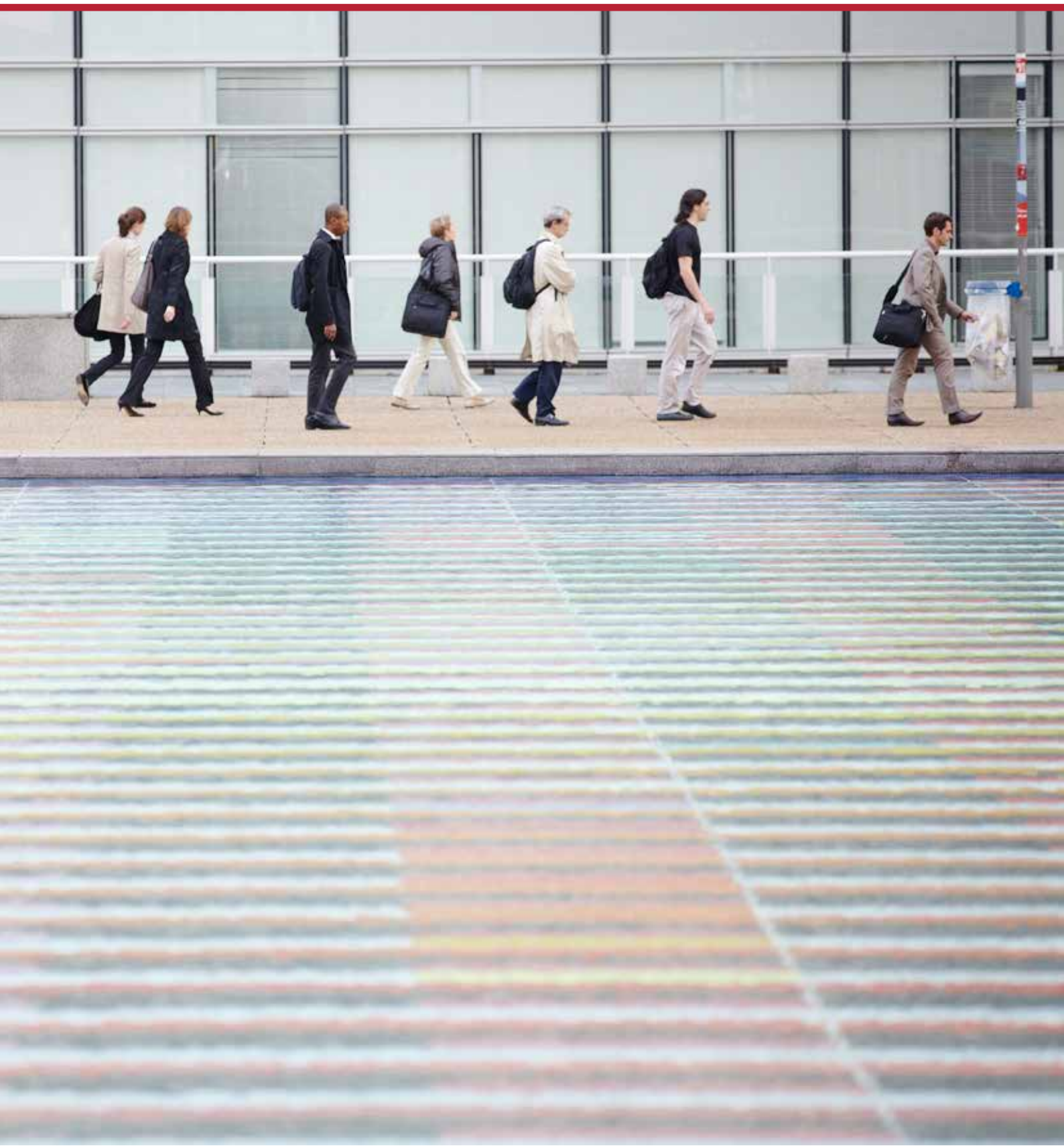
www.pwc.com/ar

Encuesta Global de Seguridad de la Información

Capítulo Argentina

pwc

Consultoría
2017

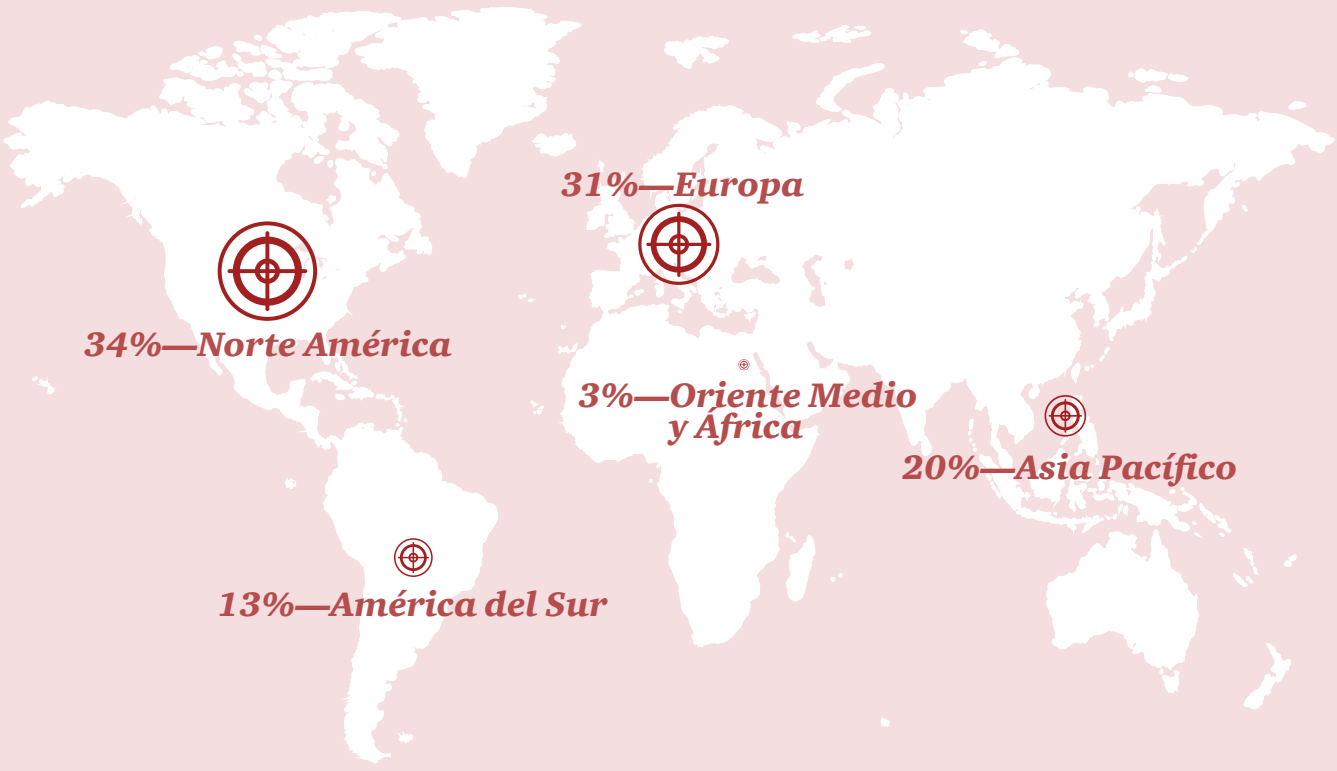


Introducción

La Encuesta Global de Seguridad de la Información 2017 de PwC es un estudio mundial realizado por PwC, CIO y CSO.

Los resultados analizados se basan en respuestas de más de 10.000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs y directores de IT y prácticas de seguridad de más de 133 países.

Entre los encuestados el 34% pertenece a América del Norte, el 31% a Europa, el 20% a Asia Pacífico, el 13% a América del Sur y el 3% a Oriente Medio y África.



Hacia una nueva mirada de la ciberseguridad

Como consecuencia de la digitalización, muchas organizaciones ya no consideran la ciberseguridad como una barrera o como un costo de IT, sino que la entienden como una solución y como una herramienta que puede facilitar el crecimiento, obtener ventajas en el mercado y construir reputación corporativa.

En la era digital un nuevo concepto de modelo de negocios está surgiendo, donde la ciberseguridad y la privacidad deben ser soluciones integrales.

