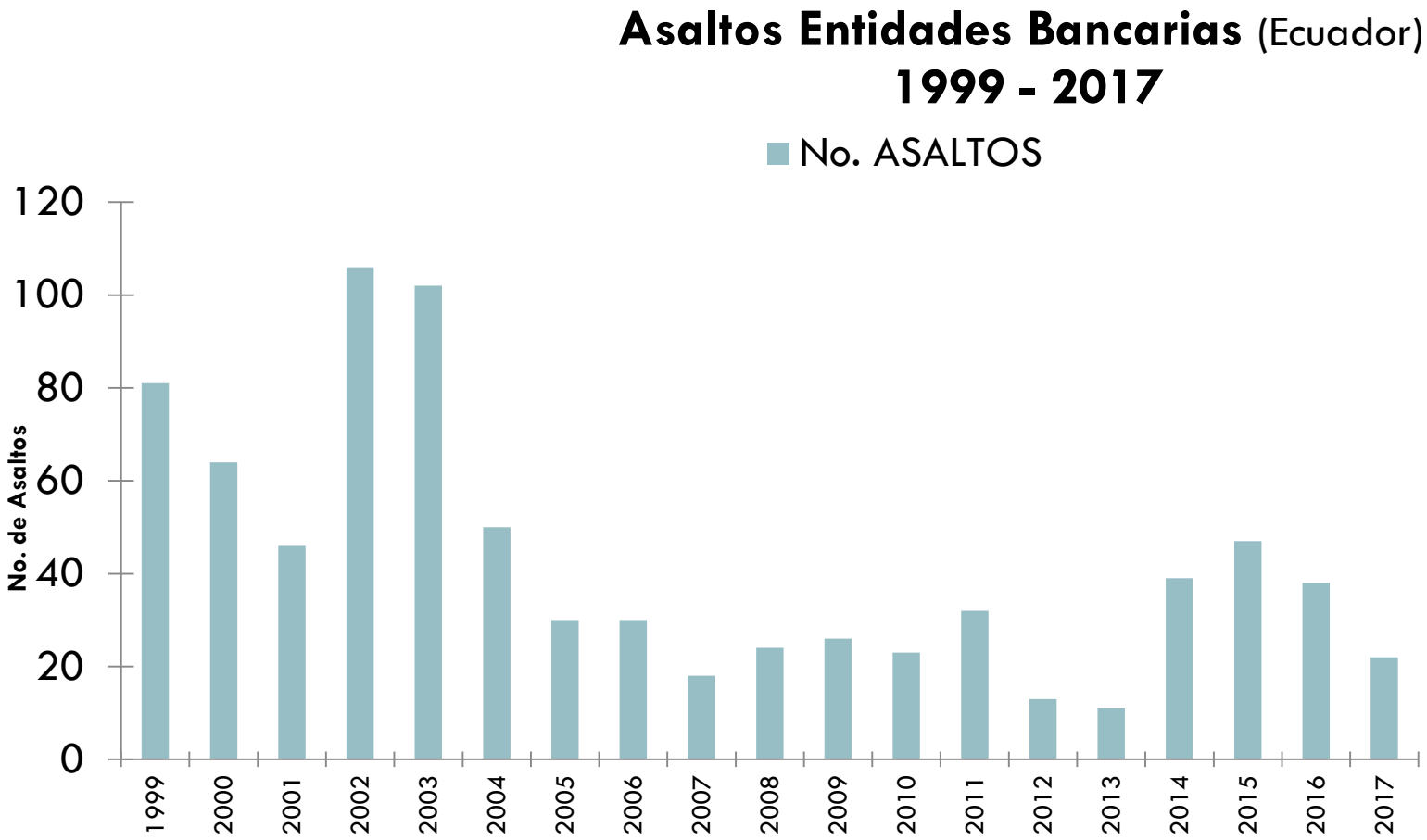
-San Pedro Sula
-Distrito Central

San Salvador

Natal

Fuente: Consejo Ciudadano para la Seguridad Pública y Justicia Penal, en México.

Riesgos no violentos

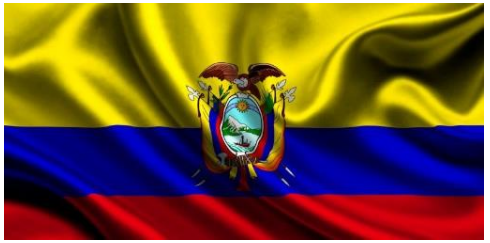


Fuente: Elaboración propia.

