

TÉCNICAS PARA LA PREVENCIÓN DE FRAUDE ELECTRÓNICO EN INSTITUCIONES FINANCIERAS

XVII CONGRESO LATINOAMERICANO DE AUDITORÍA INTERNA Y EVALUACIÓN DE RIESGOS

Julio R. Jolly Moore, CFE, CRISC, CRMA, CGEIT, Internal Audit Quality Assessment
Socio BDO Consulting de BDO Panamá

&

Oswaldo Lau C., CISA, CRISC, Internal Audit Quality Assessment
Director BDO Consulting de BDO Panamá





Agenda

1. Introducción
2. El futuro y Fraude Electrónico.
3. Aspectos generales de fraudes electrónicos.
4. Fraudes electrónicos más comunes.
5. Árbol para analizar ataques.
6. ¿Qué se puede hacer para prevenir un fraude electrónico?
7. Prevención de Fraude Electrónico desde la perspectiva del Cliente y Comercio.
8. Prevención de Fraude Electrónico desde la perspectiva del Banco.
9. Conclusiones.

INTRODUCCIÓN

Técnicas para la prevención de fraude electrónico en instituciones financieras

FRAUDES BANCARIOS

Fraudes crecen en AL: expertos

30 Septiembre, 2010 - 16:10

La tecnología y la crisis económica impulsan el fraude, un delito que generó pérdidas de entre 18,000 y 20,000 millones de dólares durante el 2009 a nivel global, según expertos en seguridad bancaria.

En América Latina específicamente se ha visto un incremento en el fraude debido al aumento de la conectividad a Internet y el uso del teléfono móvil, señalaron los expertos reunidos en el Congreso de Seguridad Bancaria "Celaes 2010"

"Está aumentando el fraude electrónico en Latinoamérica porque está aumentando la conectividad", dijo José Antonio Martínez Rubio director para el sector financiero de la firma privada europea "BT" con clientes como Banco Central Europeo y la OTAN.

Indicó que la penetración de conexión móvil se incrementó en esa región 90% en la última década y que redes sociales como Facebook cuentan con 60 millones de usuarios.

"La conectividad es un hecho muy positivo para el progreso y los negocios, pero acarreará lacras como el fraude electrónico", advirtió Martínez Rubio en declaraciones a periodistas.

COMPARTIR

Promedio:

Sin votos aún

NOTAS RELACIONADAS

[Investigan tiroteo de Nueva Orleans](#)

["Responsables de escándalo de IRS deben rendir cuentas"](#)

[Siria culpa a Turquía por atentados con coche bomba](#)

[Consejo de Seguridad condena atentados en Turquía](#)

[EU y GB piden a Rusia cambiar posición sobre Siria](#)

ÚLTIMAS NOTICIAS

Fuente: <http://eleconomista.com.mx/internacional/2010/09/30/fraudes-crecen-expertos>

Página 4

© Todos los derechos reservados. Prohibida su reproducción no autorizada por BDO Consulting.



FRAUDES BANCARIOS

98 DENUNCIAS DE ESTE TIPO EN EL OIJ, DURANTE PRIMER SEMESTRE DEL 2011

Fraudes electrónicos encabezan la lista de estafas bancarias

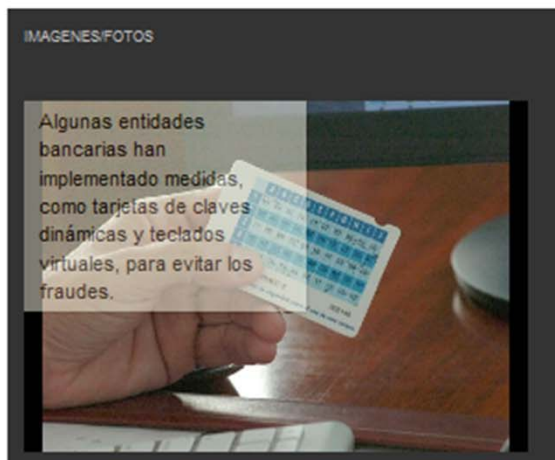
Delito corresponde a sustracción de fondos de tarjetas y cuentas de ahorro

San José es la provincia donde se presenta la mayoría de los reclamos

CALIFICACIÓN:	COMENTAR	0 COMENTARIOS	
---------------	----------	---------------	---

JUAN PABLO ARIAS | juan.arias@nacion.com | 12:00 A.M. 07/09/2011

Al menos 98 de las 166 denuncias por fraude bancario realizadas en el primer semestre de este año, corresponden a la sustracción de fondos de las tarjetas de crédito o débito, o de cuentas de ahorro, por medio de las plataformas en Internet de los entes financieros.



