

## Unisys Security Insights: Colombia

Un Punto de Vista del Consumidor - 2015



**Cuál es el sentir de los consumidores colombianos en relación a:**

- Seguridad personal de datos, clasificada por industria
- Vulnerabilidad de diversos canales de transacciones financieras

## Table of Contents

Resumen Ejecutivo	3
Perspectiva de Unisys	4
Descubrimientos Detallados: (1) Probabilidad de Violación de Datos	5
Diferencias Demográficas Claves por Industria	6
Descubrimientos Detallados: (2) Vulnerabilidad a Ciberataques	7
Diferencias Demográficas Claves	7
Perspectiva de Unisys en Relación a la Seguridad	8
Metodología de Encuesta	9
Acerca de Lieberman Research Group	10
Acerca de Unisys	11

## Resumen Ejecutivo

Unisys juega un papel predominante en los esfuerzos por combatir el riesgo mediante productos y servicios tecnológicos que proporciona al gobierno y a las industrias más importantes de Colombia. El compromiso de Unisys con la seguridad pública y financiera es el motivo de que esta encuesta monitoree el progreso en estas áreas.

Unisys Security Insights es una fotografía instantánea del sentido de seguridad de la nación, y proporciona una medida estadística de las preocupaciones del cliente para permitir a las organizaciones realizar decisiones más fundamentadas. La investigación se llevó a cabo por una compañía de investigación de mercados importante, Lieberman Research Group.

Para la encuesta de 2015, se preguntó a los consumidores de Colombia sus percepciones en relación a:

- Seguridad personal de datos, clasificada por industria
- Vulnerabilidad de diversos canales de transacciones financieras

Las amenazas a la seguridad personal de datos son altas en diversos sectores de la industria en Colombia. Dependiendo del tipo de organización, la expectativa es que las violaciones de seguridad durante los próximos 12 meses varíen del 36 por ciento para líneas aéreas al 71 por ciento para proveedores de telecomunicaciones.

Los consumidores colombianos también tienen preocupaciones con la seguridad relacionada a las transacciones financieras online. La vulnerabilidad a ciberataques es mayor para cajeros electrónicos y compras online usando computadoras de escritorio o laptops, mientras que los smartphones y tablets son considerados como los menos vulnerables.

Estos insights sirven como un recordatorio para que los negocios e instituciones de Colombia revisen y desplieguen medidas de seguridad avanzadas para proteger a los consumidores de las ciber amenazas, así como de las amenazas físicas. Una perspectiva proactiva de la seguridad yace en el corazón de la capacidad de una organización de mitigar efectivamente el entorno de riesgo. El abordaje de Unisys hacia la seguridad va más allá de bits y bytes, reconociendo que las soluciones más efectivas serán aquellas formadas a través de colaboración entre intereses. Vea también [www.unisys.com/securityinsights](http://www.unisys.com/securityinsights)

Para obtener más información acerca de las ofertas de seguridad de Unisys, visite: [www.unisys.com/security](http://www.unisys.com/security)

## Perspectiva de Unisys

### **Existe una gran preocupación entre los consumidores Colombianos en relación a la seguridad de datos personales en la industria de telecomunicaciones**

Los resultados de la encuesta Unisys Security Insights 2015 indican que los consumidores de Colombia están más preocupados acerca de sus datos personales retenidos por compañías de telecomunicación, y alrededor de dos tercios esperan una violación de datos durante los próximos 12 meses (71 por ciento). Se destaca la percepción de vulnerabilidad de las compañías de telecomunicaciones, más probablemente debido a los recientes casos de alto perfil de violación de datos. Los consumidores de Colombia también están inquietos en relación a las amenazas de ciberseguridad en bancos (57 por ciento), mientras que las amenazas de violación de datos son relativamente bajas en líneas aéreas y minoristas para los próximos 12 meses.

Para la mayoría de las industrias, las preocupaciones en relación a la ciberseguridad son consistentemente bajas en la tercera edad.

Los consumidores en Colombia tienen altos niveles de preocupación con la seguridad de datos en algunos sectores de la industria, y las organizaciones harían bien en mitigar estas percepciones aplicando de forma proactiva soluciones de seguridad de TI para mejorar la confianza.