A medida que más productos y servicios de todo tipo se conectan a Internet, la necesidad de abordar de forma proactiva la ciberseguridad y privacidad, ya que se han convertido en requisitos críticos del negocio. Hoy se produce y comparte más información al consumidor y al mercado en general.

Como resultado, las organizaciones con visión de futuro están yendo hacia un nuevo modelo de ciberseguridad, ágil, capaz de actuar con insumos analíticos y adaptable a la evolución de riesgos y amenazas.

El núcleo de este nuevo enfoque son soluciones como data analytics, monitoreo en tiempo real, servicios de seguridad gestionados, autenticación y software de código abierto.

Aunque no todas estas tecnologías son nuevas, la forma en que son distribuidas y gestionadas a menudo muchos son basados en la nube u ofrecidos como servicios de seguridad administrados. Algunos, como la adopción de Software de código abierto, representan un cambio radical.

Pero si hay un hilo unificador, es la nube. El poder y la interoperabilidad de las plataformas basadas en nube permite a las empresas sintetizar una gama de tecnologías sinérgicas. Las empresas pueden aprovechar la simplificación inherente de las arquitecturas para confeccionar nuevos productos y servicios seguros. Estas ventajas arquitectónicas representan una oportunidad para la integración y mejora de la Seguridad cibernética y herramientas de privacidad.

Ciberseguridad y privacidad: más allá del costo, una solución integral

Es necesario entregar los servicios de una manera segura para mantener la fidelidad y confianza.

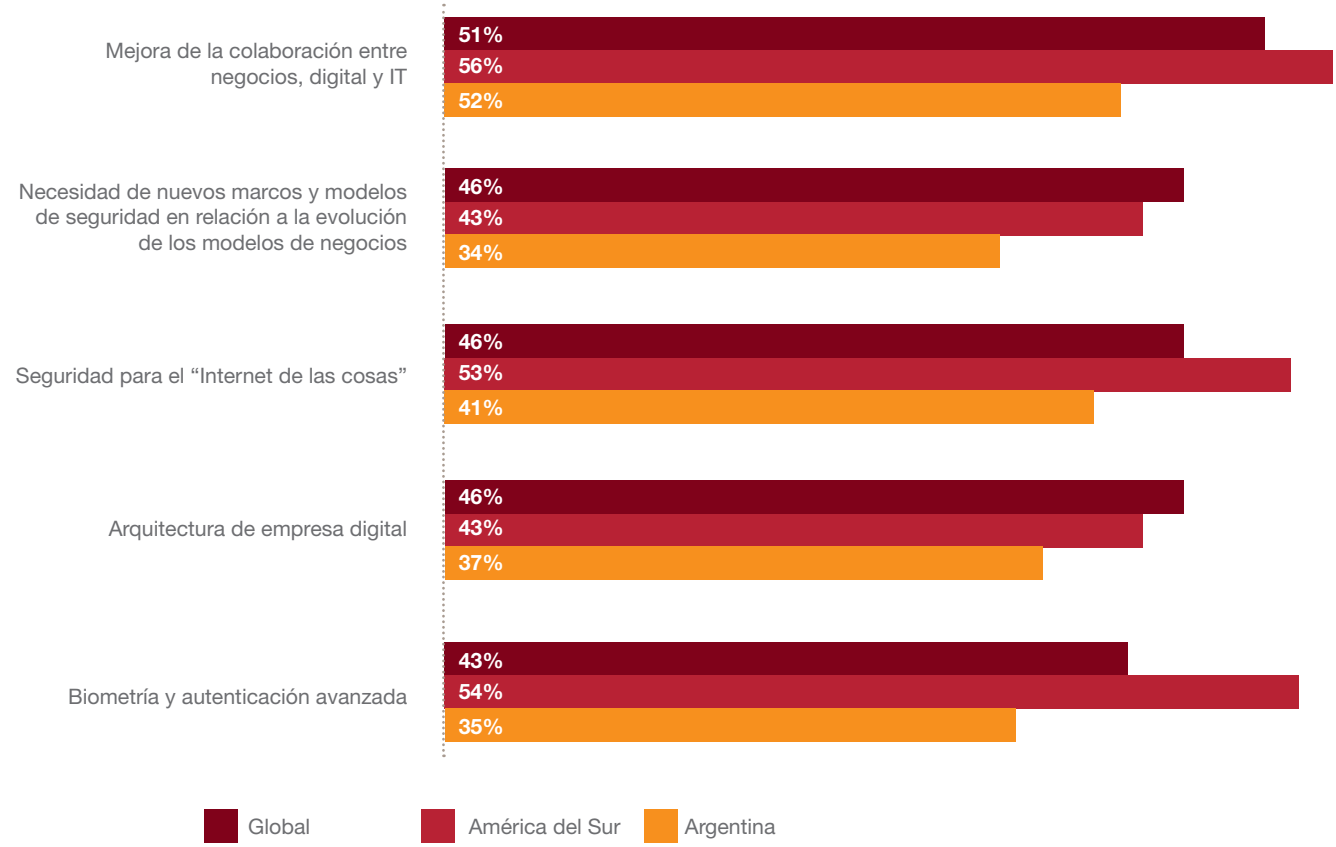
Hoy en día, la mayoría de los negocios son digitales y el software se está convirtiendo en la columna vertebral de las operaciones, productos y servicios. En este escenario la mayoría de las organizaciones, ya sean digitales o tradicionales, están explorando nuevas oportunidades para crear valor y ventajas competitivas, incorporando la ciberseguridad y privacidad con estrategias de negocios digitales.

