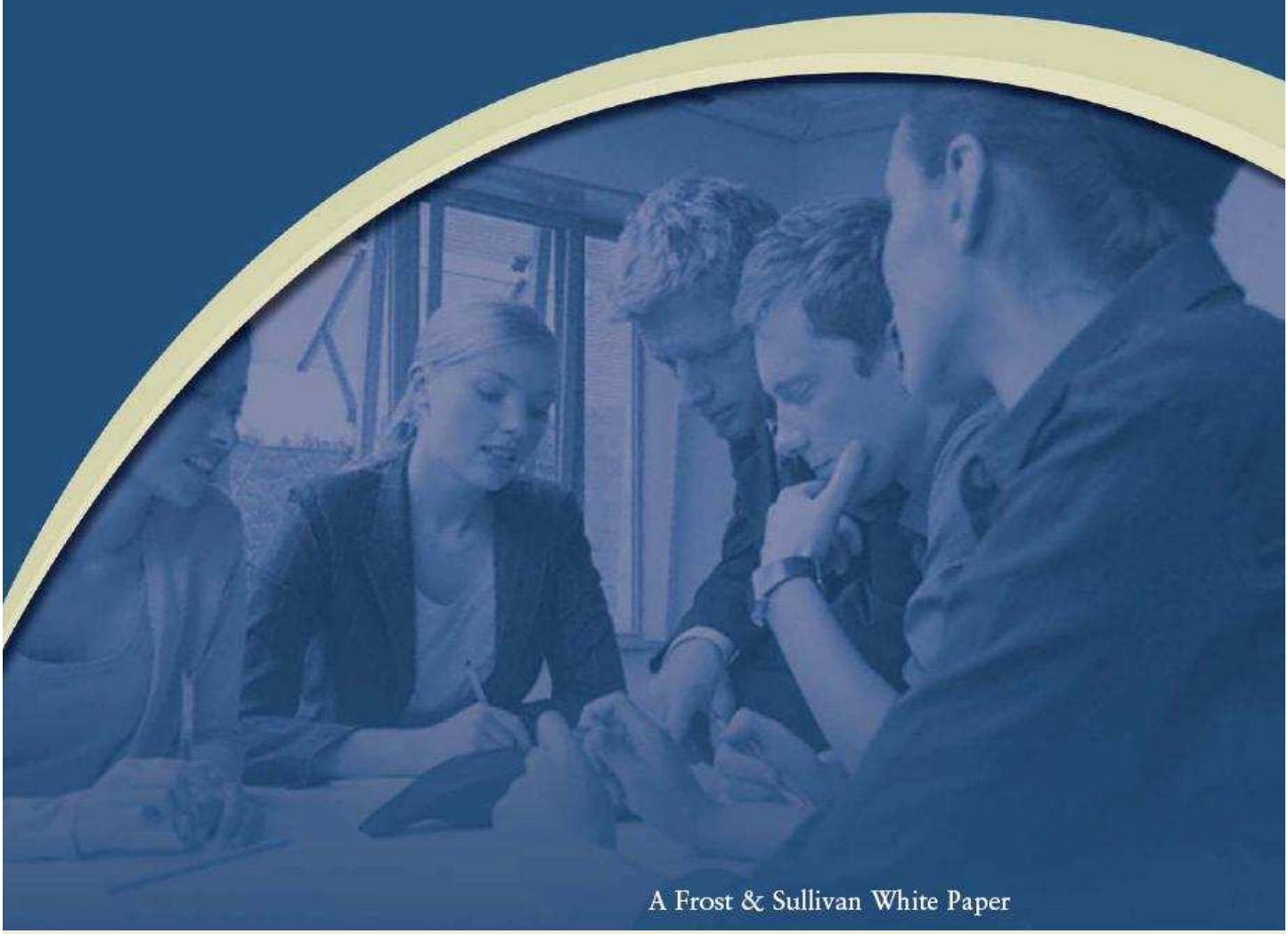
FROST & SULLIVAN

# Retos Clave Contra el Fraude Electrónico en las Instituciones Bancarias y Financieras de Latinoamérica



A Frost & Sullivan White Paper

EASYSOLUTIONS

www.frost.com

*"We Accelerate Growth"*

**TABLA DE CONTENIDO**


Panorama Actual de los Mercados de Seguridad Electrónica Anti-Fraude en Latinoamérica. 03

