



2017 Unisys Security Index™ MEXICO

Encuesta Adicional

Apoyo de los ciudadanos de México al Internet de las Cosas, Tecnologías contra la Delincuencia y una Identificación Única

Mexicanos son selectivos
cuando se trata de compartir
datos personales a través de
Internet e identificaciones de
registro





Resumen Ejecutivo

Como parte del Unisys Security Index™, entrevistamos a los mexicanos regularmente sobre tendencias y temas actuales relacionados con la seguridad. En esta ocasión, le preguntamos a los ciudadanos de México sobre sus impresiones acerca de la distribución, recolección y análisis de datos personales a través de una variedad de tecnologías y circunstancias comunes en el mundo altamente conectado de hoy.

El fenómeno del Internet de las Cosas (Internet of Things - IoT) reúne dispositivos “inteligentes”, sensores o sistemas informáticos capaces de conectarse e intercambiar información entre sí a través de Internet. Valores más económicos y diseños más cómodos o menos intrusivos han ayudado a IoT a popularizarse, abarcando desde monitores de actividad física y relojes inteligentes hasta dispositivos médicos inteligentes y etiquetas para seguimiento de ubicación. En consecuencia, los mexicanos están cada vez más conectados.

En paralelo, empresas de distintos sectores buscan formas de explorar el creciente volumen de datos disponibles para tomar decisiones más informadas y mejorar la experiencia de los clientes, utilizando los conocimientos obtenidos del análisis de datos – incluyendo datos recogidos de IoT.

La empresa 5G America de IDC reportó durante el 2016, que el mercado de IoT en México alcanzó un valor de aproximadamente 3.3 millones de dólares, impulsado principalmente por casos de uso empresarial en áreas como el transporte y manufactura. Para 2017, IDC pronosticó un crecimiento del 26% con respecto al año anterior, llegando a 4.15 millones de dólares.¹

Empresas de telefonía tienen en la mira estrategias para abordar el Internet de las Cosas, por parte del operador americano AT&T, quienes planean desplegar una red LTE-M en México y Estados Unidos, que en conjunto ofrecerá IoT a casi 400 millones de personas.²

La operadora española, Telefónica, renovará su estrategia IoT con una serie de alianzas empresariales a través de las cuales ofrecerá servicios sobre la red, como cómputo en la nube, analítica de datos, ciberseguridad y conectividad para detonar el mercado del Internet de las Cosas en el país.³

En este contexto, el Unisys Security Index pretende equilibrar el deseo de las organizaciones empresariales para explorar los datos disponibles a través de IoT con la disponibilidad de los ciudadanos de México de compartir estos datos. Los resultados muestran que el apoyo de los mexicanos varía ampliamente dependiendo de qué datos, de las razones, por quién son recogidos, cómo se utilizarán y si los individuos pueden controlar cuándo y si se compartirán los datos.

El apoyo de los mexicanos varía ampliamente dependiendo de qué datos, de las razones, por quién son recogidos, cómo se utilizarán y si los individuos pueden controlar cuándo y si se compartirán los datos.

1 – Comunicado de prensa de IDC: Valor del mercado IoT en México crecerá 26% en 2017
<http://eleconomista.com.mx/industrias/2017/05/10/preven-que-valor-mercado-iot-mexico-crezca-26>

2 – Comunicado de Prensa de AT&T: AT&T desplegará a finales de año su red para IoT en México
http://www.milenio.com/negocios/att-red_lte-m-internet_de_las_cosas-iot-mexico-cobertura-dispositivos_moviles-milenio_0_902909922.html

3 – Comunicado de Prensa de Telefónica: Telefónica busca detonar el internet de las cosas en México en 2017
<http://expansion.mx/tecnologia/2017/02/28/telefonica-busca-detonar-el-internet-de-las-cosas-en-mexico-en-2017>



Metodología

Unisys Corporation (NYSE: UIS) lanzó el Unisys Security Index – el único análisis recurrente de cuestiones de seguridad llevado a cabo en todo el mundo – en 2007 con el fin de presentar una medida continua estadísticamente robusta de las preocupaciones alrededor de la seguridad de una nación. El índice es un puntaje en una escala de hasta 300 puntos, abarcando actitudes de los consumidores en evolución en el tiempo en ocho zonas de seguridad en cuatro categorías.