En este sentido, las empresas ofrecen servicios digitales complementarios a la venta de un producto o servicio. Los clientes en la actualidad esperan productos seguros y que protejan los datos sensibles.

El 59% de los encuestados a nivel global manifestó, que la digitalización de sus ecosistemas empresariales ha impactado en el gasto en la ciberseguridad.

Las empresas que integren la ciberseguridad con estrategias digitales estarán mejor preparadas para actuar en este nuevo paradigma de negocios.

Las prioridades de gastos en ciberseguridad para los próximos 12 meses



Las sinergias en la nube

El almacenamiento de datos basado en la nube resulta más seguro que en las propias instalaciones de las compañías. Es por este motivo que más empresas están confiando información y cargas de trabajo más sensibles a los proveedores externos.

Con mayor frecuencia las funciones de negocios como contabilidad, finanzas, operaciones y recursos humanos son guardadas en la nube. Si bien esta es una tendencia en aumento, hay algunos países en donde persisten las barreras regulatorias que limitan el tipo de información que se comparte.

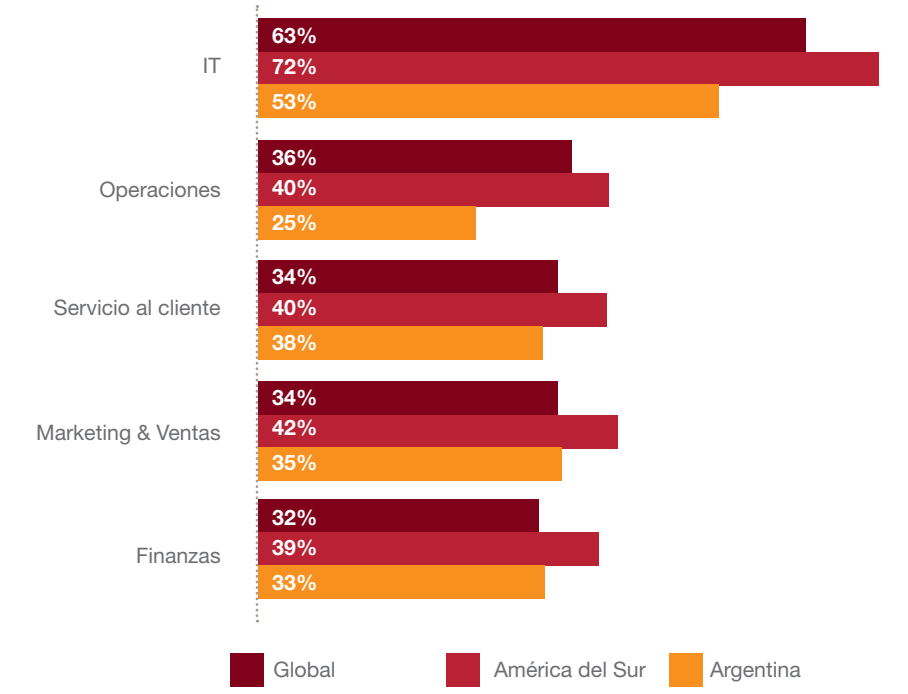
Ejecutan operaciones de IT en la nube

La ciberseguridad basada en la nube representa un enfoque dinámico para el riesgo. No solo ayuda a disuadir a los intrusos, sino que también monitorea a aquellos que intentan ingresar al sistema, ya sean empleados, socios y tercerizados.