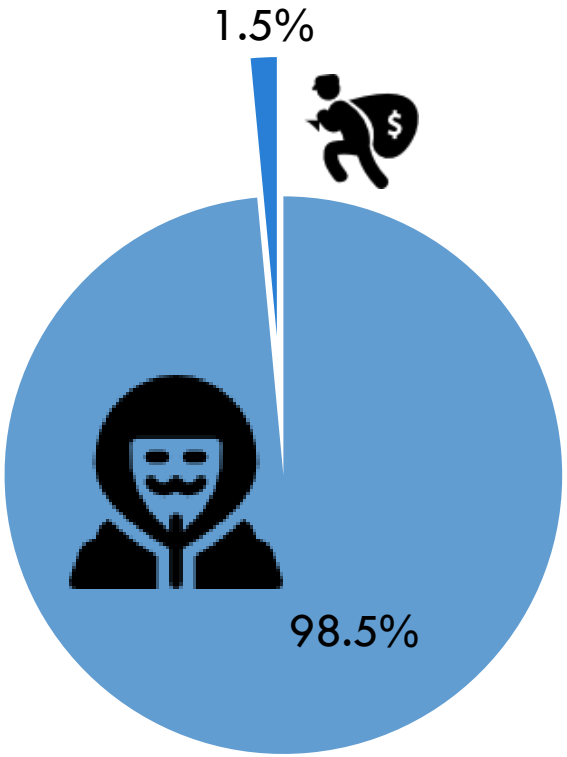
asobanca
Asociación de Bancos del Ecuador

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre

Riesgos tecnológicos o digitales

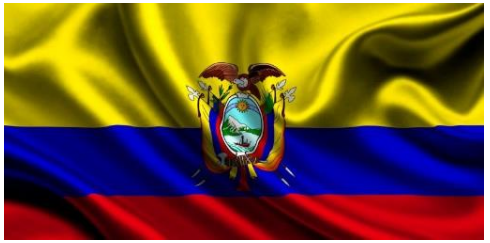


Delitos Digitales en América Latina



Fuente: FELABAN 2015.

Riesgos tecnológicos o digitales



INCREMENTO VIOLENCIA CIBERNÉTICA

+

USUARIOS DIGITALES

RIESGOS VIOLENTOS IMPERMEABLES

asobanca
Asociación de Bancos del Ecuador

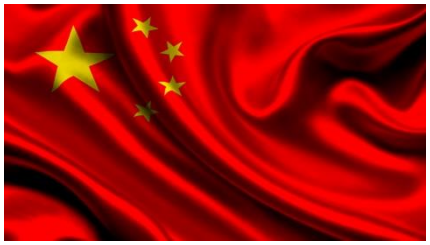
CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre

Investigación

APLICACIÓN	PAÍS	SECTOR	ESPECIALIDAD
1	Colombia	Financiero	Ciberseguridad
1	Ecuador	Financiero	Gerente
1	Ecuador	Banca	Riesgos violentos
1	Bolivia	Financiero	Consultor en seguridad
1	Venezuela	Financiero	Seguridad de la información
1	España	Seguridad de información	Ciberseguridad
1	EE.UU	Seguridad de información	Servicios Admistrados SOC
1	Ecuador	Seguridad de información	Risk Advisory & Cyber-Risk Services

RIESGOS MÁS FRECUENTES

Phishing: el rey de los males



1. China 20.22%

2. Brasil 18.63

3. Argelia 14.3%

4. Inglaterra 12.95%

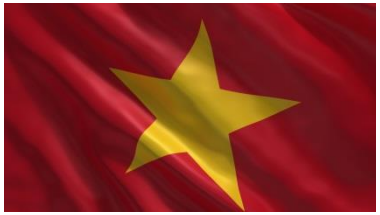
5. Australia 12.77%

Top 10 de países, de acuerdo al número de usuarios. Kaspersky Lab, 2016

asobanca
Asociación de Bancos del Ecuador

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre

Phishing: el rey de los males



6. Vietnam 11.46%

7. Ecuador 11.14%

8. Chile 11.08%

9. Catar 10.97%

10. Maldivas 10.94%

Top 10 de países, de acuerdo al número de usuarios. Kaspersky Lab, 2016

asobanca
Asociación de Bancos del Ecuador

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre

Malware, virus, troyanos, etc.

Intentos de ataque por usuarios conectados	
País	**Porcentaje**
Brasil	49,9%
Perú	41,9%
Bolivia	41,8%
Chile	40,0%
México	39,9%
Colombia	39,3%
Guatemala	37,5%
Ecuador	36,1%
Venezuela	36,0%
Uruguay	30,0%
Argentina	29,5%

Fuente: Kaspersky Lab 2017

Robo de identidad y clonación de tarjeta

1. Brasil

2. México

3. Colombia

Fuente: Kaspersky Lab 2017

asobanca
Asociación de Bancos del Ecuador

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre

Delitos violentos

"No dejan de preocupar los delitos violentos que son los de mayor impacto social y pueden afectar mucho más la imagen institucional que es presa de este tipo de delitos, como ser los Asaltos Bancarios que se da cuando existen clientes en el interior de las oficinas y el Robo Bancario que no es más que otra cosa que una intrusión a través de forados o túneles para acceder a las bóvedas de los bancos." (Consultor de seguridad, Bolivia).

