XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACION DE BANCOS DEL PARAGUAY

Nuevas tendencias del Fraude Electrónico en sector financiero

Osvaldo Lau, MSI, CISA, CRISC, Cobit 5 Foundations, ISO, IIA Quality Assessment, Auditor Líder ISO 9001

Socio

Global Advisory Solutions

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

Osvaldo Lau C.

MSI, CISA, CRISC, Cobit 5 Foundations, ISO, IIA Quality Assessment, Auditor Líder ISO 9001

Socio de la firma Global Advisory Solutions, tiene como responsabilidad dirigir proyectos de Gobierno Corporativo, Riesgos y Cumplimiento, Auditoría Interna y de Sistemas, Control Interno y Gestión de Continuidad de negocios, restructuración y mejora de procesos, Gestión de Tecnología, Seguridad de la Información, evaluaciones basadas en marcos de referencia tales como Cobit, ITIL, ISO 2700, revisiones asociadas Sarbanes-Oxley, automatización de la gestión de auditoría interna, Cómputo Forense. Cuenta con más de 10 años de experiencia en las áreas de consultoría y auditoría mencionadas participando en proyectos a nivel nacional e internacional para diferentes tipos de industrias.

Cuenta con una maestría de "Computer Science de Texas A&M University", especialización en contabilidad, certificaciones internacionales de ISACA, Eccouncil, ISO, incluyendo una especialización en Internal Audit Quality Assessment del IIA Global en New York.

Global Advisory SOLUTIONS

FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

Agenda

Nuevas tendencias del Fraude Electrónico en sector financiero

- Introducción y antecedentes
- El nuevo panorama de tecnología
- El nuevo panorama de los servicios bancarios
- Responsabilidades del auditor interno
- Tendencias de fraude electrónico y responsabilidad del auditor
- Factor común del fraude electrónico
- Matriz de riesgos tecnológico
- Conclusiones

FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACION DE BANCOS DEL PARAGUAY

INTRODUCCÓN

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

INTRODUCCIÓN

Fra
bar
Delit
San
CALIFICA
JUAN PA
Al men
corresp
de las p
IMAGENE
Algun
banca
implen
como
dinám
virtua
fraud

Más de 700 horas se invierten para revertir el robo de identidad

19 Septiembre, 2011 - 21:35 Credito:Redacción

Una persona tarda alrededor de 700 horas en librarse de un problema de robo de identidad, por lo que pueden pasar meses o incluso años en limpiar su imagen y recuperar su buen historial crediticio.

COMPARTIR

Promedio:

Sin votos aún

NOTAS RELACIONADAS

Bancos deben mejorar atención a clientes

Precio de vivienda crece 5.35% en el DF

Seguros obligatorios y el papel de las autoridades (1 / 2)

Un seguro para cada etapa de la vida

El celular cambiará la forma de pago

ÚLTIMAS NOTICIAS

Fuente: http://www.eleconomista.com.mx/finanzas-personales/2011/09/19/mas-700-horas-se-invierten-revertir-robo-identidad

"Sabes? Esto sería más fácil si lo haces en línea"

FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior
"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enfoque que asegura el éxito organizacional"

XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

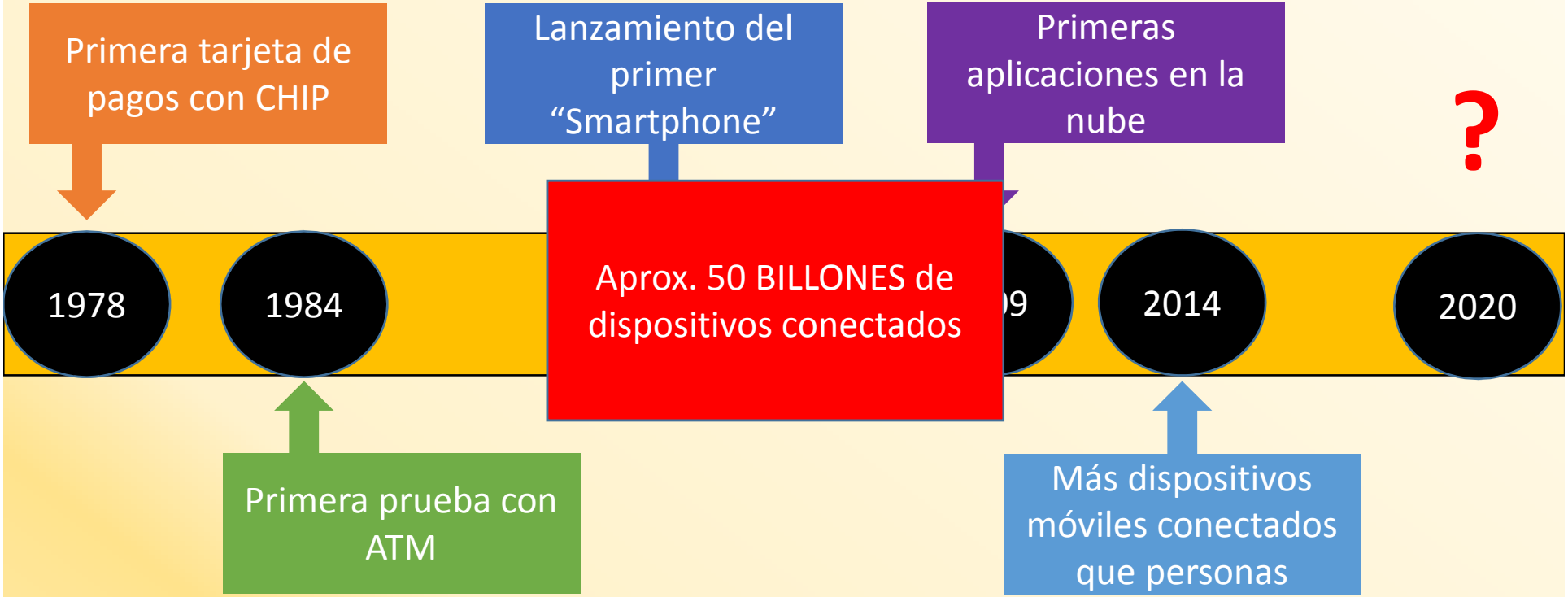
ASOCIACION DE BANCOS DEL PARAGUAY

EL PANORAMA DE TECNOLOGÍA

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

El nuevo panorama de tecnología



FELABAN

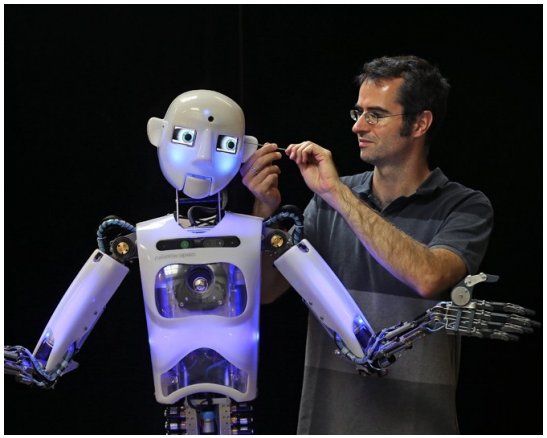
ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

El nuevo panorama de tecnología

1. Máquinas y robots están tomando un rol más activo en el mejoramiento de las actividades diarias de los humanos.
2. Los aspectos digitales están ayudando a hacer las decisiones económicas.
3. La renovación y cambio de experiencia del cliente es una prioridad digital.

Gartner®



FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

El nuevo panorama de tecnología

XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACION DE BANCOS DEL PARAGUAY

EL PANORAMA DE TECNOLOGÍA: Servicios Financieros

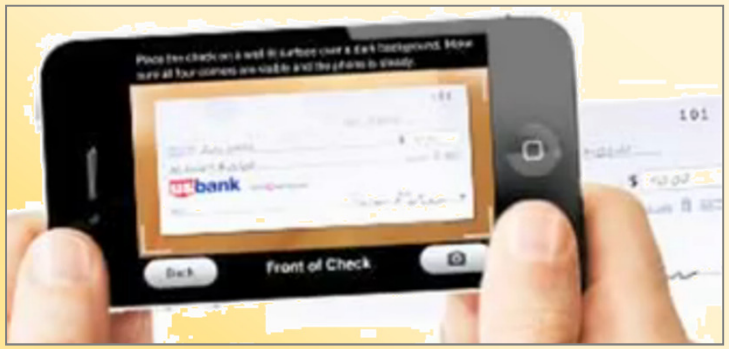
FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

El panorama de tecnología: servicios financieros

- Wallet electrónicos.
- Depósitos de cheques por teléfonos inteligentes.
- Retiros por cajeros con teléfonos inteligentes.