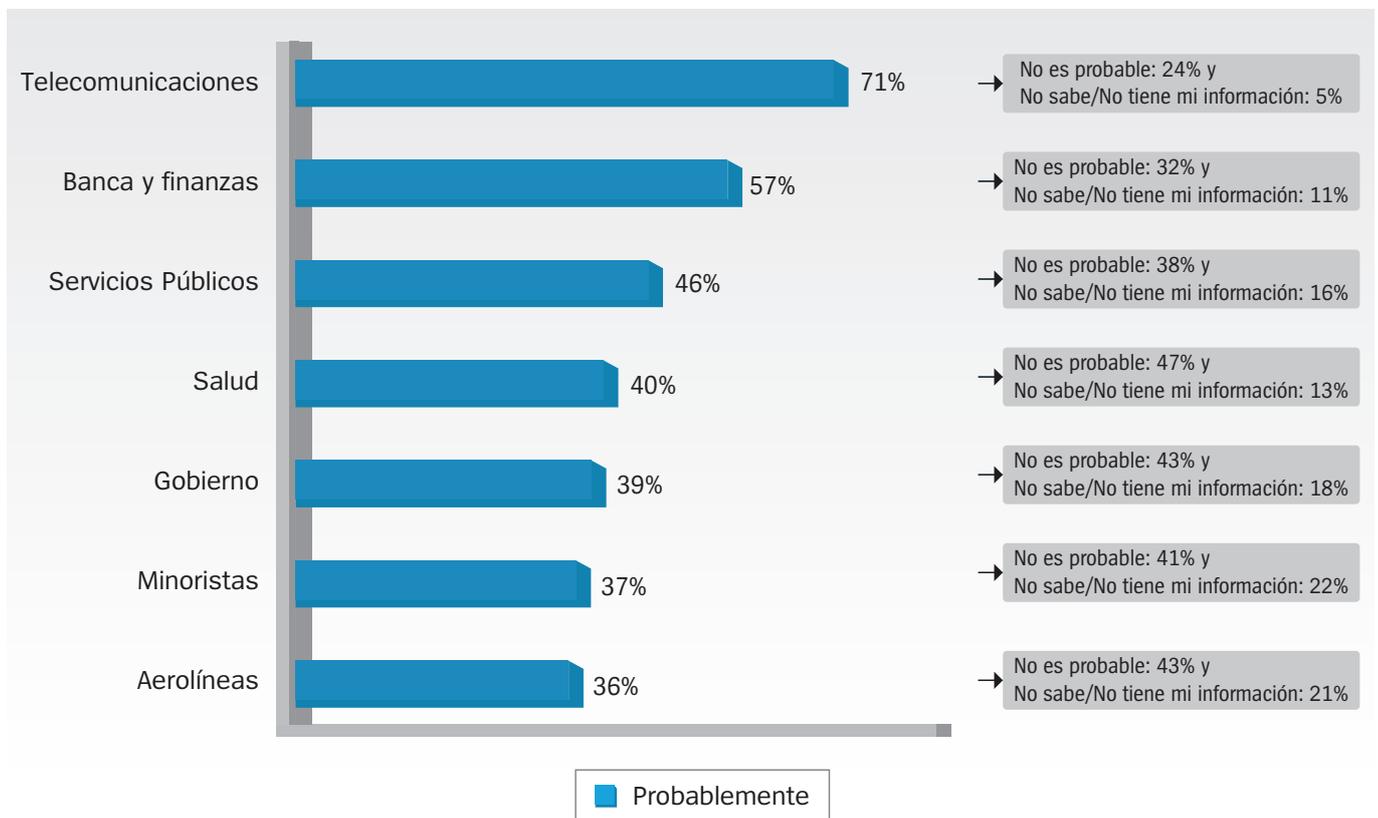
### **Preocupaciones de seguridad relacionadas a transacciones online**

Como parte del estudio Unisys Security Insights, a los consumidores también se les preguntaron sus percepciones con respecto al canal de transacción financiera más vulnerable a sufrir ciberataques. La investigación reveló que la preocupación con respecto a ciberataques en cajeros electrónicos es la mayor (34 por ciento). Los consumidores también citan las compras online con computadoras de escritorio/laptops como un canal de transacción sumamente vulnerable a los ciberataques (30 por ciento), mientras que los pagos a través de dispositivos móviles son considerados los más seguros.