Creciente Uso de Internet y Vulnerabilidades 04

Bajo conocimiento de Amenazas Impulsa el Fraude Electrónico 05

Phishing: La Creciente Amenaza. 06

Cómo los Usuarios Sobrellevan el Fraude. 07

Crecimiento Explosivo del Fraude en Línea. 08

Fraude: Una Responsabilidad de los Bancos 09

Cómo Minimizar las Amenazas 10

ACERCA DE EASY SOLUTIONS 11

ACERCA DE FROST & SULLIVAN 12

# Panorama Actual del Mercado

*Desde el inicio del siglo 21, los proveedores de Seguridad de Red y de Servicios Gerenciados de Seguridad (MSS por sus siglas en inglés) han estado operando proactivamente en Latinoamérica. La región aún se encuentra en una etapa de adopción en desarrollo y ha estado experimentado fuertes tasas de crecimiento durante los últimos 5 años, con tasas compuestas de crecimiento superiores al* ***20%***

A pesar de la fuerte recesión económica global en 2008 y 2009, los mercados de seguridad de TI crecieron considerablemente en 2009. Los mercados de Seguridad en la Red crecieron **19%** y los MSS un **25%**. Este crecimiento es significativamente mayor que el de mercados más establecidos como el de Estados Unidos y algunos países de Europa Occidental.

En 2009, uno de los factores más importantes que impulsó a los mercados de Seguridad de TI en Latinoamérica fue el crecimiento exponencial tanto en la cantidad como en la complejidad de los ataques virtuales. Desafortunadamente, la región Latinoamericana actualmente sostiene una de las comunidades más grandes y activas de hackers en el mundo. Dentro de las amenazas virtuales más comunes se encuentran Virus, Troyanos, Malware y Phishing.

Adicionalmente, el creciente interés de las compañías por enfocarse en los aspectos fundamentales del negocio y el cumplimiento de regulaciones locales, regionales e internacionales son también poderosos motivadores que permiten el crecimiento de los mercados de seguridad TI en Latinoamérica. Ejemplos de regulaciones internacionales, que han afectado significativamente la región en 2010 son el estándar de seguridad de la información para la industria de tarjetas de pago o PCI DSS, Sarbanes-Oxley y Basel II.

Por otra parte, aún existen importantes barreras de mercado que inhiben un mayor crecimiento de los mercados de Seguridad de TI en Latinoamérica. Algunas de las más importantes son:

- Falta de una medición cuantificable del Retorno de la Inversión (ROI) para soluciones de seguridad de TI.
- Falta de presupuesto para Seguridad de TI y barrera cultural.
- Inestabilidad política y económica.

*"Las empresas en Latinoamérica han aumentado su concientización sobre las amenazas virtuales y consecuentemente han realizado mayores inversiones en Seguridad de TI en los últimos años"*