Google wallet



FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

El panorama de tecnología: servicios financieros

- Tecnología móvil
- APPs

El panorama de tecnología: servicios financieros

PERO….

No sólo la tecnología, está cambiando. El cliente/usuario está cambiando también….

LOS NIÑOS DE HOY EN DÍA SABEN UTILIZAR TODO TIPO DE DISPOSITIVOS ANTES DE APRENDER A CAMINAR

XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACION DE BANCOS DEL PARAGUAY

RESPONSABILIDAD DEL AUDITOR INTERNO

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Normas para la práctica profesional de Auditoría Interna

NORMA 1210.A2 – APTITUD PROFESIONAL REQUERIDA POR EL AUDITOR

Los auditores internos deben tener conocimientos suficientes para evaluar el riesgo de fraude y la forma en que se gestiona por parte de la organización, pero **no** es de esperar que tengan conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección e investigación del **fraude**.

FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

Normas para la práctica profesional de Auditoría Interna

NORMA 2120.A2 – GESTIÓN DE RIESGOS

La actividad de auditoría interna debe evaluar la posibilidad de **ocurrencia de fraude** y cómo la organización maneja gestiona el riesgo de fraude.

NORMA 2210.A2 – OBJETIVOS DEL TRABAJO

El auditor interno debe considerar la probabilidad de errores, **fraude**, incumplimientos y otras exposiciones significativas al elaborar los objetivos del trabajo.

Responsabilidades del Auditor

- Mantener un escepticismo profesional manteniendo un entendimiento a la susceptibilidad de la entidad al fraude
- Planear y entrevistarse con la administración para conocer:
  - Cómo previenen la ocurrencia del fraude
  - Si existe información de algún fraude conocido
  - Si ha habido algún error de importancia en el periodo
  - La administración sobre el sistema de contabilidad y sus controles
  - El auditor interno debe considerar la probabilidad de errores, fraude, incumplimientos y otras exposiciones significativas al elaborar los objetivos del trabajo.

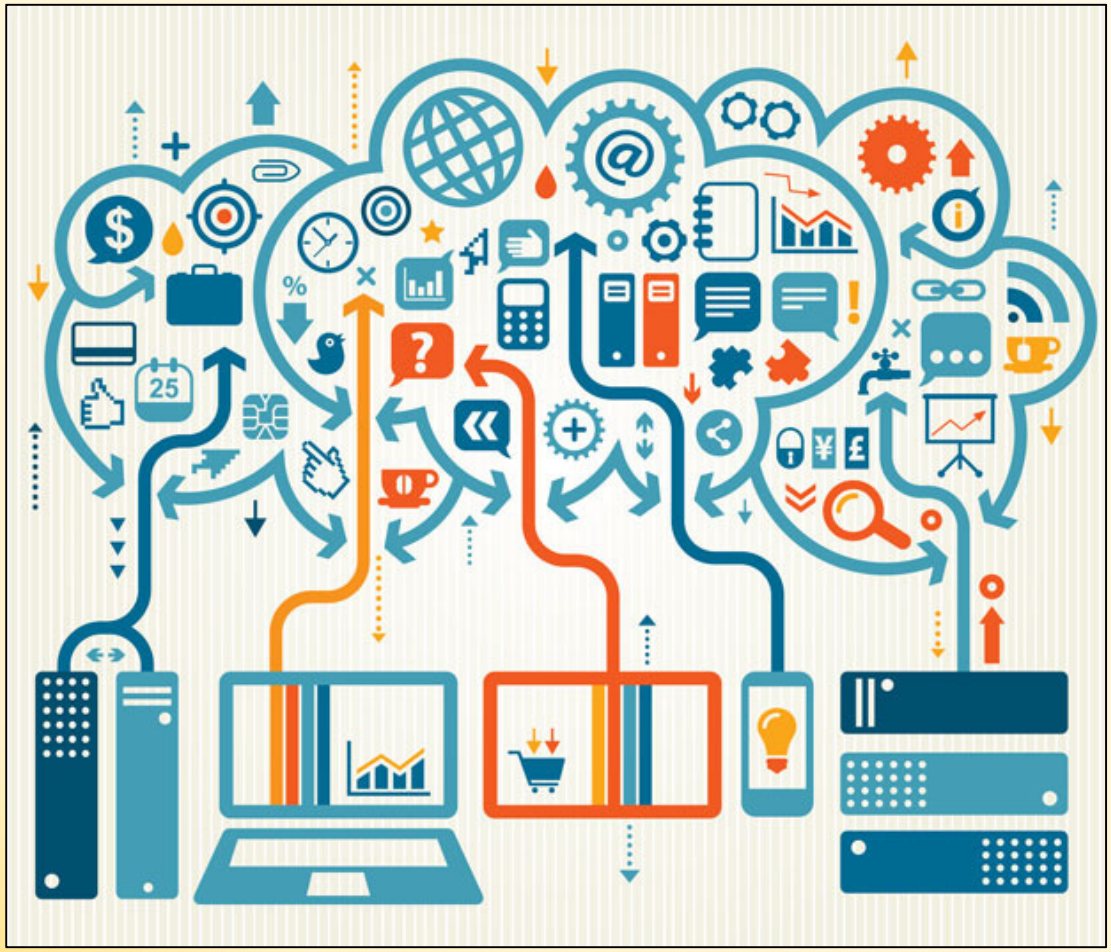
Fuente: Normas Internacionales de Auditoría NIA