SEGURIDAD NACIONAL	SEGURIDAD NACIONAL	Seguridad nacional del país en relación con guerras o terrorismo
	DESASTRES/ EPIDEMIAS	Desastre natural grave que ocurre en el país
SEGURIDAD FINANCIERA	FRAUDE CON TARJETAS BANCARIAS	Otras personas obteniendo y usando datos de tarjetas de crédito o débito
	OBLIGACIONES FINANCIERAS	Capacidad para cumplir con obligaciones financieras esenciales
SEGURIDAD EN INTERNET	VIRUS HACKEO	Seguridad informática y en Internet en relación con virus, mensajes no solicitados o hacking
	TRANSACCIONES EN LÍNEA	Seguridad en compras u operaciones bancarias en línea
SEGURIDAD PERSONAL	ROBO DE IDENTIDADES	Acceso no autorizado o uso indebido de información personal
	SEGURIDAD PERSONAL	Seguridad personal en general en los próximos seis meses

El Unisys Security Index 2017 se basa en encuestas en línea realizadas entre 6 y 18 de abril de 2017 con muestras nacionalmente representativas de al menos 1,000 adultos en cada uno de los siguientes países: Argentina, Australia, Bélgica, Brasil, Colombia, Alemania, Malasia, México, Países Bajos, Nueva Zelanda, Filipinas, Reino Unido y Estados Unidos. En todos los países, las muestras son ponderadas en términos de características demográficas nacionales, como sexo, edad y región. El margen de error (con un nivel de confianza del 95%) es de +3.1% a nivel nacional y de 0.9% a nivel mundial.

El Unisys Security Index fue llevado a cabo por la empresa de investigación Reputation Leaders, que entrevistó a 1,005 adultos en México en abril de 2017. En 2017, el Índice de Seguridad para México fue de 173, sobre un total de 300 puntos, por encima de los 143 registrados en la última encuesta en 2014 y el mayor nivel de preocupación desde la primera edición del estudio en México en el año 2007. Para obtener más detalles, visite <http://www.unisys.com/unisys-security-index/mexico>.



Mexicanos son selectivos cuando se trata de apoyar IoT

Hoy, muchos objetos, aparatos y sistemas informáticos pueden conectarse e intercambiar información entre sí a través de Internet. Esta información estará potencialmente disponible a terceros.

Los resultados del estudio revelan que, en lugar de una respuesta homogénea al concepto de IoT, los consumidores mexicanos son selectivos cuando se trata de las instancias de IoT con las cuales se sienten cómodos, haciendo hincapié en una relación compleja entre privacidad, seguridad y beneficios tales como comodidad. En última instancia, los consumidores quieren tener control sobre qué, dónde, cuándo y con quién comparten sus datos a través de IoT, así como el derecho a decidir si la razón para esto es suficientemente convincente.

La gran mayoría de los mexicanos (92%) apoya el uso de un botón en sus relojes inteligentes para alertar a la policía sobre su ubicación en cierto momento, pero sólo el 18% darían a la policía la capacidad para seguir datos del monitor de actividad física en cualquier momento para determinar si alguien estuvo en un cierto lugar en un cierto momento.

También se identificó un gran apoyo (87% de los encuestados) a dispositivos médicos, como marcapasos o sensores de azúcar en la sangre, capaces de transmitir inmediatamente al médico del paciente cambios significativos, y a los sensores de equipaje que se comunican con el sistema de gestión de los aeropuertos y a aplicaciones móviles que informan si se descargó el equipaje y en que estera se colocarán (86%).