FALENCIAS EN SEGURIDAD BANCARIA EN AMÉRICA LATINA

Institución

No existen un sistema de gestión de riesgos

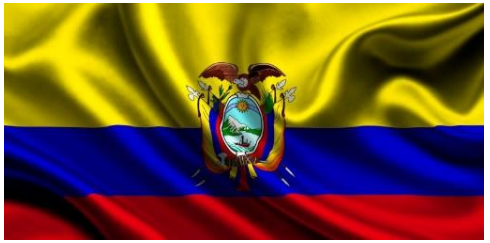
- *"No existe un sistema de gestión que le permita detectar y monitorear los riesgos. La perspectiva proactiva de mantener una red o un sistema lo más seguro posible es una carrera infinita. Los actores de la banca tienen que dedicar recursos y esfuerzos para mantener adecuados sus sistemas."* (Especialista en seguridad informática, USA/Colombia)

Institución

El enfoque proactivo ha fracasado

- *"Una empresa criminal busca esas vulnerabilidades. Siempre va a existir una carrera en descubrir una vulnerabilidad determinada. Y esa carrera en algún momento se va a perder. Siempre va a existir la amenaza de la empresa criminal. Tienen un balance, un modelo de negocio, reparten utilidades, se van de vacaciones. El enfoque proactivo ha fracasado. Hay que ir a un enfoque reactivo, donde yo tengo que entrenar a mi gente para que pueda reaccionar a un ataque cibernético."* (Especialista en seguridad informática, USA/Colombia).

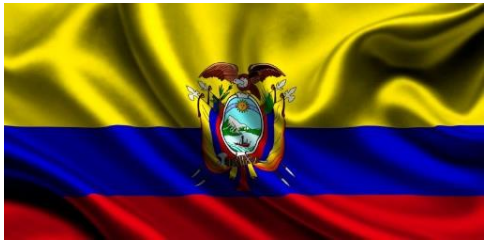
Institución



Aprendizajes “a fuerza”

- *“México y Brasil en un nivel un poco más alto. Les ha tocado a la fuerza, por la magnitud de la población. No es lo mismo atacar a Uruguay que atacar a México. La probabilidad de éxito es mucho más alta. Les ha tocado aprender a la fuerza.”* (Especialista en seguridad informática, USA/Colombia)

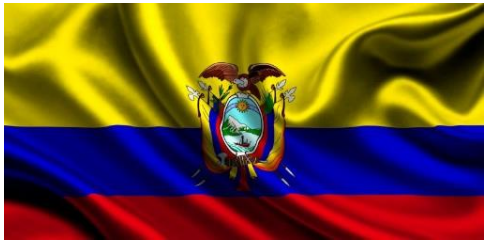
Institución



Falta personal capacitado

- *"Hay una vulnerabilidad importante. Falta personal capacitado, especialmente en Ecuador, es muy complicado encontrarlos. El profesional debe ser muy dinámico porque las vulnerabilidades cambian."* (Especialista en seguridad informática, USA/Colombia)

Institución



Delincuencia transnacional fortalecida

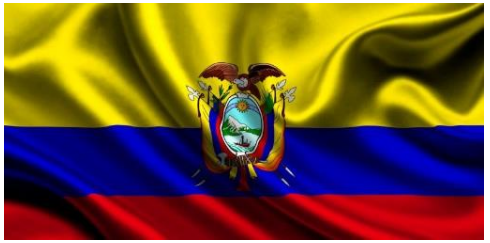
- *"Yo creería que los más expuestos serían siempre los canales electrónicos, siempre es más fácil materializar un evento o un ataque en aquellos canales donde mi exposición física sea mínima, esto quiere decir que es más vulnerable una página transaccional, esta tendencia actual que hay a nivel de los celulares, donde simulan una aplicación válida y tú la descargas desde las tiendas oficiales inclusive y sucede que debajo de esa descarga tu teléfono queda comprometido tienes un troyano dentro y no te has dado cuenta porque es imperceptible para el usuario, tu teléfono forma parte de una red de zombis donde frecuentemente le están información a China, Rusia que la mayoría de estos vienen de allá."* (Especialista en Seguridad de la Información, **Venezuela**).