Responsabilidades del Auditor

- Responsabilidad de los auditores en la prevención y detección del fraude:
  - Esta revisión debería ser llevada acabo por expertos forenses quienes podrían hacer una investigación profunda del fraude que permitiría identificar los responsables y cómo se pudieron llevar a cabo estas actividades.
  - Esto es importante dado que dependiendo de los eventos sucedidos, podría ser requerido el uso de herramientas especializadas y una metodología de investigación forense con lo cual se lograría recopilar evidencia de una manera tal que pueda ser utilizada en una corte de ley.

Fuente: Normas Internacionales de Auditoría NIA

Internet de las cosas



XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACION DE BANCOS DEL PARAGUAY

TENDENCIAS DE FRAUDE ELECTRÓNICO Y RESPONSABILIDAD DEL AUDITOR

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

Ransomware

- El ejercicio de “secuestrar” un activo de tecnología (datos, una red, un sistema, etc.) y un criminal toma control del activo hasta que pague un monto de rescate.

Ransomware

¿QUÉ RIESGOS HAY?

- Perder el acceso para utilizar información, aplicaciones o equipos informáticos para su destino final.
- Inmediato impacto reputacional al no poder brindar un servicio a los clientes.

Por ejemplo…

Ransomware

¿QUÉ DEBE HACER EL AUDITOR?

- Auditor la realización de respaldos frecuentes de los datos e información crítica del negocio, así como dispositivos de respaldo para evitar dependencia de un punto específico.
- Evaluar la actualización de los medios de seguridad (antivirus, por ejemplo) en los equipos de usuarios finales.
- Confirmar la existencia de controles para evitar instalación de programas sin permisos del administrador.

Riesgos en RDC (Remote Deposit Capture)

- RDC – Captura de Depósito Remoto: Servicio bancario que permite al cliente hacer un depósito en su cuenta con sólo enviar una imagen de un cheque mediante un canal encriptado.

Riesgos en RDC (Remote Deposit Capture)

¿QUÉ RIESGOS HAY?

- En el 2020, se espera que haya más de 2 Billones de usuarios de servicios bancarios dispositivos móviles

  Fuente: Juniper Worldwide Digital Banking report

- El uso de servicios RDC aumentará en un 98% en el sector bancario.

  Fuente: Celent State of Remote Deposit Capture 2015 report

FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

Riesgos en RDC (Remote Deposit Capture)

¿QUÉ DEBE HACER EL AUDITOR?

- Revisar el monitoreo de la dirección IP utilizada para conectarse al servidor del banco.
- Analizar y auditar la frecuencia de los “log-in” a la cuenta bancaria.
- Identificar y analizar patrones de apertura y consulta a cuentas nuevas.
- Utilizar herramientas de análisis de datos para realizar pruebas asistidas por computador.

Robo de identidad por medios inalámbricos.

- RFID o “Radio Frequency Identificator” habilita la posibilidad de hacer pagos de tarjetas de crédito con sólo mostrar o acercar la tarjeta al POS.

Riesgos en RFID o “Radio Frequency Identificator”

¿QUÉ RIESGOS HAY?

- Lectura inalámbrica de los datos de la tarjeta de crédito (número, fecha de expiración, etc.).

Por ejemplo…

Robo de identidad por medios inalámbricos.

¿QUÉ DEBE HACER EL AUDITOR?