Una porción mucho menor de personas apoya el uso de aplicaciones de bancos o compañías de tarjetas de crédito para relojes inteligentes con el propósito de realizar pagos (51%) o de compañías de seguros de salud para consultar datos de monitores de actividad física dirigidas a añadir valor a clientes con recompensas por un comportamiento saludable (37%).

IoT en aplicación de la ley

“Cuando se trata de datos personales, hay un equilibrio muy delicado entre privacidad, seguridad y comodidad – incluso para organizaciones generalmente de confianza para el público – como la policía.”

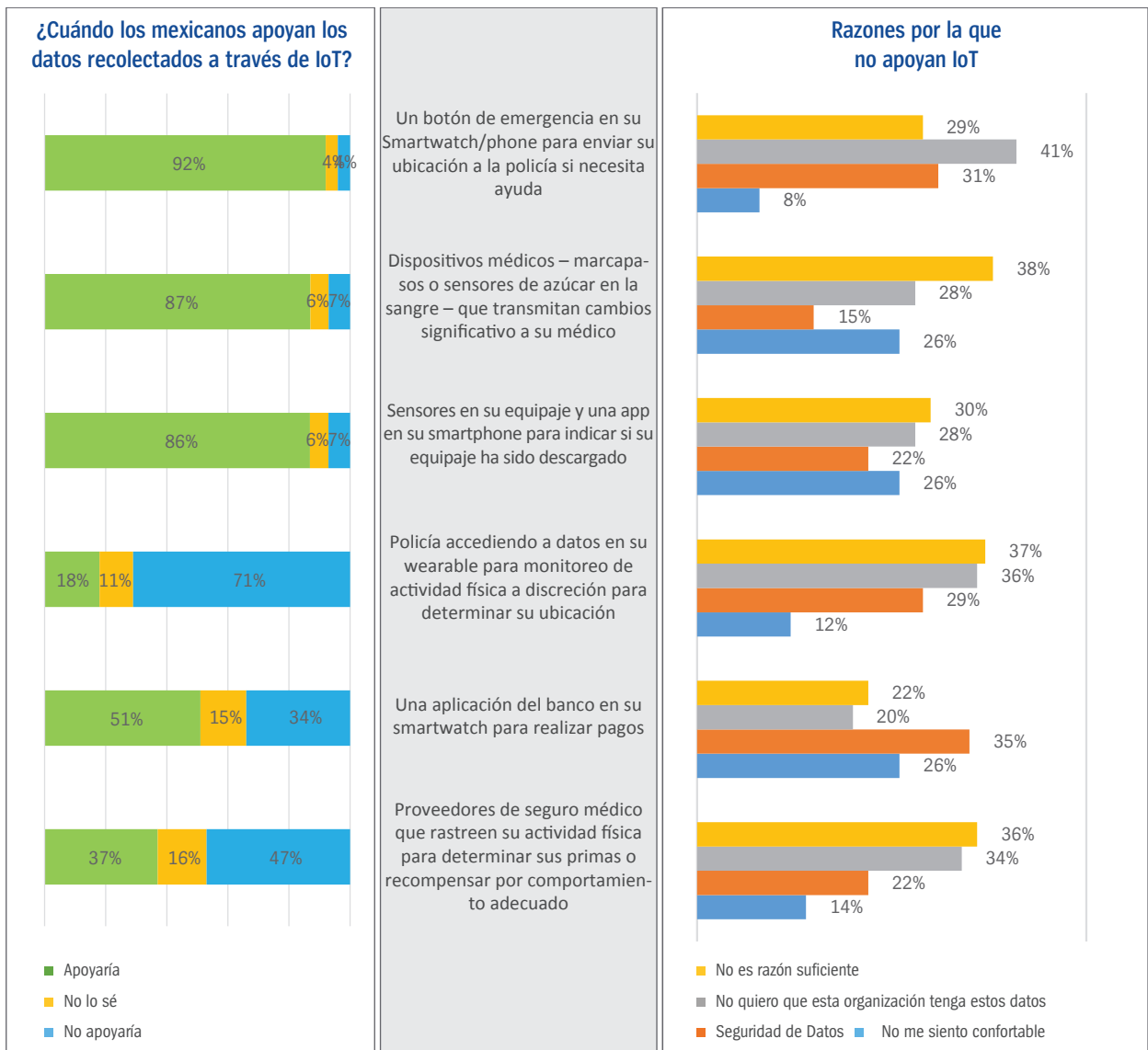
“Por ejemplo, las personas se sienten bien en usar su smartwatch para alertar a la policía acerca de su ubicación cuando necesiten ayuda, pero no quieren dar a la policía libre acceso a sus datos en cualquier momento – desean controlar cuando comparten sus datos.”