Parece que los colombianos son escépticos en relación a la seguridad de sus canales de transacción. Sería prudente que los negocios y agencias públicas revisaran y aumentaran sus medidas de seguridad existentes a lo largo de varias plataformas de transacción para ganar la confianza de los consumidores.

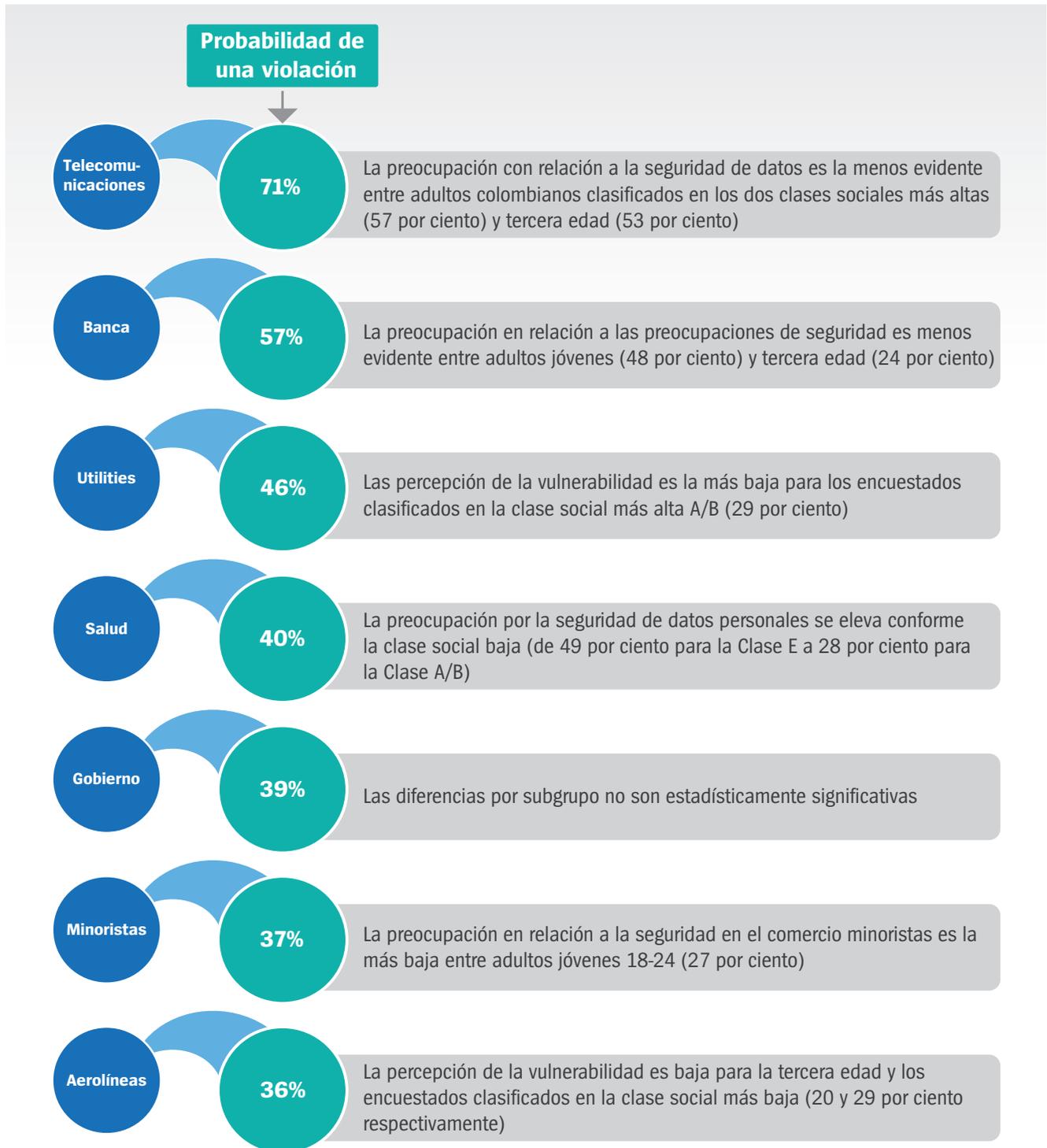
**Resultados Detallados: (1) Para cada uno de los siguientes tipos de organizaciones que recopilan su información personal, ¿qué tan probable piensa usted que su información personal sea accedida por personas no autorizadas, ya sea accidentalmente o deliberadamente dentro de los próximos 12 meses?**