- Auditar la existencia y eficiencia de un programa de educación y concientización de seguridad a los clientes del banco y sus empleados.
- Sugerir la utilización y distribución de sobres para proteger la señal RFID de las tarjetas.

Phishing y Malware

- Engañar al usuario y hacerle creer que está ingresando sus credenciales en un sitio web o página del banco falsificada.

FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

Phishing y Malware

¿QUÉ RIESGOS HAY?

- Otorgar las credenciales de acceso a personal no autorizado.
- Reducir la capacidad de trazabilidad de las transacciones fraudulentas.

Por ejemplo…

Phishing y Malware

¿QUÉ DEBE HACER EL AUDITOR?

- Sugerir aumentar los boletines de concientización del usuario y cliente bancario, alertando de los diferentes tipos de phishing que pueden haber.
- Auditar los métodos de autenticación y sugerir un factor de autenticación dinámico para reducir los riesgos de transacciones no autorizadas.

XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

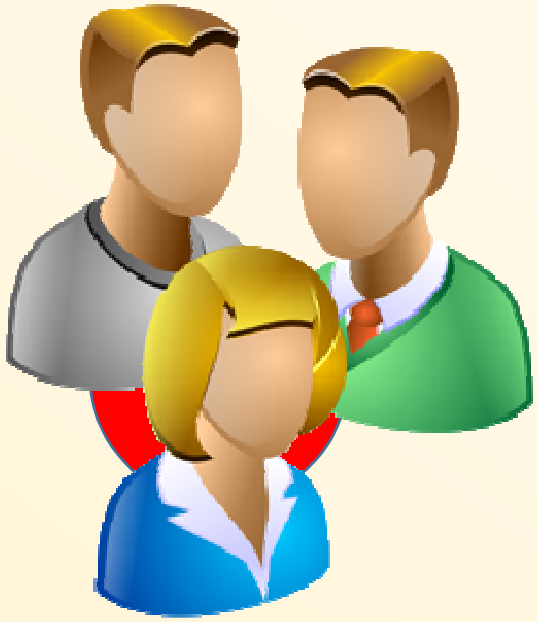
ASOCIACION DE BANCOS DEL PARAGUAY

FACTOR COMÚN

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Prevención de fraude: ¿Factor Común?

- Robo de identidad
- Remote Deposit Capture
- Phishing y Malware
- Ransomware



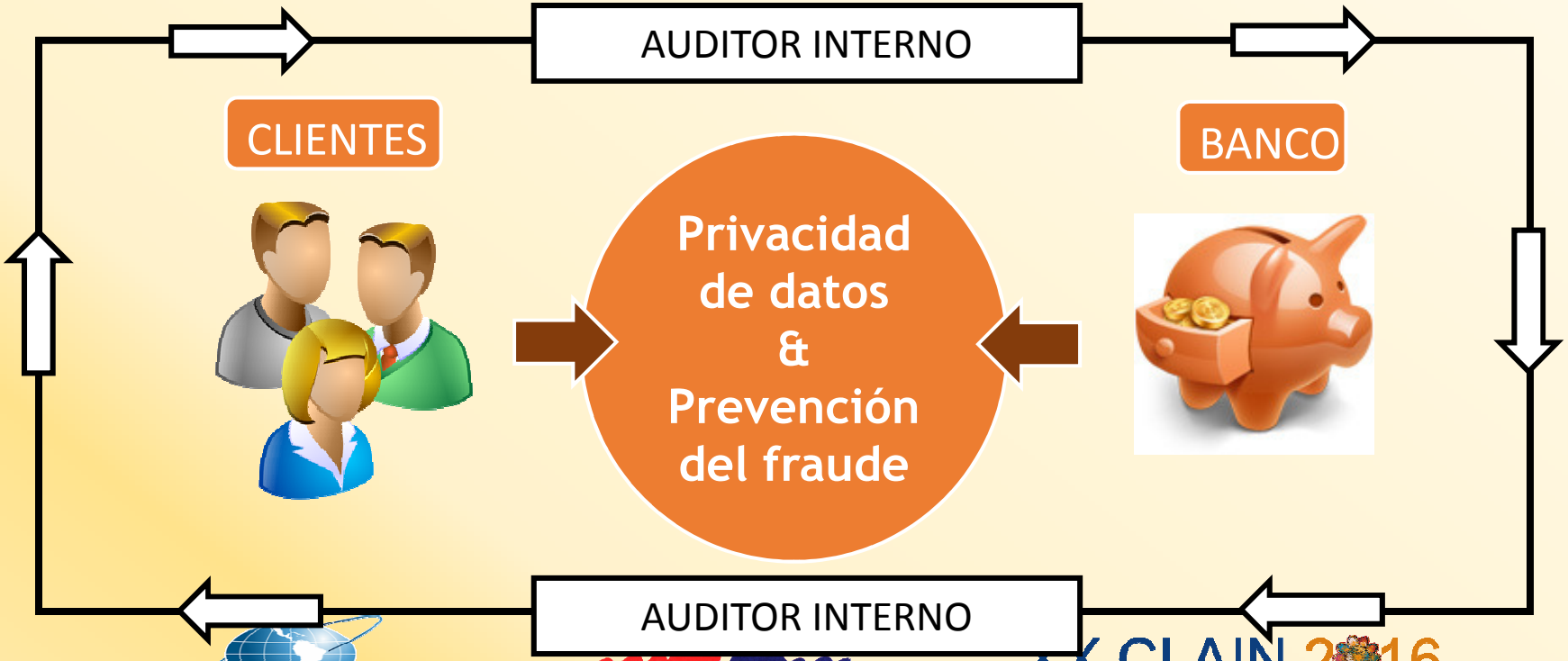
FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