Frost & Sullivan
Latinoamérica

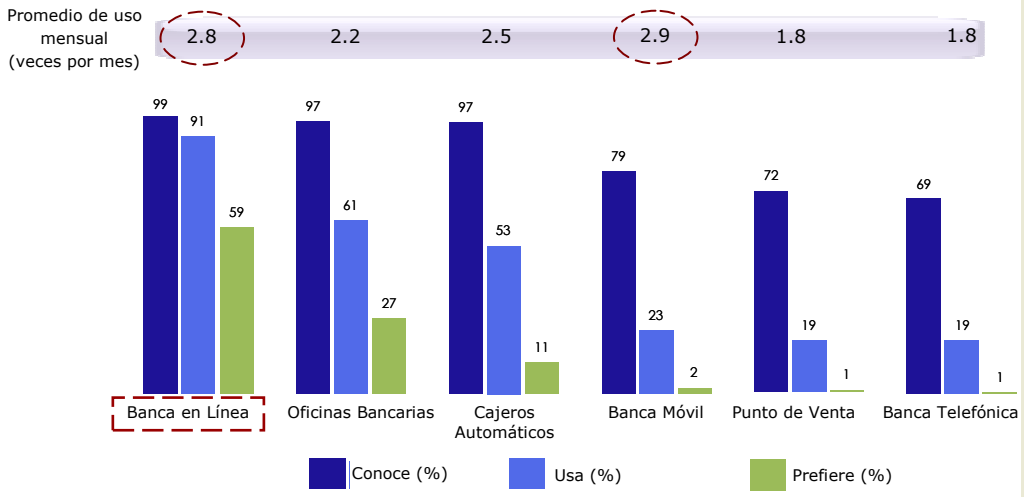
# Creciente Uso de Internet y Vulnerabilidades

*La creciente penetración de Internet en Latinoamérica es un fuerte impulsor para la adopción de la Banca en Línea.*

En 2009, aproximadamente **20%** de los hogares en la región ya contaban con disponibilidad de banda ancha de Internet. La banca por Internet es el medio de mayor preferencia para la realización de transacciones, con un impresionante 59% de usuarios en Latinoamérica que prefieren las transacciones online.

Por otra parte, los usuarios tienen un bajo nivel de preferencia por realizar sus transacciones financieras tanto en las oficinas bancarias como en cajeros automáticos, con un **27%** y **11%** respectivamente.

Conocimiento, Uso y Preferencia de Canales Transaccionales en Latinoamérica




*Fuente: marketteam; Frost & Sullivan*

Cuando se tiene en cuenta la frecuencia de uso, tanto la banca por Internet como la banca móvil son los medios más frecuentemente usados para realizar transacciones.

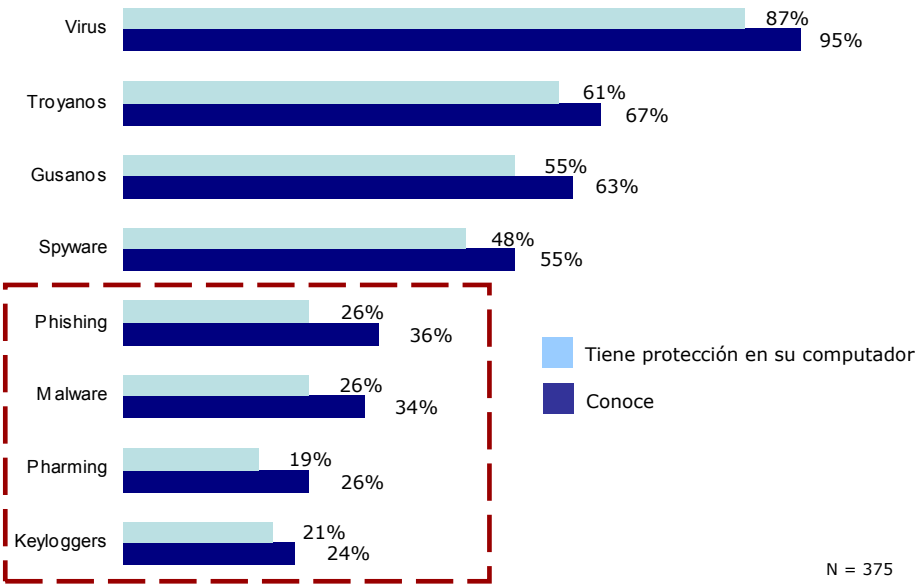
Es necesario resaltar que el **59%** de los entrevistados no considera que las amenazas virtuales hayan disminuido en el 2010 en comparación con el 2009. Esto muestra claramente la falta de confianza que tienen los usuarios de Internet en las instituciones financieras y plataformas de comercio electrónico en Latinoamérica.