La vulnerabilidad percibida de las firmas de telecomunicaciones sobresale en las mentes de los adultos colombianos, siendo que más de dos terceros (71 por ciento) describe la ocurrencia de una violación de datos de telecomunicaciones durante los próximos 12 meses como “probable”. Las preocupaciones en relación a la banca también son altas (57 por ciento), y de un tercio a la mitad de los colombianos también se preocupan por otras organizaciones.



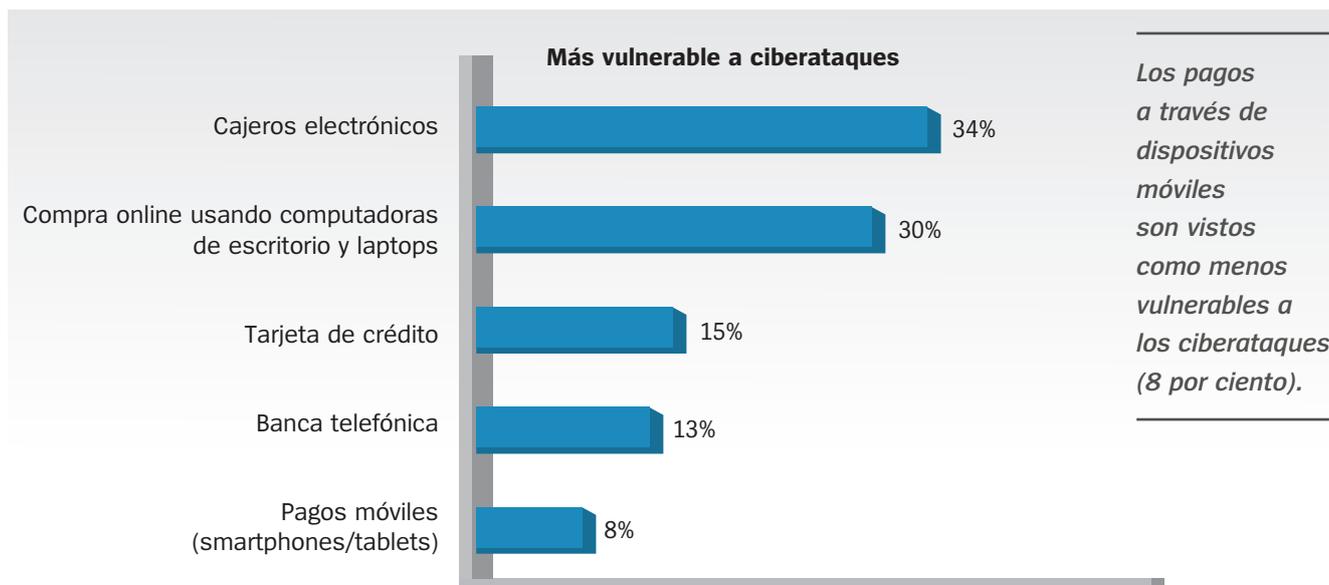
## Diferencias Demográficas – Datos por Industria

Las respuestas de los consumidores fueron analizadas con base en los sectores demográficos de género, edad y clase social. Las categorías son 18-34, 35-49, 50-64 y 65 + y las clases sociales son clasificadas como Clase A/B (más alta), Clase C, Clase D y Clase E (más baja).



## Resultados Detallados: (2) En su opinión, ¿cuál de estos canales de transacciones financieras es el MÁS vulnerable a sufrir ciberataques?

Los encuestados colombianos citan a los cajeros electrónicos (34 por ciento) y las compras online con computadoras de escritorios/laptops (30 por ciento) como los canales más vulnerables a sufrir un ciberataque.