Usuarios

Los usuarios son más vulnerables que los propios bancos

- *"Los ciberdelincuentes ven más atractivo dirigir sus ataques directamente a los clientes bancarizados debido a que no es desconocido que en América Latina por las características propias de la región, es muy difícil crear conciencia y cultura de seguridad informática entre la población."* (Especialista en ciberseguridad bancaria, **Colombia**)

Usuarios



Falta cultura de seguridad bancaria

- *"El tema es culturizar, el dinero electrónico podría ser una solución para todos estos temas violentos, aunque el día de mañana te engañarán y te pedirán que transfieras a otra cuenta, nunca vamos a dejar de tener este tipo de agresiones; pero si disminuirá el momento en que perdamos la costumbre de sacar el dinero en efectivo para ir a comprar un auto, por ejemplo."* (Especialista en riesgos violentos, Ecuador)

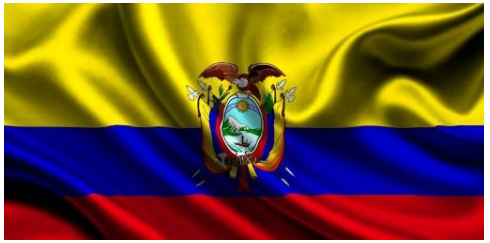

LEGISLACIÓN

Avances en la legislación

Colombia a la vanguardia de la legislación

- *"Colombia a la vanguardia, los fiscales y los jueces tienen más experiencia. Esto disuade al delincuente. Hay una política cibernética. Policia cibernética. Falta el tema penal más fuerte. El gobierno debe dar lineamientos al sector privado para saber que hacer."* (Especialista en seguridad informática, USA/Colombia)

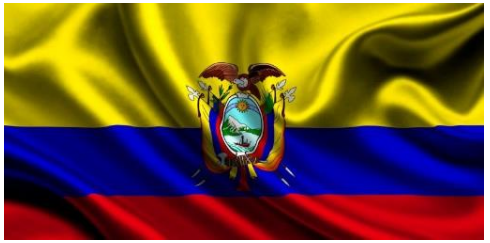
Limitaciones en la legislación



Penas débiles

- *"Colombia fue pionera. Ecuador tiene algo similar, hace dos años con el COIP. Dio una visión. Pero considero que las penas son ridículas. Penas de 5 años, 3 años; y en relación al dinero que puedo ganar. Hay pocas probabilidades que me detecten, tengo alta probabilidad de éxito. Y si me descubren, la aplicación de la ley es complicada porque los jueces y los fiscales no tienen conocimiento, no conocen de la tecnología. La ley no es disuasiva."* (Especialista en seguridad informática, USA/Colombia)

Limitaciones en la legislación



Operadores de la justicia sin conocimiento de riesgos de seguridad cibernética

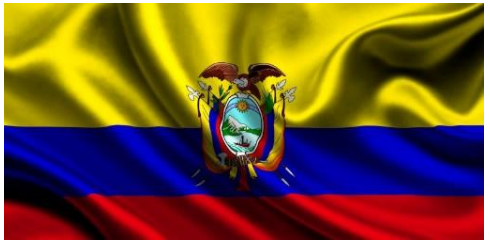
- *"Además de las penas, se debe entrenar. Es imposible que un abogado conozca del tema tecnológico. Es más factible que un técnico conozca más de leyes. El perito debe estar muy bien entrenado. Por cualquier ambigüedad, el criminal puede quedar libre."* (Especialista en seguridad informática, USA/Colombia)

Limitaciones en la legislación

Vacíos legales en materia de ciberseguridad

- *"Nos falta regular sobre comercio electrónico, pasarelas de pago etc., ya que el fraude de comercio electrónico es una de las mayores tipologías de fraude, la cual adolece de una regulación, así mismo algunas entidades financieras carecen de un SOC (Security operation center) que permita monitorear, generar alertas tempranas y prevenir ataques externos a la infraestructura tecnológica de la organización."* (Especialista en ciberseguridad bancaria, Colombia)