# Bajo conocimiento de Amenazas Impulsa el Fraude Electrónico

*Los servicios bancarios a través de Internet y el aumento de los trabajadores remotos, son dos fuertes impulsores globales de fraude virtual. Los niveles de conocimiento de amenazas en toda la región Latinoamericana son relativamente bajos, particularmente cuando se comparan con los de países más desarrollados. Este bajo conocimiento tiene como consecuencia una pobre adopción de soluciones de prevención, aumentando a la vez el riesgo de fraude en Internet.*

Aun cuando amenazas comunes como Virus, Troyanos, Gusanos y Spyware muestran altos niveles de conocimiento, otras amenazas son apenas conocidas por unos pocos.

Conocimiento y Protección de Amenazas Electrónicas




*Fuente: marketteam; Frost & Sullivan*

Las amenazas con un nivel de conocimiento relativamente bajo y consecuentemente un bajo nivel de protección, incluyen ataques de Phishing, Malware, Pharming y Keyloggers. Todas estas amenazas tienen niveles de conocimiento inferiores al **40%** y niveles de protección por debajo del **30%**, maximizando así, las vulnerabilidades del usuario por ataques de fraude virtual.

La falta de conocimiento de serias amenazas electrónicas es uno de los principales impulsores para el creciente número de ataques tanto a plataformas de Banca por Internet como de comercio en línea

# Phishing: La Creciente Amenaza

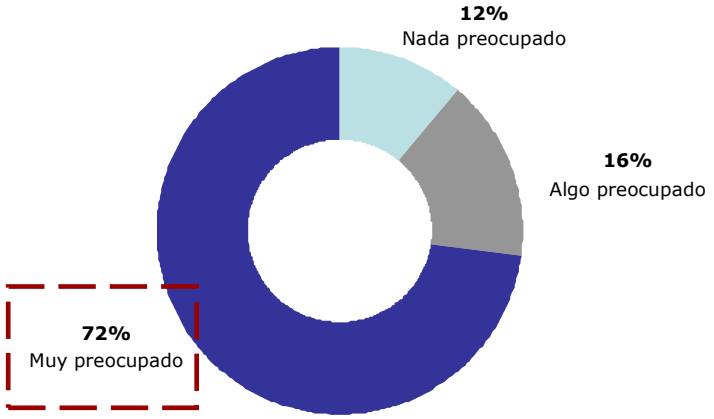
**El Problema**

El Phishing es actualmente una de las amenazas virtuales más peligrosas en Latinoamérica. Se trata de un mecanismo criminal y fraudulento el cual usa Internet para adquirir información personal crítica, como nombres de usuario, contraseñas o números de tarjetas de crédito, por medio de una interfaz o comunicación similar a la de una pagina Web auténtica.

Un error común es pensar que los ataques de Phishing ocurren solo vía e-mail. Este tipo de ataque también puede darse a través de otros medios de comunicación, siendo los más comunes, a través del teléfono y de servicios de mensajera instantánea (SMS).

Los criminales virtuales son cada vez más creativos y están utilizando redes sociales, eventos importantes, celebridades e instituciones financieras a fin de seducir a sus víctimas. Adicionalmente, las instituciones bancarias y financieras en Latinoamérica están sufriendo cada vez más ataques sofisticados y evolucionados de Phishing como lo son el Pharming y Malware.

Preocupación sobre el Phishing en Latinoamérica




N = 375

*Fuente: marketteam; Frost & Sullivan*

Cuando se explica la definición de Phishing, **72%** de los usuarios Latinoamericanos manifiestan estar muy preocupados por la privacidad de su información confidencial. Los usuarios que conocen poco acerca de los ataques de Phishing y que no poseen una solución especifica para estos, se encuentran en un riesgo constante cada vez que entren a Internet.

Tanto las soluciones de Anti-Phishing, como los servicios de autenticación han experimentado altas tasas de crecimiento en Latinoamérica en el 2010, impulsados particularmente por las verticales de Banca y Finanzas.