Según estadísticas del Organismo de Investigación Judicial (OIJ), este delito es seguido por la falsificación de tarjetas, con 54 denuncias, la alteración o “gemeleo” de cheques y la solicitud fraudulenta de plásticos, con cinco denuncias cada una; el resto de los reclamos fueron hechos por falsedad ideológica.

Además, Marisel Rodríguez, vocera del ente investigador, explicó que un 76% de las denuncias realizadas entre enero y junio de este año se hicieron en la provincia de San José.

Las otras áreas geográficas con mayor número de reclamos

Fuente: <http://www.nacion.com/2011-09-07/Economia/fraudes-electronicos-encabezan-la-lista----de--estafas-bancarias.aspx>

Página 5

© Todos los derechos reservados. Prohibida su reproducción no autorizada por BDO Consulting.



FRAUDES BANCARIOS

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

19 Septiembre, 2011 - 21:35 Crédito: 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.

Según datos de CPP, empresa que ofrece protección y asistencia contra el robo de identidad. Los delincuentes pueden realizar diversos delitos al robar **la** identidad de otras personas.

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

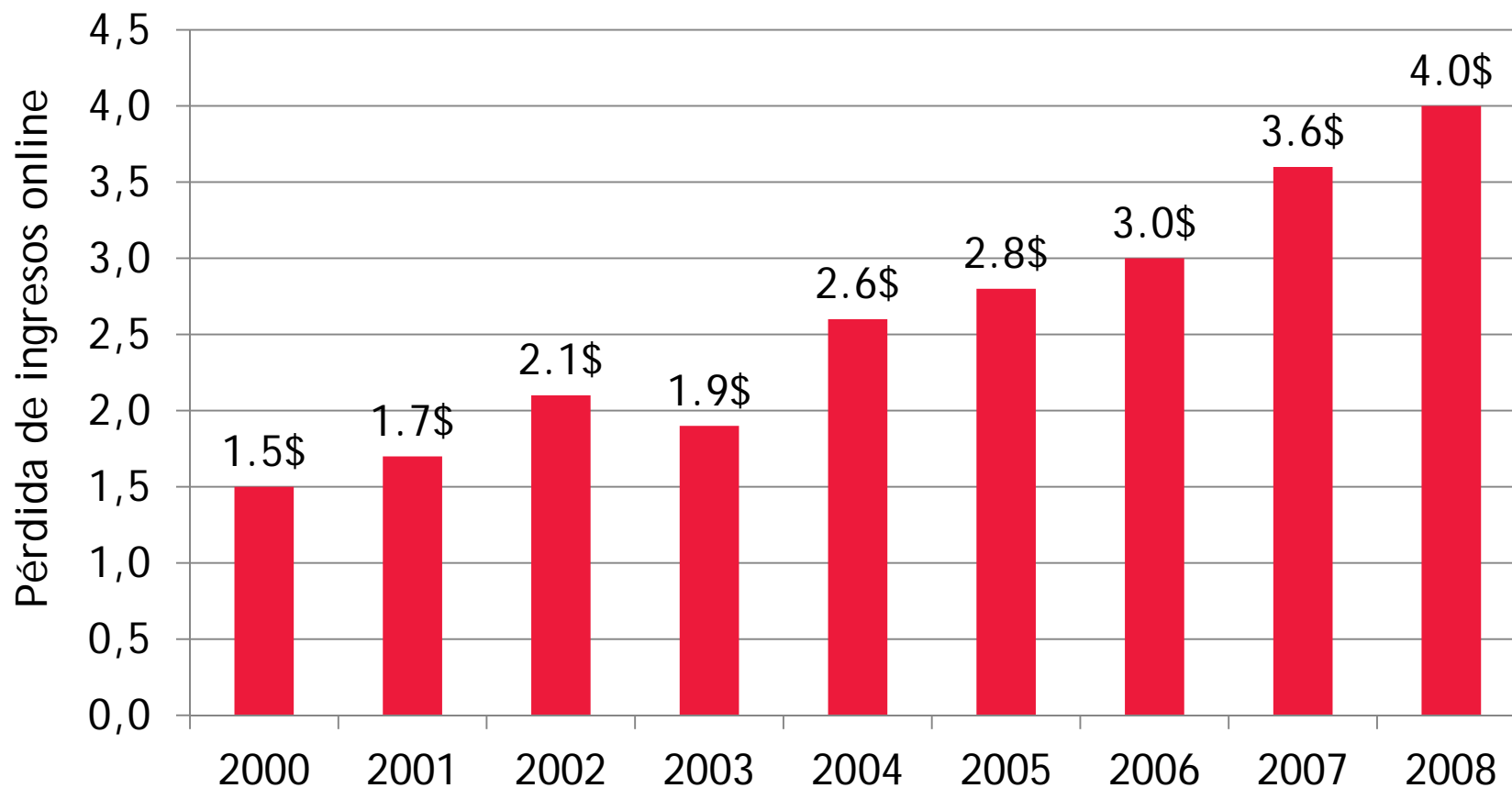
Página 6

© Todos los derechos reservados. Prohibida su reproducción no autorizada por BDO Consulting.



FRAUDES BANCARIOS

Pérdida de ingresos online



Fuente: <http://www.mcafee.com/es/resources/reports/rp-financial-fraud-int-banking.pdf>