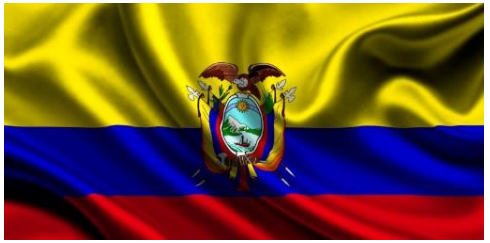
Limitaciones en la legislación



Hecha la ley, hecha la trampa

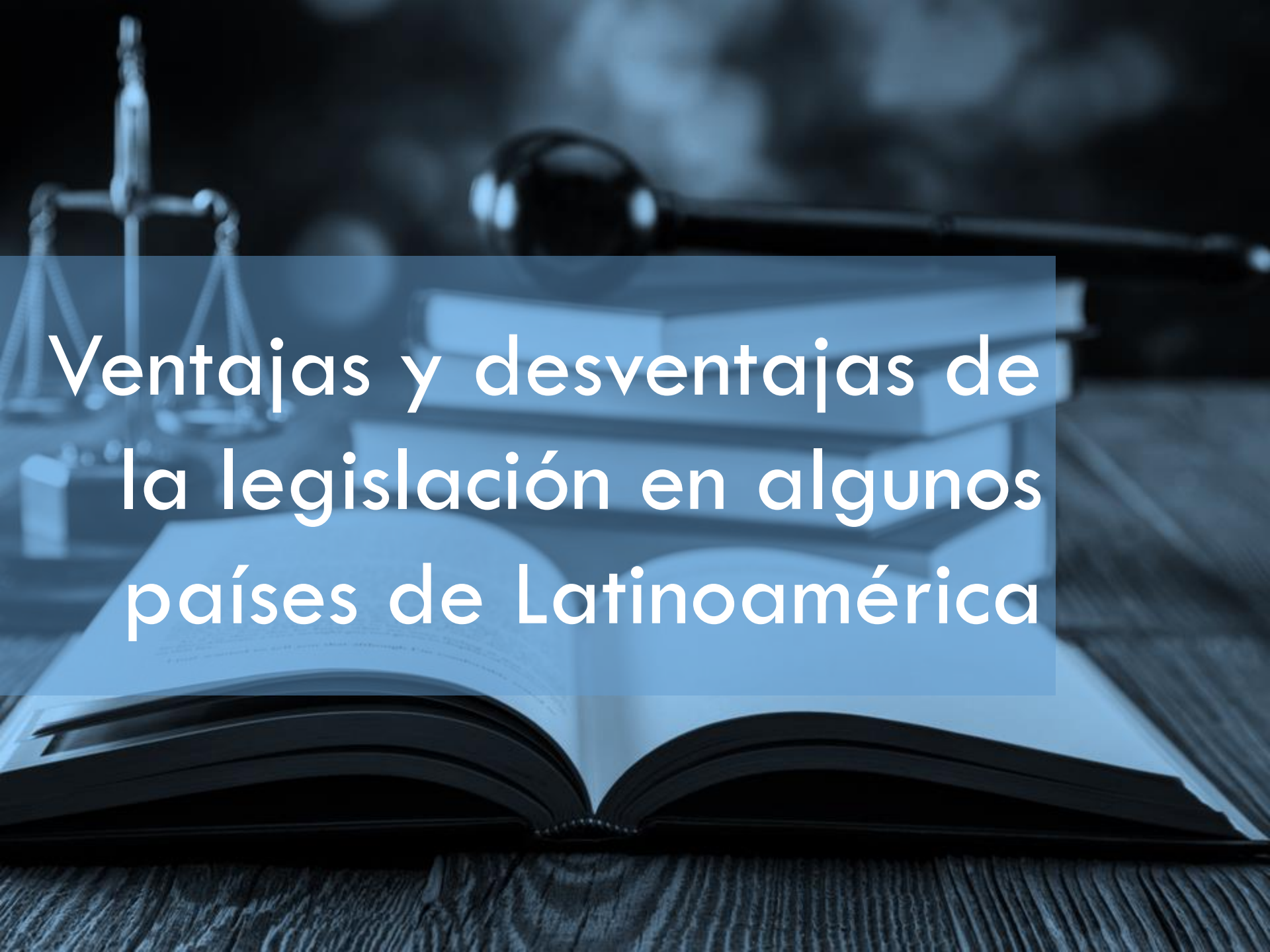
- *"Los delitos migran, evolucionan, son dinámicos y la ley no está al mismo ritmo; además no hay especialización puntual de la justicia (personeros) en ello."* (Especialista de seguridad financiera, Ecuador)

Limitaciones en la legislación



No existe un buen nivel de articulación regional

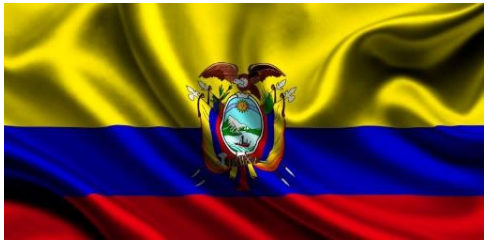
- *"…Ideal que normativa de delitos informáticos tuviera alcance internacional. La mayoría de ataques se encuentran alojados en servidores comprometidos en el extranjero, cuyos gobiernos son exigentes y se muestran poco colaborativos a la hora de desmontar o de cooperar con las labores de neutralización y desmonte de las amenazas que afectan a los clientes de nuestro país. Para concretar la idea se requieren formalizar alianzas con las autoridades competentes de cada país y generar sinergias que conlleven a la neutralización inmediata de las amenazas, al seguimiento, localización y captura de los individuos responsables."* (Especialista en ciberseguridad bancaria, Colombia)