# Cómo los Usuarios Sobrellevan el Fraude

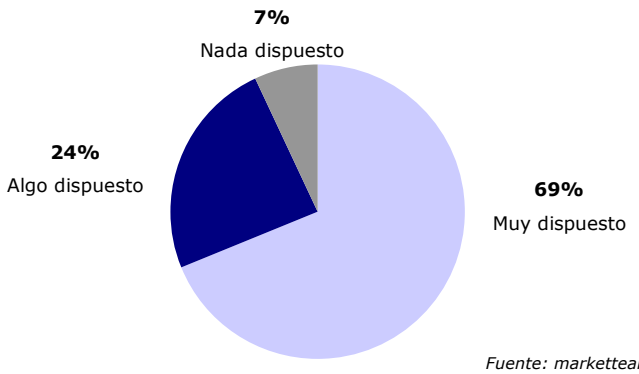
***22%** de los usuarios en Latinoamérica han dejado de usar la banca en línea, y **10%** han cambiado de banco debido a incidentes de fraude.*

Un impresionante **95%** de los usuarios de transacciones en línea creen que su banco debe implementar mayores y mejores soluciones de seguridad, a fin de minimizar los riesgos por fraude.

También es interesante anotar que el **89%** espera un monitoreo transaccional por parte de su entidad financiera a fin de detectar actividad maliciosa.

De forma similar, **69%** de los usuarios manifiestan estar dispuestos a adoptar soluciones adicionales de seguridad, y solo el **7%** las desaprueban.

Disposición a usar soluciones adicionales de seguridad en Latinoamérica




N = 375

*Fuente: marketteam; Frost & Sullivan*

**Principales acciones de los usuarios ante Fraude en Línea:**

- Sólo visita sitios Web con los que está familiarizado.
- Sólo hace compras en sitios Web de compañías reconocidas.
- Verifica certificados de seguridad de las páginas Web antes de comprar.
- Ha disminuido o detenido las compras en línea.
- Ha dejado de realizar transacciones financieras en línea.

*Fuente: marketteam; Frost & Sullivan*

En Latinoamérica, a pesar de que la identificación de certificados de seguridad de paginas Web es una acción común que pueden realizar los usuarios para protegerse del fraude, sólo un **pequeño porcentaje** de usuarios de transacciones en línea lo verifican.

Aun cuando la mayoría de usuarios están dispuestos a usar métodos adicionales de seguridad, **47%** no están dispuestos a pagar un costo adicional, ya que consideran que los bancos son los principales responsables de la seguridad en línea.

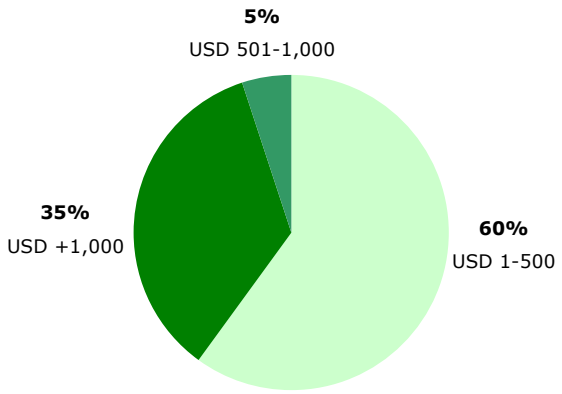
# Crecimiento Explosivo del Fraude en Línea

| Tipos de Fraude más Comunes en Latinoamérica, 2010 |
|---|
| Clonación de tarjetas crédito/debito |
| Fraudes relacionados con comercio en línea |
| Phishing |
| Transacciones Fraudulentas Involucrando Cajeros Automáticos |

*Fuente: Frost & Sullivan*

La clonación de tarjetas crédito y débito, fue el fraude más común en Latinoamérica en 2010, seguido por fraudes virtuales incluyendo compras en línea. Las compras no autorizadas por Internet se están convirtiendo en el ataque más común entre los usuarios de transacciones electrónicas. Adicionalmente, hay un alto número de transacciones fraudulentas sobre cajeros automáticos.