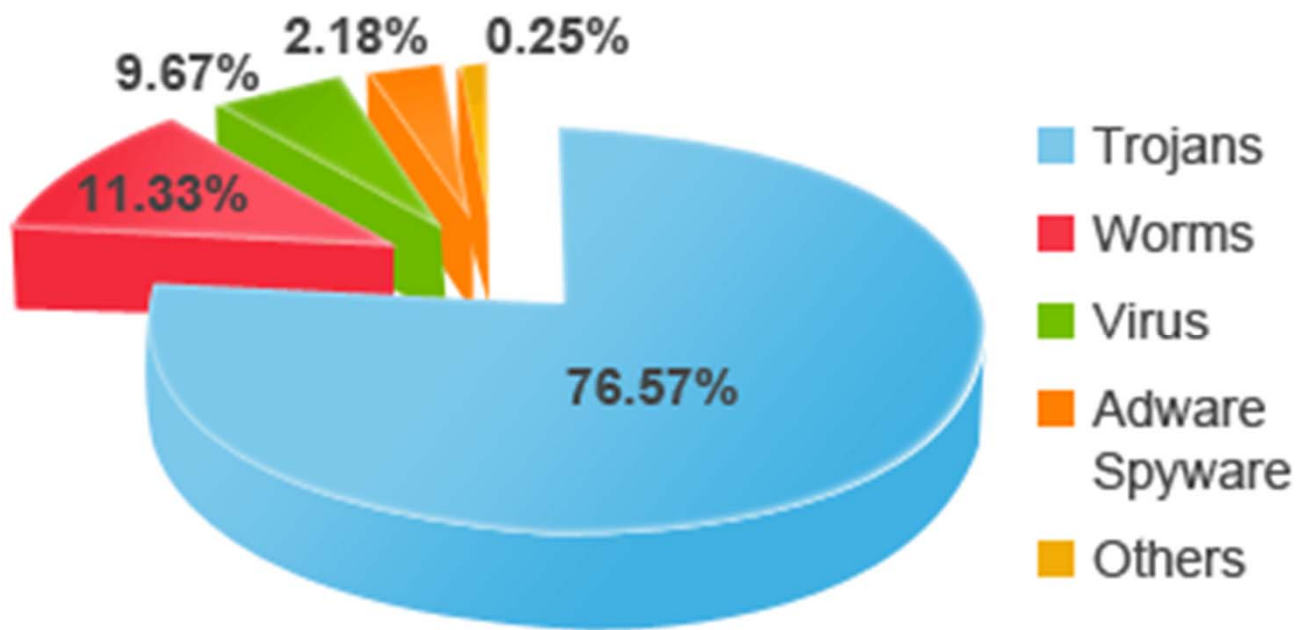
Página 7

© Todos los derechos reservados. Prohibida su reproducción no autorizada por BDO Consulting.



FRAUDES BANCARIOS

En el 2012 se crearon más de 27 millones de programas malignos (Malware) lo que se traduce a 74,000 cada día.



Fuente: <http://www.mcafee.com/es/resources/reports/rp-financial-fraud-int-banking.pdf>

EL FUTURO Y FRAUDE ELECTRÓNICO

Técnicas para la prevención de fraude electrónico en instituciones financieras





EL FUTURO Y FRAUDE ELECTRÓNICO

El panorama futuro del mundo tecnológico

En el 2013, los teléfonos celulares serán el dispositivo para acceso a la Internet más común del mundo (más que las computadoras personales PC) [[Gartner](#)]

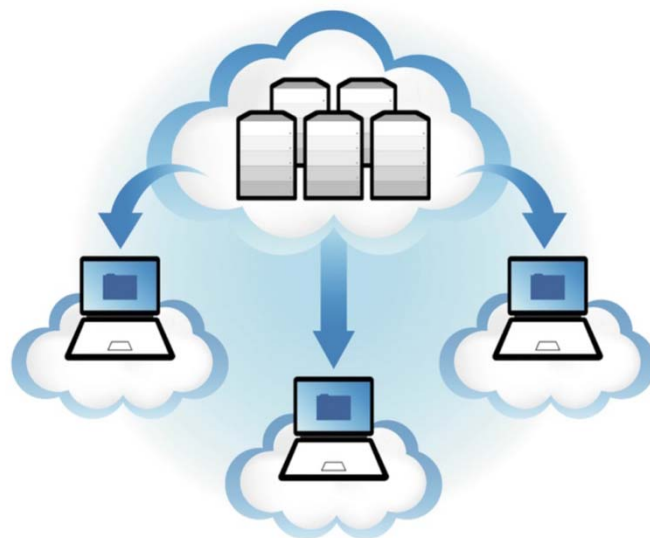
En el 2013, el número de teléfonos inteligentes a nivel mundial será más de 1.82 billones en todo el mundo. [[Gartner](#)]

El 78% del tráfico de datos móviles en todo el mundo se consume por los teléfonos inteligentes [[Royal pingdom](#)]

EL FUTURO Y FRAUDE ELECTRÓNICO

El panorama futuro del mundo tecnológico

Tercerización de servicios de tecnología y servidores en la nube son hoy día más comunes, lo trae nuevos riesgos e impacta la capacidad de realizar una investigación interna durante un fraude pues la información se almacena en servidores virtuales fuera de sitio.



EL FUTURO Y FRAUDE ELECTRÓNICO

El panorama futuro de los servicios financieros



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



ASPECTOS GENERALES DE FRAUDES ELECTRÓNICOS

Técnicas para la prevención de fraude electrónico en
instituciones financieras

DEFINICIONES

¿Qué es el fraude electrónico?

Cualquier actividad por la cual un ser humano toma acciones mediante equipos o recursos informáticos para obtener una ventaja (por ejemplo, económica) sobre otra persona o entidad por medio de falsedades, engaños u omisión de la verdad.