Ventajas y desventajas de la legislación en algunos países de Latinoamérica

PAÍS	LEGISLACIÓN	VENTAJAS	DESVENTAJAS
Colombia	Ley 1273 de 2009 delitos informáticos. Ley 1776 de 2016 regula las cuentas abandonadas, inactivas por más de 3 años ininterrumpidos. Ley 1266 del 2008 ley de habeas data. Circular 052 modificada por la 042 requerimientos mínimos de seguridad y calidad para la realización de operaciones, seguridad de la información. Decreto 587 del 11 de abril de 2016: Reversión de transacciones con dinero fraudulentos. Ley 1581 de 2012, protección de datos personales.	Es uno de los países más avanzados de la región en cuestión de legislación.	No se ajusta a la realidad del país. Falta de compromiso de las autoridades. Poco conocimiento de las autoridades en el tema. Sanciones muy leves. No existe articulación regional.
Ecuador	Código orgánico integral penal (COIP). Resoluciones: -JB 2012 2148. -JB 2014 3066. - JB-2005-834. (Actualizándose) -SB 2016 940. PCI – Tarjetas de crédito en Ecuador. Ley 2148. Ley 3066.	La legislación toma referentes de la legislación Colombiana. Procedimientos maduros y consistentes. Se tipifican muchos nuevos tipos de delitos informáticos: -La transferencia de activo patrimonial. -El acceso a bases de datos. -La afectación de infraestructura tecnológica de forma voluntaria.	Ambigua. Confunde a las autoridades a la hora de dictar una sentencia. Los delitos evolucionan más rápido que la ley. Responde a una realidad ajena. Penas insignificantes. Falta de personal capacitado para ejecutar la ley. La norma está demasiado acotada, dificulta la fluidez del canal electrónico.
Bolivia	Normas del Sistema Financiero – ASFI: Requisitos mínimos de seguridad. Reglamento para la Gestión de Seguridad Física.	Ha mejorado en los últimos años, teniendo en cuenta que hasta el 2011 no existía una normativa específica.	Falta de personal capacitado para implementar la normativa.
Venezuela	Ley de Tarjetas de Crédito, Débito, Pre-pagadas y Demás Tarjetas de Financiamientos o Pago Electrónico. Ley general de bancos y otras Instituciones financieras. Ley especial contra los delitos informáticos.	Visitas anuales del regulador.	Matices políticos complicados. Los delincuentes siempre están un paso delante de lo que tipifica la ley.

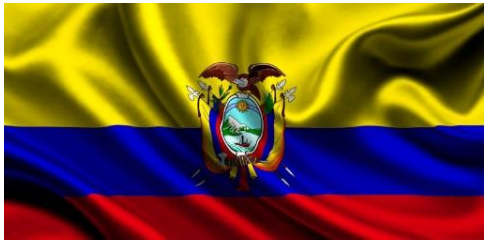
Desafíos para la seguridad bancaria



Adoptar un sistema de gestión de riesgos violentos y no violentos

- *"No hay una bala de plata para detener estas amenazas. Una buena práctica es adoptar un buen sistema de gestión. Y que conforme a eso pueda determinar sus planes de tratamiento."* (Especialista en seguridad informática, USA/Colombia)

Desafíos para la seguridad bancaria



Generar conciencia acerca de la importancia de la seguridad bancaria

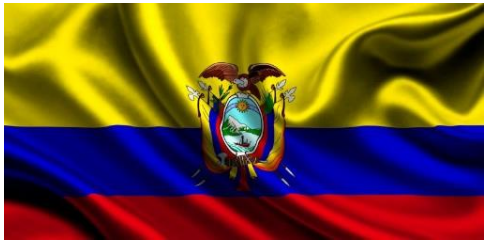
- *"Considero que la mejor practica en materia de seguridad bancaria es la creación de conciencia de cultura se seguridad, es dar a conocer a las empresas y clientes bancarios las diferentes amenazas en torno a la seguridad bancaria mediante presentaciones teóricas y prácticas que toquen la sensibilidad de las personas."* (Especialista en ciberseguridad bancaria, Colombia)

Desafíos para la seguridad bancaria

Monitoreo permanente y cooperación interbancaria

- *"El monitoreo en tiempo real, analítica, cooperación entre los bancos y el trabajo articulado con autoridades, la transferencia de conocimiento hacia fiscales y jueces ha permitido la desarticulación de estructuras delincuenciales."* (Especialista en ciberseguridad bancaria, Colombia)

Desafíos para la seguridad bancaria



Comités de seguridad bancaria

- *"Considero una buena práctica la conformación de los Comités de Seguridad Bancaria, ello coadyuva en alcanzar los objetivos que cada institución tiene en el marco de la seguridad" (Experto en seguridad, Bolivia)*


PROYECCIONES

Proyecciones

Delitos cibernéticos el ingreso más rentable del futuro

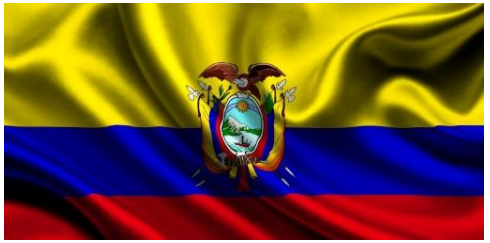
- *"Hoy, el mayor delito es el trafico de drogas. Se estima que para el 2030 sea la mayor fuente de ingresos para las organizaciones criminales. Eso nos pone en una posición incómoda en un futuro. Una regulación no debe atarse a una tecnología determinada, tiene que agregar una capa abstracta que permita a una compañía mitigar sus riesgos. El riesgo está, se debe identificar y ese es un tema de gestión."* (Especialista en seguridad informática, USA/Colombia)