Prevención de fraude: ¿Quién es el responsable?

- Una actividad en conjunto entre la institución bancaria y el cliente para crear un ambiente para la prevención del uso inadecuado o no autorizado de recursos tecnológicos para tomar ventaja sobre una persona o entidad financiera.



XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACION DE BANCOS DEL PARAGUAY

MATRIZ DE RIESGOS - EJEMPLO

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

Matriz de Riesgos - Ejemplo

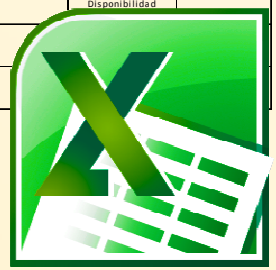
Mantener una matriz de riesgos para la clasificación de datos que ayude a determinar su nivel de privacidad y manejo

- Una matriz debe existir para poder tener un inventario de los activos de información que ayude a administrar los riesgos que pueden afectar la privacidad de los datos.

ACTIVO AFECTADO		MANEJO DE INFORMACIÓN			
Nombre del activo	Clasificación	Confidencial	Privada	Pública	Dueño
Base de datos ABC	Información	X			Juan Sánchez
Registro de cuentas y clientes XYZ	Información	X			Juan Sánchez
Servidor 2	Equipos				Osvaldo Lau
Política de compras	Información			X	Osvaldo Lau

RIESGO			RIESGO INHERENTE		
REF.	Título del Riesgo	Descripción del Riesgo	Probabilidad	Impacto	Calificación
R1	Acceso no autorizado	Acceso no autorizado a la información, aplicaciones o sistemas del banco	Bajo	Bajo	Riesgo Aceptable
R2	Continuidad	Indisponibilidad a la información o servicios de tecnología de información	Bajo	Medio	Riesgo Aceptable
R3	Falta de documentación	Falta de documentación, políticas o procedimientos formales para administración de recursos tecnológicos	Medio	Alto	Riesgo Moderado
R4	Recuperación de info	Incapacidad para recuperar o restaurar información, sistemas o servicios de tecnología	Muy Alto	Bajo	Riesgo Tolerable

CONTROLES MITIGANTES		
Controles	Criterio de Control	Dueño del Control
	Confidencialidad	
	Disponibilidad	