FRAUDES ELECTRÓNICOS MÁS COMUNES

Técnicas para la prevención de fraude electrónico en instituciones financieras

FRAUDES ELECTRÓNICOS MÁS COMUNES

Tipos de fraudes más comunes en Latinoamérica

- Phishing & Pharming
- Fraudes relacionados con banca en línea (Spyware, Keylogger, Screenlogger, Mouselogger, etc.)
- Clonación de tarjetas de crédito/débito
- Transacciones fraudulentas con Cajeros Automáticos



ÁRBOL PARA ANALIZAR ATAQUES

Técnicas para la prevención de fraude electrónico en instituciones financieras



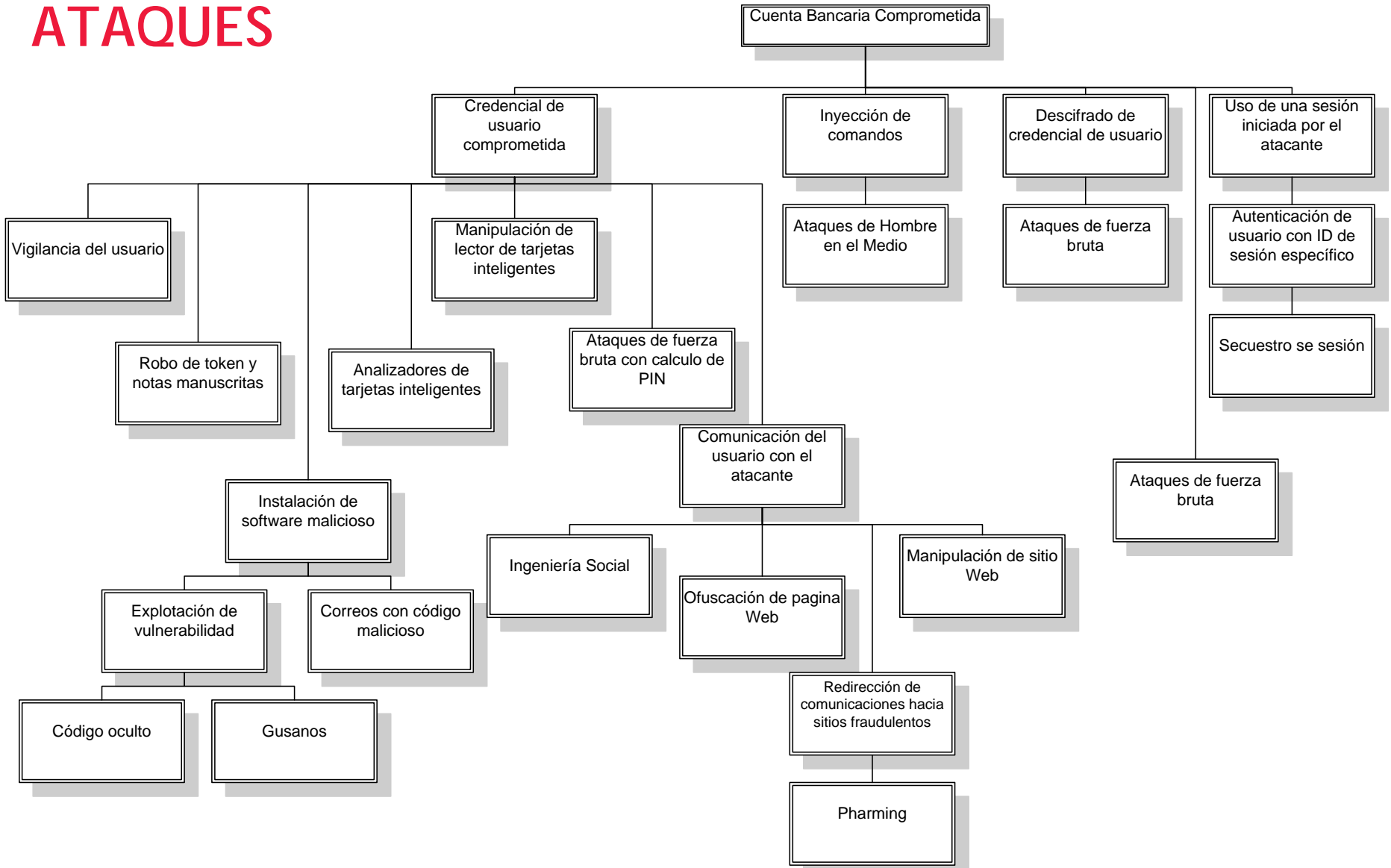


ÁRBOL PARA ANALIZAR ATAQUES

Desarrollar un “árbol de ataques”

- 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.