**– Leonardo Carissimi,
director de soluciones de seguridad
de Unisys en América Latina**



Obstáculos al apoyo de los consumidores a IoT

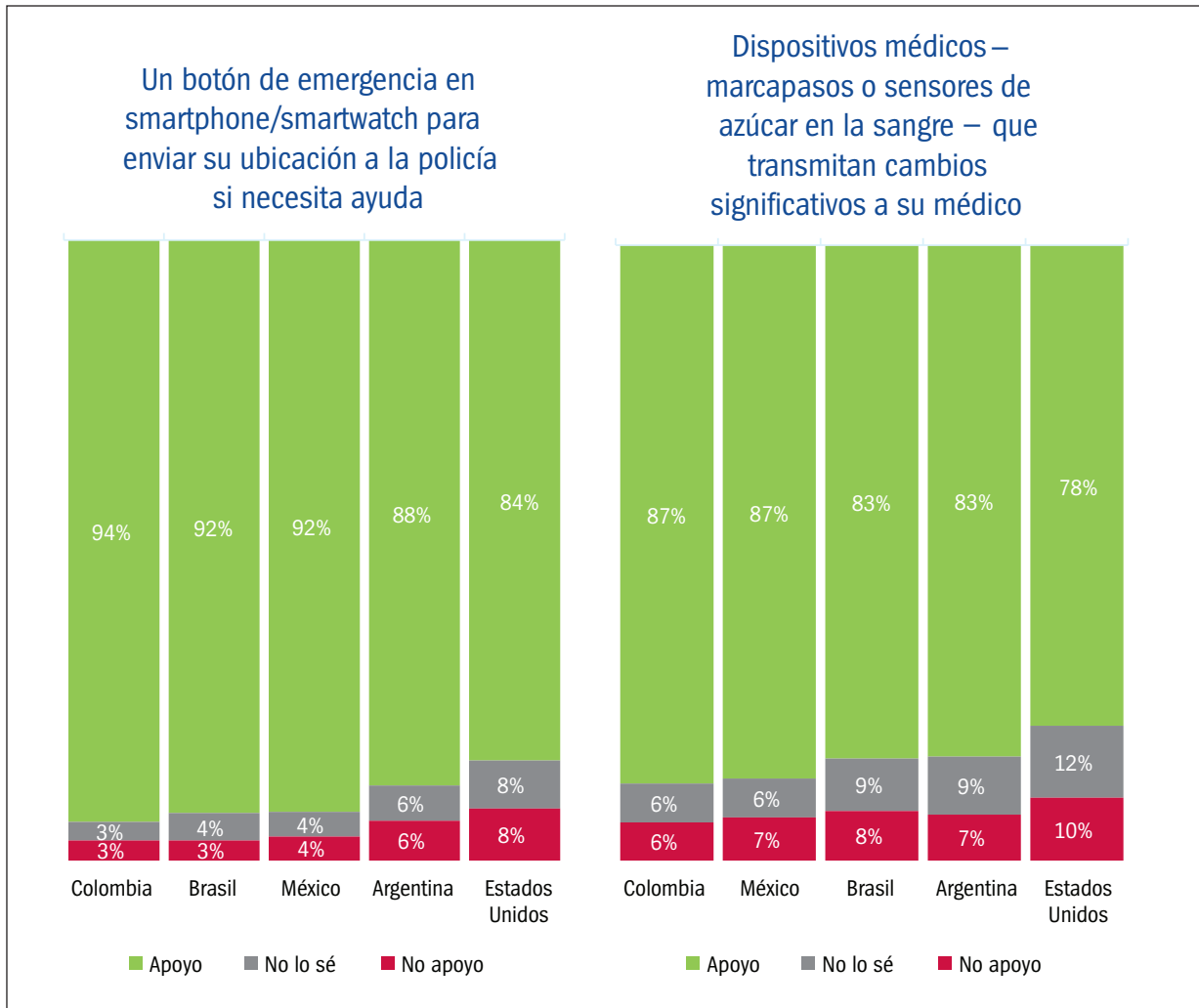
Las razones más comunes dadas por los mexicanos para no apoyar estos escenarios de IoT son la inexistencia de una razón suficientemente convincente para compartir sus datos o por qué no quieren que las organizaciones tengan esos datos sobre ellos. Sin embargo, la barrera más grande para no apoyar una aplicación de pago en relojes inteligentes es la preocupación por la seguridad de los datos recopilados.