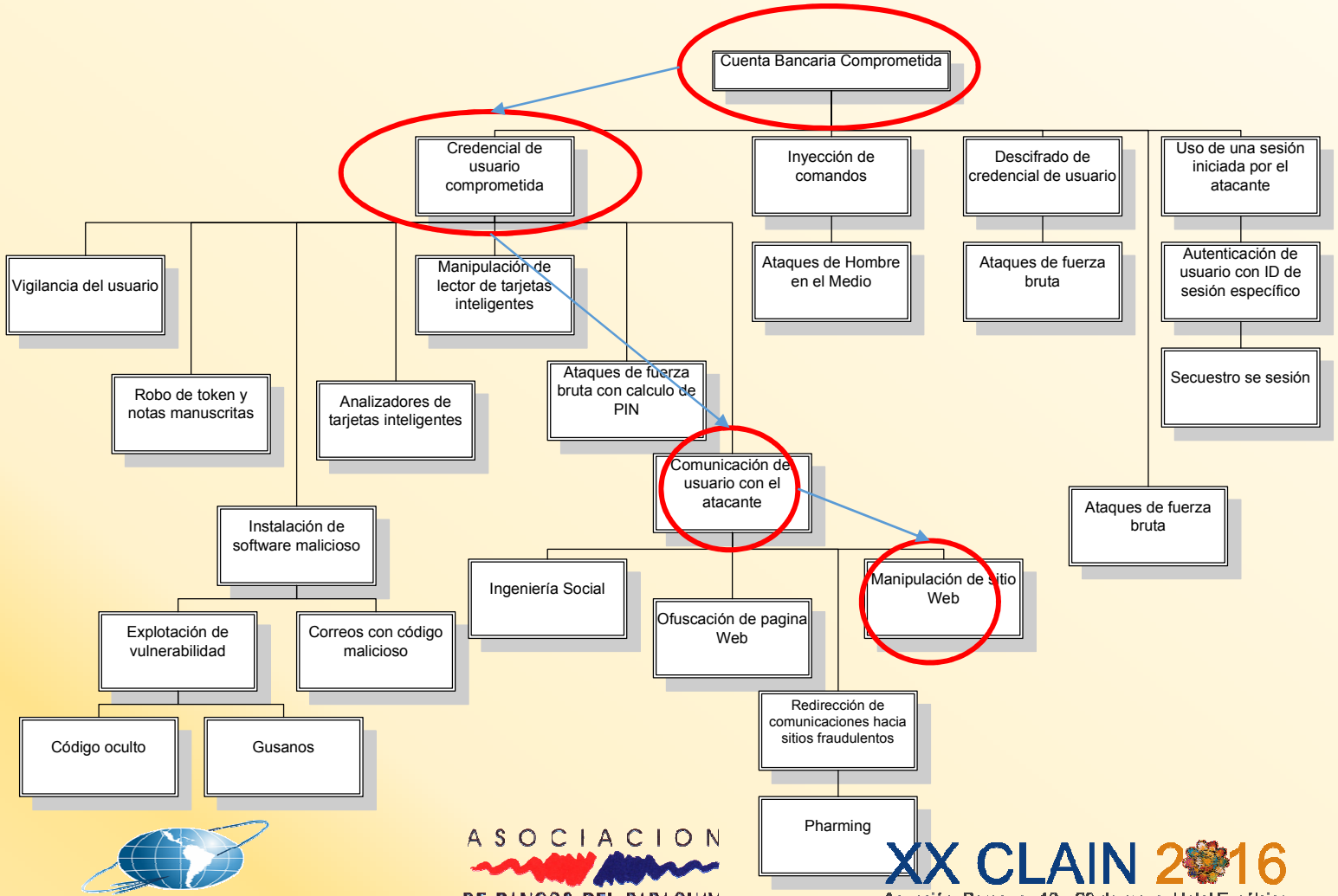


Árbol para analizar ataques: Procedimiento para respuesta a incidentes

Un árbol de ataque ayuda a desarrollar una metodología para analizar la seguridad de los sistemas que manejan las transacciones.

Ayudan a responder a los cambios en la seguridad y los tipos de fraude.

Árbol para analizar ataques: Procedimiento para dar respuesta y auditar incidentes



FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

XX CLAIN 2016

Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enlace que asegura el éxito organizacional"