La fusión de tecnología avanzada con la arquitectura en la nube le permite a las organizaciones comprender mejor el funcionamiento del ecosistema empresarial.

La ciberseguridad, es en esencia, una fuente de fortaleza que puede dar lugar a una verdadera diferenciación de las capacidades empresariales.

Funciones empresariales ejecutadas en la nube



Gestión de la seguridad de afuera hacia adentro

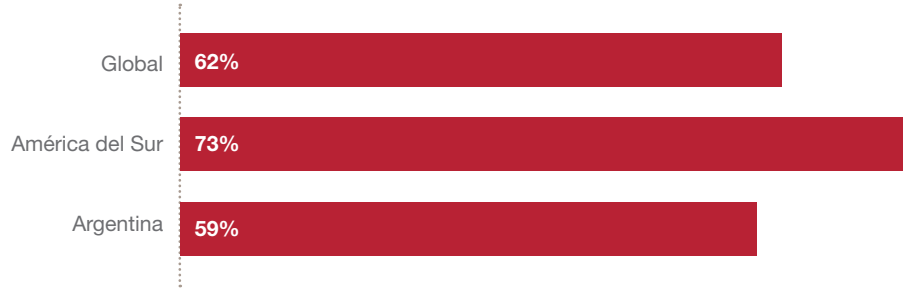
El diseño e implementación de un programa de ciberseguridad y privacidad es un reto. Una vez que el programa está implementado, los distintos componentes deben ser integrados, gestionados profesionalmente y mejorados continuamente.

Esta es una tarea complicada cuando los recursos de las empresas son limitados es por esto que han abordado este reto mediante la implementación de servicios de seguridad. De hecho, casi dos tercios de los encuestados dicen utilizar proveedores de servicios de seguridad para operar sus programas de ciberseguridad.

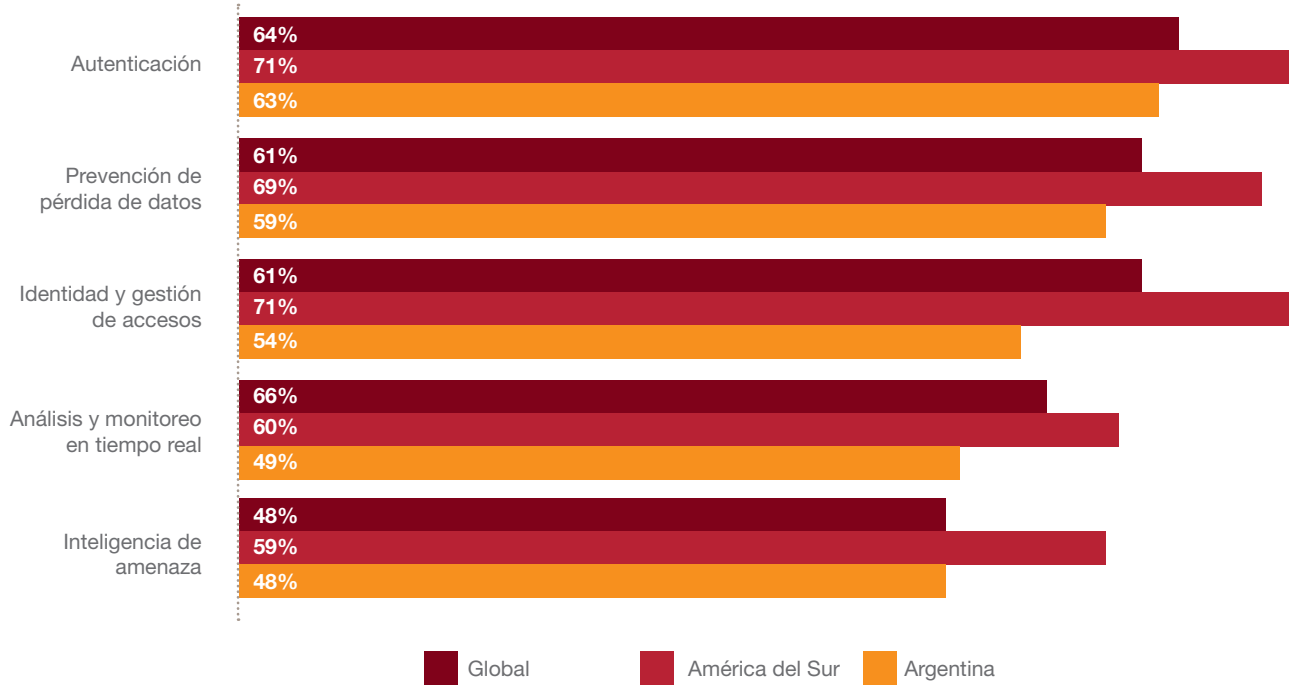
Con el avance acelerado de la tecnología resulta muy difícil capacitarse constantemente en materia de ciberseguridad. Según un informe de Cybersecurity Ventures, la falta de talento en la materia aumentará para 2019. Esta tendencia obliga a las compañías a tercerizar parcial o totalmente los programas de seguridad.