Valor promedio robado por incidente de fraude en Latinoamérica




*Fuente: marketteam; Frost & Sullivan*

Al analizar a profundidad los fraudes que ocurrieron en Latinoamérica en 2010, podemos concluir que **35%** de estos sumaron más de $1000 USD. El promedio por incidente de fraude en Latino America fue la importante suma de $941 USD

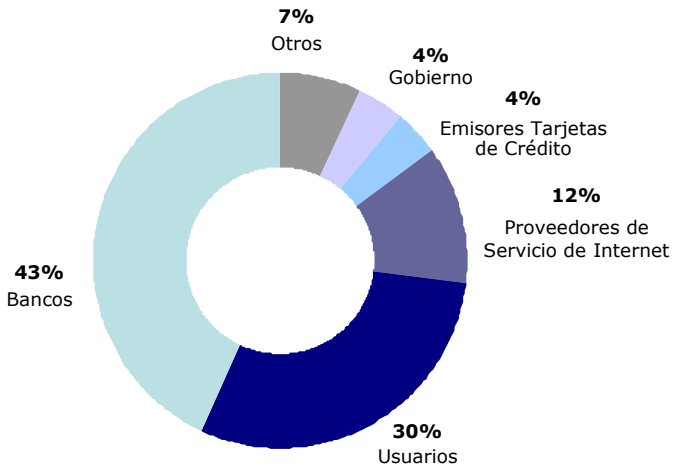
**8%** de los usuarios de transacciones en línea en Latinoamérica declaran haber sido víctimas de al menos un ataque de fraude en los últimos 12 meses. Este número es potencialmente mayor debido a que muchos ataques no son detectados por los usuarios, a causa de falta de atención a facturas bancarias y de tarjetas de crédito.

# Fraude: Una Responsabilidad de los Bancos

*Es importante resaltar que **59%** de los usuarios culpan a los proveedores de servicios en línea, tales como bancos, proveedores de servicios de Internet (ISP) y emisores de tarjetas de crédito por los fraudes ocurridos en línea.*

**43%** de los usuarios en Latinoamérica consideran a los bancos como la principal entidad responsable de asegurar las transacciones electrónicas. Dado que los usuarios otorgan su confianza a los bancos para todas sus transacciones, cada vez que sucede un fraude electrónico, son los bancos los principales responsables.

Responsables del fraude electrónico en Latinoamérica, según los usuarios




N = 375

*Fuente: marketteam; Frost & Sullivan*

**No sólo los bancos son los culpables**

**30%** de los usuarios Latinoamericanos se consideran responsables de su seguridad electrónica. Además, los proveedores de servicios de Internet, es decir, los que posibilitan la conexión a Internet, son también, considerados responsables por el **12%** de los usuarios. Las compañías proveedoras de tarjetas de crédito y el Gobierno deberían ayudar a crear un ambiente en línea más sano, de acuerdo a la opinión de usuarios Latinoamericanos.

# Cómo Minimizar las Amenazas

*Los proveedores de banca y comercio en línea deberían invertir en tecnologías efectivas y probadas, tal como servicios de autenticación Multi-Factor y servicios gestionados de Seguridad especializados en protección contra fraude.*

Los bancos deben informar a sus usuarios sobre como tener un papel más proactivo para la identificación de amenazas virtuales. Así mismo, deben empoderar a sus clientes educándolos de forma que puedan minimizar el riesgo de fraude. Para esto, los bancos y proveedores de servicios transaccionales deben invertir constantemente en soluciones de seguridad para la red y en servicios gestionados de seguridad especializados en prevención y detección de fraude.

| Tecnologías Clave para Minimizar el Fraude Virtual |
|---|
| **Análisis en tiempo real de riesgo individual de transacciones** |
| **Soluciones de autenticación Multi-factor y servicios profesionales.** |
| **Soluciones proactivas Anti-Phishing y Anti-Pharming.** |
| **Monitoreo de malware en cajeros electrónicos** |

*Fuente: Frost & Sullivan*

Para 2010, se espera que los servicios de autenticación crezcan aproximadamente **28%**, impulsados principalmente por los sectores Banca, Finanzas y Gobierno. La autenticación es considerada una de las soluciones de mayor efectividad contra crecientes amenazas tales como hurto de identidad en línea y Phishing.