Proyecciones

Modernizarse o morir

- *"Entonces la transformación digital va a generar un punto de quiebre un punto de inflexión en cuanto a cómo se hace un negocio y por ende esto va a ser normado por el ente aquí en Ecuador, ya hay bancos, conozco el caso de un banco mediano aquí en Ecuador, que ya está en proceso de transformación digital, ya entró a la banca digital, entonces el resto de bancos necesariamente para mantenerse competitivos, van a necesitar ingresar al proceso de transformación digital que no sólo se trata de meter tecnología a lo que ya haces, tienes que apalancarte en tecnología pero al mismo tiempo tú tienes que modificar procesos, estructuras etcétera."* (Especialista en Risk Advisory & Cyber-Risk Services, Ecuador).

Proyecciones



"Millennials" serán los clientes neurálgicos de la banca

- *"…acordémonos de algo muy claro de aquí a 20 años la mayoría de clientes del banco van a estar muertos se van a morir por causas naturales así de simple, los nuevos clientes van a hacer la nueva generación los millennials y los nativos digitales, yo no soy un millennial, pero yo siempre tengo este lema: la banca es algo que hago no es a donde voy yo ya no creo en las sucursales físicas, de los bancos obviamente hay ciertos trámites que tienes que ir presencialmente pero para eso ya vas a tener algo muy pequeño en el futuro la mayoría de trámites van a ser simplemente por el teléfono, por eso es algo hacia dónde la banca va a ir, la transformación digital, la banca digital y eso va a ser la próxima nueva regulación, al menos desde mi punto de vista aquí en Ecuador."* (Especialista en Risk Advisory & Cyber-Risk Services, Ecuador).

Alexis Alcántara

Manejo Delitos Patrimoniales en República Dominicana

	Instruidos/ Recomendados por	Aplicables a	Monitoreados por
Constitución	-Congreso Nacional. -Asamblea Constituyente.	Todas las organizaciones y personas.	-Poder ejecutivo. -Poder judicial.
Leyes	-Senado RD. -Camera de Diputados.	A cada sector o persona que le competa.	-Poder ejecutivo. -Poder judicial. -Sociedad misma.
Reglamentos/ Decretos / Resolusiones	-Poder Ejecutivo. -Banco Central. -Superintendencia de Bancos. -Asociación de Bancos.	Entidades de intermediacion Financiera.	-Poder Judicial. -Superintendencia. -Banco Central.

Manejo Delitos Patrimoniales en República Dominicana

Fortalezas

- Legislación y Regulación actualizada y en constante revisión.
- Seguimiento constante de las Autoridades Monetarias.
- Crecimiento sostenido de la Nación (estimacion 4% del PIB para 2017).
- Liquidez y solvencia del sector Financiero.
- Calificadoras de Riesgos con valoracón Positiva.

Manejo Delitos Patrimoniales en República Dominicana

Debilidades

- Temas Migratorios.
- Temas Judiciales / Riesgos Reputacionales.
- Inversiones en Seguridad Pública y Privada.

Manejo Delitos Patrimoniales en República Dominicana

Retos

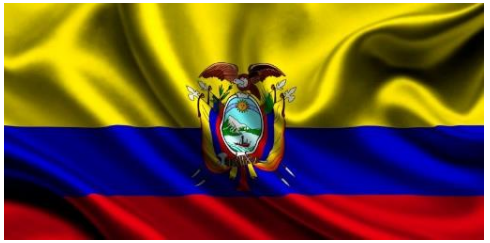
- Adecuación e inversión apropiada en CiberSeguridad.
- Controles de Migración.
- Fortalecimiento en Seguridad de nuestros portafolios de productos.
- Seguir evolucionando hacia las nuevas tecnologias aplicables al negocio.

¿Con qué contamos?

- Constitución de la Republica Dominicana.
- Código Penal de RD.
- Código Civil y Comercial de RD.
- Ley Monetaria y Financiera.
- Ley de delitos de Alta Tecnología.
- Ley de Lavados de activos.
- La voluntad del Sector.

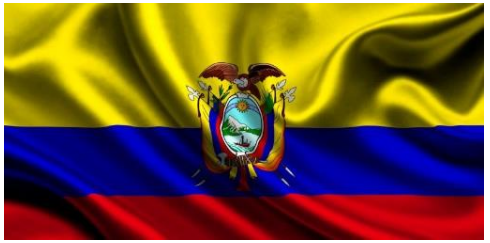
CONCLUSIONES

Conclusiones



- La subsistencia de riesgos violentos es una realidad en América Latina.
- Encontrar vacíos legales para cometer delitos cibernéticos.
- El desarrollo de la normativa es lento en comparación con el avance vertiginoso de nuevas modalidades de delitos en el ámbito financiero.
- Ser reactivo no debe ser sinónimo de ineficiencia.
- Crear cultura de seguridad bancaria en los usuarios es clave.