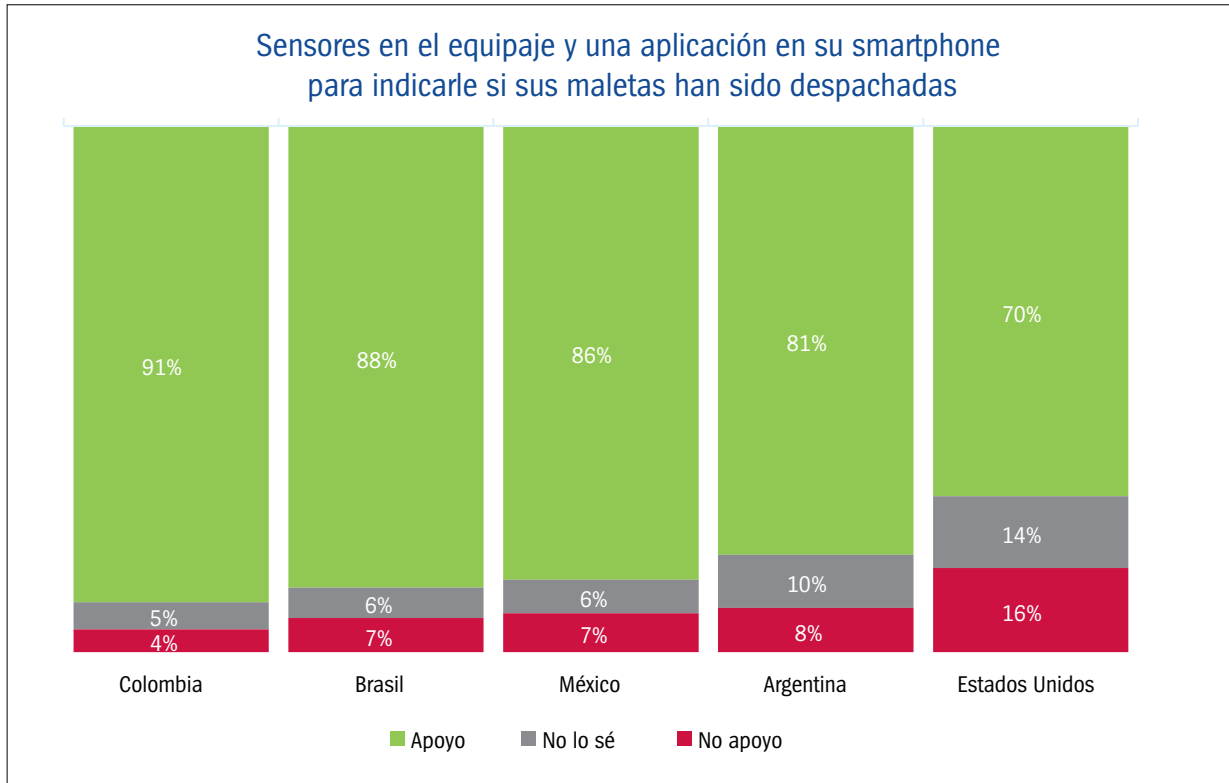




México en comparación

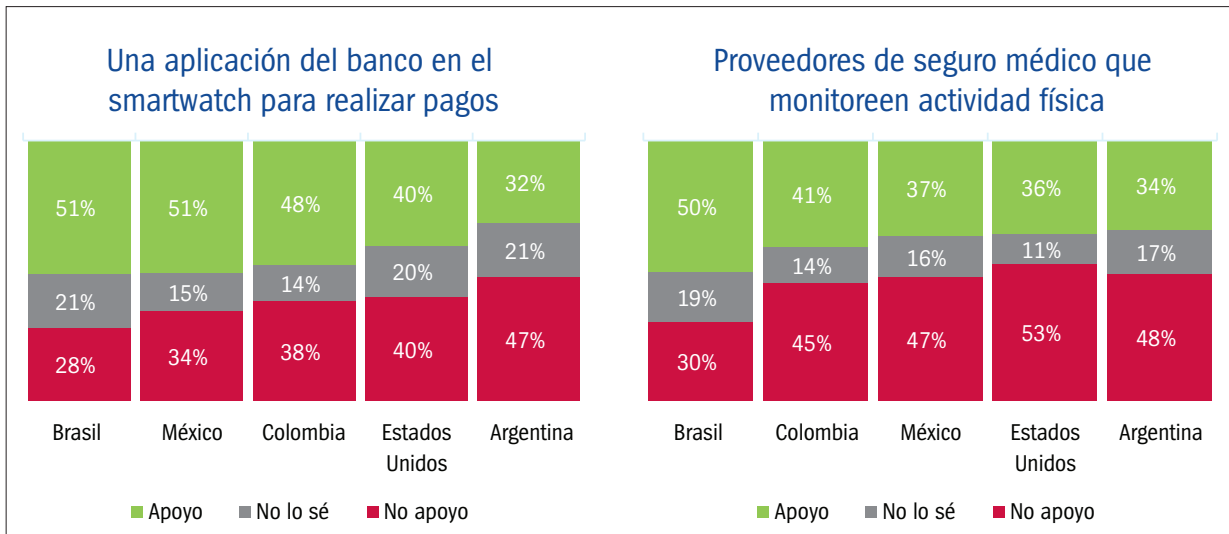
En una perspectiva regional, México se ubica en lugares intermedios con un alto apoyo a datos recolectados a través de IoT, teniendo resultados similares a Colombia y Brasil, siendo los mexicanos quienes muestren mayor apoyo, entre los países de América, a dispositivos médicos que recopilen datos de marcapasos o sensores de azúcar en la sangre, con el fin de transmitir cambios significativos a los médicos.