### Diferencias Demográficas Claves

#### Cajeros electrónicos

Los adultos clasificados en la clase social más baja fueron los que consideran que los cajeros electrónicos son los más vulnerables (41 por ciento), mientras que los jóvenes adultos fueron los que mostraron menor probabilidad (25 por ciento)

#### Compras online vía computadora

La preocupación acerca de las transacciones online a través de computadoras es significativamente alta entre adultos clasificados en la Clase C y Clase A/B (46 y 39 respectivamente)

#### Tarjetas de Crédito

Los adultos de la Clase C (6 por ciento) son los que menos consideran que las transacciones de tarjetas de crédito sean vulnerables

#### Banca Telefónica

Las diferencias de subgrupo no son significativas estadísticamente

#### Pagos Móviles

Las diferencias de subgrupo no son significativas estadísticamente

## Recomendaciones de Seguridad de Unisys

La encuesta sugiere que los consumidores están realmente preocupados por sus datos personales retenidos por las organizaciones. La confianza de los consumidores fue en general baja para las compañías de telecomunicaciones, agencias gubernamentales y bancos, ya que estas organizaciones no han tenido éxito con sus medidas destinadas a recuperar la confianza. Con una siempre creciente hiper-conectividad de consumidores a través de varias plataformas digitales, los mecanismos tradicionales para proteger los datos personales delicados contra ataques avanzados resultan insuficientes. Para que las organizaciones recobren la confianza ante dicho ambiente de incertidumbre en relación a la seguridad, ellas deben seguir:

- **Un abordaje convergente de seguridad física y lógica** – Conforme las medidas de seguridad lógicas y físicas convergen, las empresas líderes en todo el mundo deben buscar maneras de resolver desafíos críticos en el punto de convergencia. Dichas medidas ayudan a integrar sensores, consolidar datos, proporcionar comando y control centralizado o disperso, utilizar la información de identidad y el soporte en tiempo real así como los análisis offline. La seguridad convergente proporciona monitoreo continuo desde la Puerta pasando por el Escritorio, hasta los Datos.
- **Biometría para obtener autenticación** – Una estrategia robusta de seguridad integra métodos de autenticación de múltiples factores, que proporcionan certeza. La autenticación puede ser proporcionada a través de varias técnicas biométricas como reconocimiento de rostro, comparación de ADN, huellas dactilares, reconocimiento de voz y estructura de venas en las manos. Como las organizaciones, los dispositivos móviles también permiten técnicas avanzadas de autenticación para prevenir intrusiones y robo de información. Esta es la oportunidad para que las organizaciones crezcan junto con las preferencias del consumidor mientras aseguran los niveles más altos de protección.
- **Aislamiento y compartimentación para protección de datos** – Proteger la información delicada del acceso no autorizado es el objetivo fundamental de cualquier estrategia de seguridad. Esto implica típicamente dos actividades claves para identificar el alcance de tarea de protección de datos, y aislar a las personas, procesos y tecnologías que interactúan con los datos delicados. El aislamiento de datos es logrado utilizando controles de acceso y cifrado para asegurar que sólo los sistemas y usuarios autorizados puedan obtener acceso a información delicada. Además, la compartimentación de grupos de usuarios también minimiza las amenazas.
- **Estrategia Integral de Seguridad** – Mantener un monitoreo de seguridad de primera y tener conocimiento y capacidades de elaboración de informes dentro de una infraestructura integral de ciberseguridad, ayudan a proteger los datos y redes de amenazas internas y externas. Una estrategia de seguridad que abarque todo, comprendería capacidades predictivas, preventivas, de detección y capacidades retrospectivas.

Para obtener información acerca de las ofertas de seguridad de Unisys, visite: [www.unisys.com/security](http://www.unisys.com/security)

## Metodología de Encuesta

La encuesta Unisys Security Insights en Colombia se basó en entrevistas personales llevadas a cabo del 14 al 21 de abril de 2015. La encuesta se llevó a cabo de la siguiente manera:

- 510 entrevistas completadas entre adultos nacionalmente representativos, con edad de 18 años o mayor.
- La encuesta se llevó a cabo en español.
- Los datos de esta encuesta fueron ponderados para asegurar la proyectabilidad de los datos hacia adultos colombianos.