Conclusiones



- La Ley por si misma no es suficiente para reducir el riesgo.
- Es fundamental desarrollar capacidades en los especialistas de seguridad informática y operadores de justicia.
- Articulación regional para el desarrollo de alertas tempranas y legislación de alcance internacional.

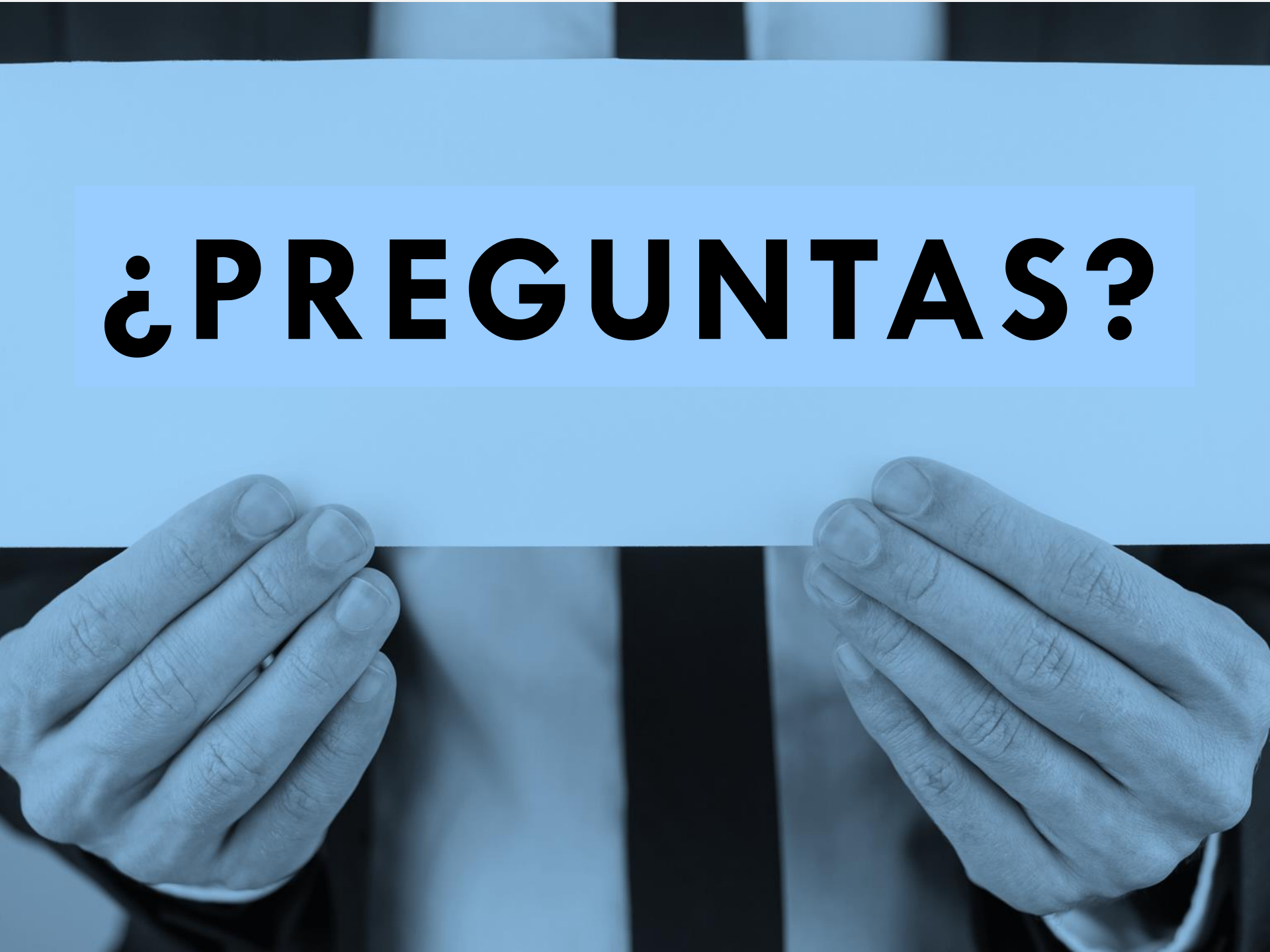
Conclusiones

Las legislaciones se deben adaptar a los cambios.

"NULLA PAEAN SINE LEGE PRAEVIA"

- No hay crimen sin ley previa / no hay delito sin Ley.

En la medida que podamos realizar una oportuna transferencia de informaciones, podremos evitar la propagación de males, actualizando nuestras líneas de defensas, apoyando a nuestros pares en la región y dándole seguridad a nuestras empresas, a nuestras familias y a nuestros Países.


¿PREGUNTAS?

asobanca
Asociación de Bancos del Ecuador

¡Muchas gracias!

CELAES XXXII ECUADOR 2017 Congreso Latinoamericano de Seguridad Bancaria 5-6 Octubre