ASOCIACION DE BANCOS DEL PARAGUAY

CONCLUSIONES

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Conclusiones

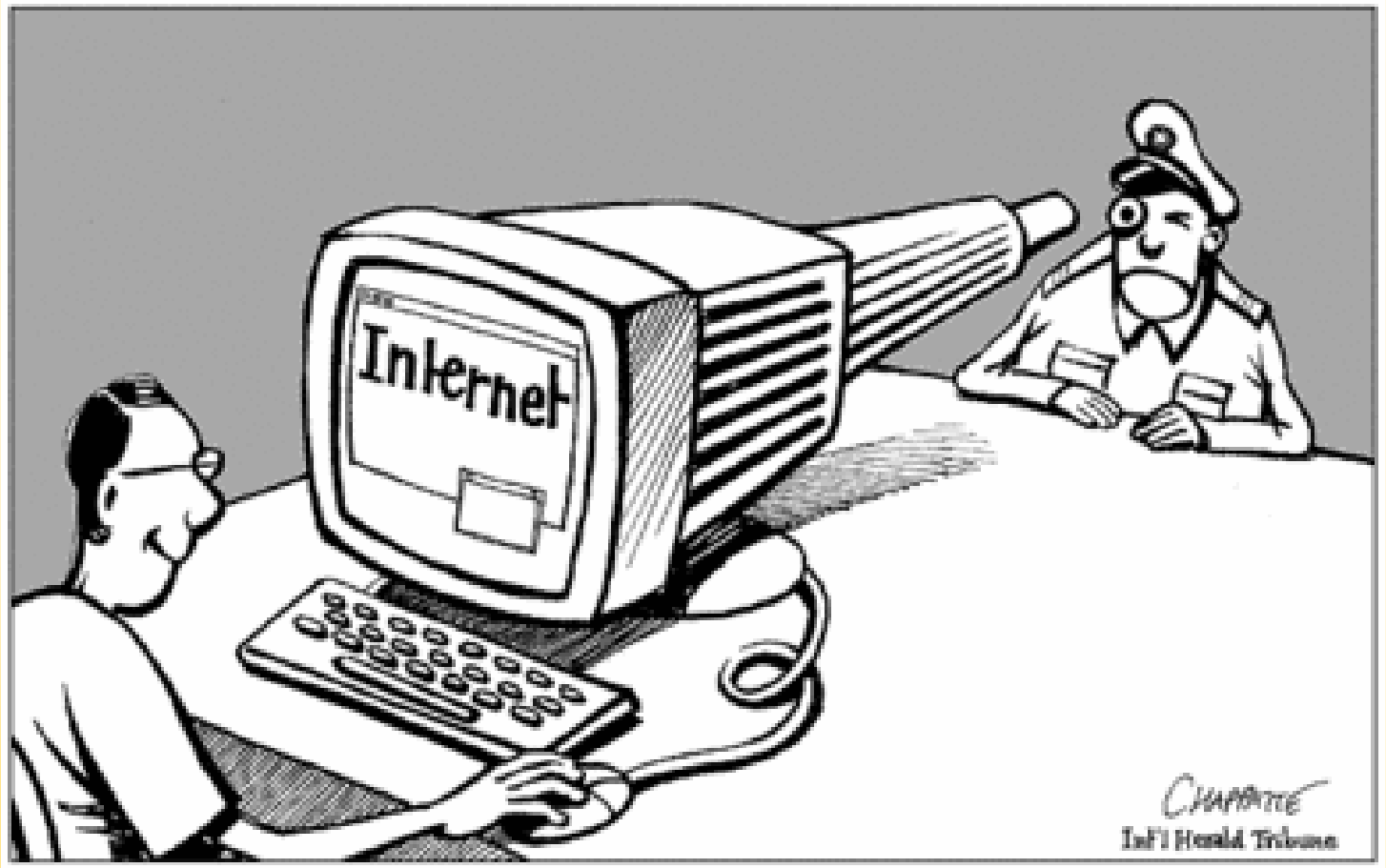
- Elaborar un plan de auditoría interna
  - Un plan de revisión mediante los recursos de auditoría interna es crucial para mantener un ambiente de control eficiente y detectar oportunidades de mejora.
- Educar, concientizar y enseñar!!
  - La seguridad inicia fundamentalmente con el cliente bancario. Si ellos no saben como aplicarla, todos los controles fallarán.
- Herramientas para detectar y analizar tendencias
  - No basta con herramientas para alertar la ocurrencia de brechas en la seguridad, es igual de importante analizar movimientos y accesos legítimos para identificar tendencias de fraude.

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior
"Gobierno Corporativo, Gestión de Riesgos y Auditoría, un enfoque que asegura el éxito organizacional"

Conclusiones



Información de Contacto

Osvaldo Lau C., MSI, CISA, CRISC, Cobit 5 Foundations, ISO, IIA Quality Assessment, Auditor Líder ISO 9001

Socio - Global Advisory Solutions

- olau@gloadso.com
- (507) 392.3200
- www.GLOADSO.com

FELABAN

ASOCIACION DE BANCOS DEL PARAGUAY

XX CLAIN 2016
Asunción, Paraguay 19 y 20 de mayo. Hotel Excélsior

Muchas Gracias

Por su Atención!