Los porcentajes se basaron en la muestra completa de 510. Las diferencias del subgrupo se anotaron si eran estadísticamente significativas a un nivel del 95 por ciento de confianza.

## Acerca de Lieberman Research Group

Lieberman Research Group es una organización de investigación de mercados nacionalmente reconocida ubicada en los primeros lugares de su clase, que brinda servicio a los mercados de negocio a negocio (B2B) y de consumo (B2C). Fundada en 1966, ahora es una compañía de investigación personalizada de \$30 millones. Sus instalaciones para realizar entrevistas en Manhattan y Brooklyn tienen la capacidad de llevar a cabo entrevistas en más de 20 idiomas.

Lieberman Research es el único miembro en los EE.UU. de The Global Research Alliance – un consorcio internacional de firmas de investigación de mercados independientes en más de 20 países que proporciona acceso a instalaciones para entrevistar internacionalmente, así como conocimiento local e información que son fundamentales para obtener estudios internacionales exitosos.

A través de su investigación en los EE.UU. y en todo el mundo, Lieberman Research proporciona investigación y análisis de información a la medida de sus clientes en una gran variedad de asuntos, que incluyen satisfacción de clientes y empleados, lealtad, marketing multicultural y étnico, desarrollo de nuevos productos, políticas públicas, publicidad, relaciones públicas y muchos otros.

Lieberman Research Group es miembro del Council of American Survey Research Organizations (CASRO). Como una de las 150 compañías miembro de CASRO en todo el país, nos apegamos al Código de Estándares para Encuestas de CASRO.

Este código tiene la intención de promover los más altos estándares de conducta ética en la práctica de elaboración de encuestas, protege a nuestros clientes y ayuda a asegurar un entorno en el que el público, nuestra fuente de información en la mayoría de las encuestas, respeta y coopera con su opinión en el proceso de investigación.

Aunque los no miembros también pueden sujetarse a los mismos estándares que los miembros de CASRO, la membresía en CASRO es una indicación de que nuestra compañía toma seriamente su obligación de realizar su negocio de acuerdo con los más altos estándares éticos.



[www.casro.org](http://www.casro.org)

## Acerca de Unisys

Unisys es una compañía global de tecnología de información que resuelve los desafíos más apremiantes de TI y de negocios de las organizaciones. Cuenta con más de 20.000 empleados que sirven a clientes de todo el mundo, nuestras ofertas incluyen servicios de nube e infraestructura, servicios de aplicaciones, servicios de BPO, y tecnología de servidores de alta gama.

Entregamos soluciones a 10 de los 15 principales bancos globales, a 15 de las 25 aerolíneas globales más importantes, y a más de 200 líneas aéreas en todo el mundo. Se manejan 10 millones de incidentes de usuario en 26 idiomas diferentes todos los años, y 130 millones de transacciones de servicios a la salud son procesadas cada año por sistemas de Unisys. Nuestros procesos están en conformidad con ITIL v3 y Global ISO 20000 de principio a fin, y cuentan con los certificados 27001 y 9001. Unisys cuenta con 1.500 patentes dentro y fuera de los EE.UU.

Las ofertas de seguridad de Unisys cuentan con la confianza de clientes gubernamentales y comerciales en todo el mundo para entregar seguridad avanzada para contrarrestar amenazas avanzadas. Conforme las amenazas lógicas y físicas a la seguridad convergen, las empresas más importantes del mundo buscan un asociado que pueda aportarles nuevas maneras de resolver desafíos críticos en el punto en el que convergen. Nuestro portafolio ganador de premios y comprobado a lo largo del tiempo de servicios profesionales, productos y servicios gestionados, entrega seguridad de misión crítica a escala, ayudando a los clientes a mitigar el riesgo mientras se reduce la complejidad y el costo, y se navega a lo largo de los requisitos de conformidad regulatoria.

---

Para obtener más información visite [www.unisys.com.co](http://www.unisys.com.co)

© 2015 Unisys Corporation. Todos los derechos reservados.

Unisys y otros servicios y productos de Unisys mencionados aquí, así como sus respectivos logotipos, son marcas registradas de Unisys Corporation. Todas las demás marcas registradas referenciadas aquí son propiedad de sus respectivos dueños.