Variedad de visiones

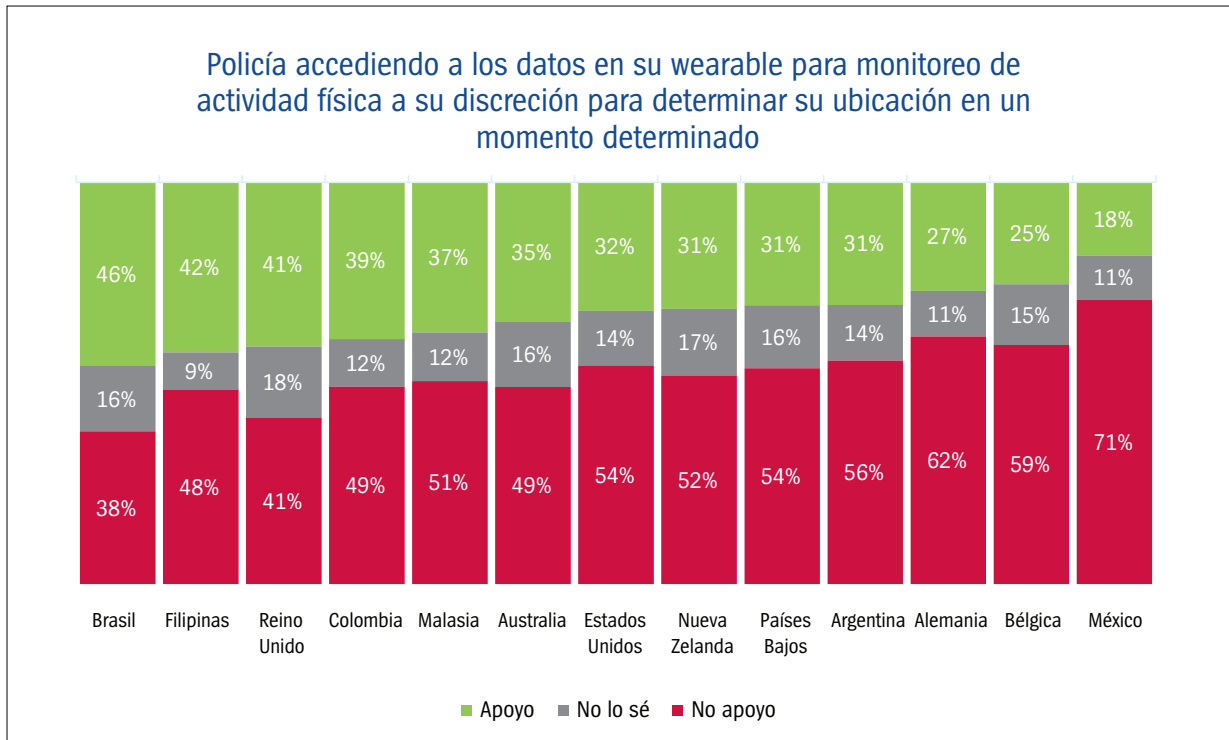
Entre los encuestados mexicanos, hay gran variedad de opiniones sobre la opción de confiar sus datos financieros para pagos digitales, a través de aplicaciones de compañías bancarias. Y un menor apoyo a que las aseguradoras médicas monitoreen y obtengan datos de actividad física para determinar primas.





Bajo apoyo al rastreo

Los mexicanos mostraron el menor apoyo entre todos los países encuestados, ante la idea de que la policía tenga acceso a sus dispositivos móviles como Smartphones o Smartwatch para monitorear la actividad física para determinar su ubicación en momentos determinados.



Resultados clave:

- Gran apoyo al uso de un botón en el Smartwatch/Smartphone para alertar a la policía acerca de su localización en caso de emergencia, pero muy poco apoyo para dar a la policía la capacidad de supervisar la ubicación del monitor de actividad física en cualquier momento.
- Gran apoyo a dispositivos médicos IoT capaces de automáticamente alertar a médicos, pero poco apoyo para que las empresas de seguro de salud sean capaces de utilizar datos del monitor de actividad física para establecer recompensas.
- La gente no desea compartir datos a través de IoT si no ve una razón convincente para hacerlo o si no quiere que las organizaciones tengan sus datos.
- Preocupación por la seguridad de datos es la principal razón para no apoyar aplicaciones de pago en relojes inteligentes.