Otras soluciones extremadamente poderosas para la Seguridad en TI, incluyen el análisis de transacciones de manera individual y en tiempo real, certificaciones de sitios Web y monitoreo de cajeros electrónicos 7x24.

Medidas de seguridad como Tokens, contraseñas vía SMS y autenticación de imágenes de seguridad, también son usadas por las instituciones financieras. Desafortunadamente **más de la mitad** de los usuarios de transacciones electrónicas en Latinoamérica no confían en estos métodos de seguridad. La solución más efectiva incluye la combinación de diferentes soluciones de autenticación, lo que constituye un **enfoque de autenticación multi-factor verdaderamente fuerte.**

*"Las principales instituciones financieras en Latinoamérica están aliándose con proveedores de seguridad innovadores a fin de minimizar la vulnerabilidad de sus propios clientes."*

Frost & Sullivan Latinoamérica

# Acerca de Easy Solutions

Easy Solutions es el único proveedor de seguridad enfocado exclusivamente en protección contra fraude electrónico, ofreciendo soluciones multi-canal para combatir Phishing y Pharming, Autenticación Multi-Factor y Calificación de Transacciones basada en riesgo.

La Estrategia de Protección Total Contra Fraude de Easy Solutions, es la más avanzada en prevención contra el fraude y un diferenciador único en la industria. Easy Solutions ofrece una visión holística para el manejo del fraude a través de diferentes canales transaccionales y en cualquier etapa de desarrollo de un incidente.


• Detect Monitoring Service (DMS): monitoreo en tiempo real 7x24 para rápidamente identificar, derribar y reparar ataques de Phishing. El enfoque proactivo de DMS detiene ataques de Phishing incluso antes de ser lanzados.

• Detect Safe Browsing: Protección Anti-Pharming y Anti-Phishing a nivel del usuario final para evitar el redireccionamiento hacia sitios Web fraudulentos.

• Detect ID: Autenticación Multi-factor/Multi-canal combinado con detección de Malware y aseguramiento de políticas de usuario final.

• Detect TA: Protección Multi-canal contra fraude que provee calificación en tiempo real a nivel transaccional basado en el perfil de hábitos del cliente.

• Detect ID Web Authenticator: Solución de autenticación fuerte que controla el acceso a aplicaciones críticas.

El equipo de Easy Solutions trabaja de la mano con empresas del sector financiero y líderes de la industria en otras disciplinas de seguridad, soportando un amplio rango de plataformas heterogéneas.

Easy Solutions es miembro del Anti-phishing Working Group (APWG) y de la Asociación de Banqueros Americanos (ABA - American Banker Associations). Para mayor información, por favor contáctenos: info@easysol.net.

EASYSOLUTIONS

**EASY SOLUTIONS**

Oficina Principal:

1401 Sawgrass Corporate Parkway, Sunrise, FL 33323 Teléfono: +1-866-524-4782

Latinoamérica:

Calle 93A No. 14 – 17 Of. 506 Bogotá, Colombia Tel. +57 1- 236 2455

www.easysol.net

# Acerca de Frost & Sullivan

Frost & Sullivan, es un aliado para el crecimiento estratégico, permitiendo a clientes acelerar su crecimiento y lograr mejores posiciones estratégicas en su clase, innovación y liderazgo. El servicio de alianza para el crecimiento de la compañía, proporciona al CEO y a su equipo de crecimiento, la investigación disciplinada y modelos de mejores prácticas para impulsar la generación, evaluación y aplicación de estrategias de crecimiento de gran alcance. Frost & Sullivan goza de más de 45 años de experiencia de asociación con las 1000 compañías globales, negocios emergentes y la comunidad de inversores desde más de 35 oficinas en seis continentes. Para unirse a nuestra alianza para el crecimiento estratégico, por favor visite www.frost.com