ATAQUES



¿QUÉ SE PUEDE HACER PARA PREVENIR UN FRAUDE ELECTRÓNICO?

Técnicas para la prevención de fraude electrónico en instituciones financieras

¿QUÉ SE PUEDE HACER PARA PREVENIR UN FRAUDE ELECTRÓNICO?

¿Qué es la PREVENCIÓN del fraude electrónico?

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.



PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL CLIENTE Y COMERCIO

Técnicas para la prevención de fraude electrónico en
instituciones financieras

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL CLIENTE

Aspectos clave para la prevención



El usuario y cliente debe también tomar acción proactiva para prevenir el fraude tomando nota de simples prácticas como por ejemplo:

- REPORTE LA OCURRENCIA O SOSPECHA DE UN FRAUDE.
- Abra una cuenta aparte para realizar transferencias electrónicas donde pueda hacer retiros o recibir pagos (Planilla por ejemplo).
- Verifique siempre que el certificado de autenticidad pertenece al banco con que está haciendo la transacción.
- Evite contraseñas repetidas o muy simples. Cambiar regularmente.
- Borre mensajes de correos de personas no conocidas.
- Bloquee ventanas emergentes (pop-up) y no descargue archivos de sitios desconocidos.

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL CLIENTE

Aspectos clave para la prevención *(Continuación)*



- Notificar al banco sobre viajes y por cuánto tiempo.
- Conozca los números de tarjeta, saldos y números telefónicos del banco y guárdelos en un lugar seguro.
- Nunca proporcionar información a nadie a menos que usted haya iniciado la comunicación.
- Denunciar inmediatamente las tarjetas extraviadas.
- Triturar documentos con información confidencial antes de tirarlos a la basura.
- Instalar y mantener actualizados su software antivirus y antispyware en sus equipos.

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL COMERCIO

Aspectos clave para la prevención



Un comercio es tan susceptible al fraude como un usuario tradicional, por lo cual debe tomar acción para prevenir el fraude:

- REPORTAR LA OCURRENCIA O SOSPECHA DE UN FRAUDE.
- Realizar auditorias recurrentes sobre sus sistemas e información financiera.
- Segregar las funciones y dividir las responsabilidades delicadas (de carácter financiero) entre varios ejecutivos claves.
- Destruir los cheques anulados o información financiera vieja.
- Cambie las contraseñas y usuario si ocurre algún evento sospechoso, o si la persona que la utiliza cambia o sale de la empresa.

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL BANCO

Técnicas para la prevención de fraude electrónico en
instituciones financieras

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL BANCO

Servicios clave del banco para la prevención



El banco debe asegurarse de ofrecer a sus clientes servicios importantes que les permitan estar alertas a posibles fraudes, como por ejemplo:

- Emitir/enviar alertas sobre transacciones por correo electrónico o mensajes de texto.
- Mensajes frecuentes para educar sobre seguridad de TI.

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL BANCO

Tecnologías clave para prevención de fraude



- Métodos de autenticación de “Multi-Factor” .
- Soluciones de Anti-Phishing y Anti-Pharming.
- IDS (Intrusion Detection System)
 - Detectar escaneo maliciosos o no autorizados y alertar a la administración o gerencia.
 - Crear bitácoras detalladas para habilitar un análisis y forense y asistir en las posibles acciones legales.
 - Detectar explotación de vulnerabilidades (Network IDS) o archivos o bitácoras que se están borrando (Host IDS) y alertar a la gerencia.

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL BANCO

Tecnologías clave para la prevención



- Análisis en tiempo real de transacciones
 - Auditoría Continua
 - Monitoreo Continuo
 - Aseguramiento Continuo

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL BANCO

Implementar buenas prácticas de control interno



- Reforzar el proceso de selección y reclutamiento.
- Implementar el uso de herramientas y sistemas para la identificación de actividades sospechosas o no autorizadas.
- Realizar charlas o entrenamientos de concientización al personal sobre el buen uso de los recursos tecnológicos.
- Establecer políticas claras sobre el manejo de incidentes y las sanciones por incumplimiento de las políticas de seguridad.
- Entrenar y certificar a personal de TI para poder prevenir e investigar incidentes de fraude.