Llamados a la Acción

Al desarrollar una estrategia de IoT o análisis de datos, Unisys recomienda a las organizaciones considerar el punto de vista de los consumidores en cinco factores clave:

- 1. Propósitos convincentes: ¿Cuáles son los beneficios para mí?** – ¿Es una razón suficientemente fuerte para que los consumidores quieran revelar un poco de su privacidad?
- 2. Confianza: ¿Quiero que esta organización tenga esta información acerca de mí?** – ¿Los consumidores estarán preocupados de que esa información se utilizará para el propósito que fue pensado originalmente?
- 3. Protección: ¿Mis datos estarán seguros?** – Use la tecnología, procesos y políticas para evitar brechas de seguridad y minimizar su impacto, en caso de suceder. Después comuníquese estas medidas para tranquilizar a los clientes acerca de las medidas adoptadas para proteger ellos y sus datos.
- 4. Control: ¿Puedo decidir cuándo y si comparto mis datos?** – Los consumidores quedan más cómodos cuando pueden elegir si comparten sus datos en un momento específico en lugar de conceder acceso sin restricciones.
- 5. ¿Sólo porque usted puede, debe hacerlo?** – Comprenda que la aceptación pública de IoT y del análisis de datos consiste en una mezcla compleja de recursos tecnológicos, actitudes humanas, normas culturales y ética.

“Las empresas están buscando nuevas e innovadoras maneras para mantenerse en contacto con sus clientes. La tecnología juega una gran parte con sus soluciones emergentes como los dispositivos wearables.

Al mismo tiempo, los clientes están cada vez más preocupados por su identidad y datos personales. Cualquier empresa que quiera explorar este nuevo canal necesita convencer a sus clientes que garantizan la privacidad y la seguridad de sus datos. Es imperativo que las organizaciones revelen abiertamente cómo van a usar los datos y asegurar que los clientes permanecerán en el control de su información en todo momento, y no se utilizará para fines distintos a los divulgados.

Las empresas que tratan esos puntos claramente van a tener mayores posibilidades de conectarse con sus clientes y obtendrán una ventaja sobre su competencia.”

– David Barrios, Líder de Sistemas para Unisys América Latina



Conclusión

La tendencia de IoT sólo acaba de comenzar. La riqueza de los datos generados por aplicaciones personales y de trabajo seguirá creciendo. Sin embargo, la recopilación y el análisis de los datos implican una relación compleja entre tecnología y factores humanos de confianza, propósito aceptable y disposición para renunciar a la privacidad. Organizaciones comerciales y del gobierno que buscan explorar IoT y el análisis de datos deben hacerlo en el contexto de estos factores humanos.

Para obtener más información sobre soluciones de seguridad de Unisys, visite: www.unisyssecurityindex.com/mexico

Acerca de Unisys Security Index

Unisys ha llevado a cabo desde 2007 el Unisys Security Index (La única instantánea recurrente de las preocupaciones de seguridad llevada a cabo a nivel mundial), con el fin de proporcionar una medida continua, estadísticamente robusta de la preocupación por la seguridad. El índice es un puntaje calculado que cubre las cambiantes actitudes de los consumidores a lo largo de múltiples áreas de seguridad en cuatro categorías: Seguridad Nacional, Seguridad Financiera, Seguridad en Internet y Seguridad Personal. Para obtener más información sobre el Unisys Security Index 2017 de Unisys, visite: www.unisyssecurityindex.com/mexico

Acerca de Unisys

Unisys es una empresa de tecnología de la información global que se especializa en proporcionar soluciones centradas en la industria integrada con seguridad de vanguardia a clientes en el gobierno, los servicios financieros y los mercados comerciales. Las ofertas de Unisys incluyen soluciones de seguridad avanzada, análisis de datos, y servicios de infraestructura cloud, servicios de aplicaciones y software de aplicaciones y servidores. Para obtener más información, visite: www.unisys.com.mx

Siga Unisys en [Twitter](#) y [LinkedIn](#).



For more information visit www.unisys.com

© 2017 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.