PREVENCIÓN DE FRAUDE ELECTRÓNICO DESDE LA PERSPECTIVA DEL BANCO

Implementar buenas prácticas de control interno (Continuación)



- Establecer una cultura corporativa de control.
- Establecer una políticas para la denuncia confidencial de posibles fraudes.
- Identificar los riesgos de manera oportuna y establecer los planes para administrarlos.
- Monitorear y probar la eficiencia de los controles.

ANÁLISIS DE RIESGOS DE VULNERABILIDADES ASOCIADAS A FRAUDE ELECTRÓNICO

Técnicas para la prevención de fraude electrónico en
instituciones financieras



ANÁLISIS DE RIESGOS DE VULNERABILIDADES ASOCIADAS A FRAUDE ELECTRÓNICO

El análisis de riesgo de un sistema debe estar basado en su vulnerabilidad al fraude, abuso interno o externo, mal uso o administración y/o control interno.

Debe considerar por lo menos:

- Factores de riesgo (como por ejemplo, propósito del sistema, documentación existente, frecuencia de las auditorías, etc.)
- Categorizar cada factor de riesgo (alto, medio o bajo) para asignar un valor (3, 2 ó 1).
- Asignar un peso o valor de importancia para cada factor identificado, por ejemplo muy importante, importante, etc.



ANÁLISIS DE RIESGOS DE VULNERABILIDADES ASOCIADAS A FRAUDE ELECTRÓNICO

- El análisis de riesgo permite identificar que sistemas son de mayor riesgo, es decir alta probabilidad a propiciar un fraude.
- Conlleva a determinar donde se deben enfocar los esfuerzos e inversiones para mantener la seguridad y prevenir fraudes.
- Indica la frecuencia de la revisiones que se deben realizar.

PREPARACIÓN DE INFORMES Y MATRICES

Tabla de Evaluación de Fraudes Electrónicos - Riesgos y Controles																
Sistema				Personal con acceso		Historial de eventos		Riesgos/ Fraudes	Controles					Recomendaciones		
Nombre	Nivel de Riesgo			Valor	Usuario	Perfil	Cantidad		Descripción	Detalle/Objetivo	Tipo de control		Efectividad del control			
	Alto	Medio	Bajo								Automático	Manual	Alta		Media	Baja

CONCLUSIONES

Técnicas para la prevención de fraude electrónico en instituciones financieras



CONCLUSIONES

Técnicas para la prevención de fraude electrónico en instituciones financieras

- El mundo de tecnología y servicios financieros de hoy, es un mundo diferente lleno de nuevos riesgos y fraudes.
- La mejor herramienta para la prevención es la colaboración entre el cliente y el banco.
- Toda empresa debe mantener y propiciar un ambiente de control interno adecuado para ayudar a prevenir el fraude.
- Un análisis de riesgos es necesario para saber que sistemas son más susceptibles al fraude.
- Se requiere de una metodología y pasos definidos (árbol de ataque) para aplicar técnicas y herramientas de prevención y detección de fraude de manera correcta.

CONCLUSIONES

Consideraciones para la prevención de fraude electrónico



GRACIAS

TÉCNICAS PARA LA PREVENCIÓN DE FRAUDE ELECTRÓNICO EN INSTITUCIONES FINANCIERAS

XVII CONGRESO LATINOAMERICANO DE AUDITORÍA INTERNA Y EVALUACIÓN DE
RIESGOS

Julio R. Jolly Moore, CFE, CRISC, CRMA, CGEIT, Internal Audit Quality Assessment
Socio BDO Consulting de BDO Panamá - jjolly@bdo.com.pa

&

Oswaldo Lau C., CISA, CRISC, Internal Audit Quality Assessment
Director BDO Consulting de BDO Panamá - olau@bdo.com.pa