El costo es otro factor a considerar. Las empresas que no cuentan con el presupuesto para contratar el servicio de ciberseguridad, deben acudir a personal interno.

Utilizan servicios de seguridad gestionados para la ciberseguridad y privacidad



Uso de servicios de seguridad administrados



Anticipando los riesgos con el análisis e inteligencia de amenazas

Las empresas deben entender las motivaciones y tácticas de los hackers para anticiparse y detectar amenazas.

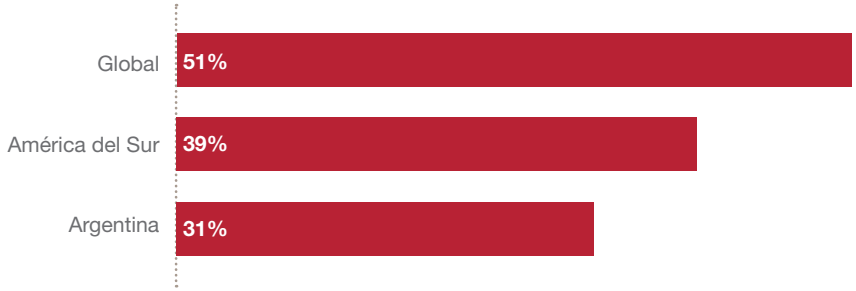
Es necesario un análisis preciso sobre las amenazas en tiempo real para obtener una conciencia contextual de los riesgos y comprender las tácticas, técnicas y procedimientos de los hackers. Cuando el análisis y la inteligencia de amenazas se sintetizan en la nube, se hace posible crear una fuente única de datos de toda la empresa que se correlaciona de manera transparente y se puede gestionar en tiempo real. Cuando se identifica una nueva amenaza, el análisis basado en la nube puede priorizar las respuestas basadas en el impacto comercial y en los activos de datos.

La capacidad de almacenamiento de la nube permite a las organizaciones monitorear grandes volúmenes de datos, así como aplicaciones altamente complejas e interconectadas, para identificar actividades sospechosas.

Este año, más de la mitad de los encuestados a nivel global manifestaron que utilizan el análisis de Big Data para modelar las amenazas de la ciberseguridad e identificar incidentes. Entre los encuestados que utilizan servicios de seguridad administrados, el 55% dice utilizar proveedores de servicios para monitoreo y análisis en tiempo real. Además de las ventajas computacionales y de almacenamiento y conocimientos técnicos, los grandes proveedores de servicios gestionados, a menudo tienen acceso a los Centros de Operaciones de Seguridad (SOC) y al Centro de fusión de inteligencia de amenazas.

Los SOC y la fusión de inteligencia de amenazas son absolutamente críticos para agregar datos, filtrar falsos positivos y obtener información valiosa.

Utilizan análisis de "Big Data" para modelar e identificar amenazas



Más allá de las contraseñas: La autenticación avanzada

El desconocimiento por parte del usuario sobre las prácticas de uso de contraseñas con cierto grado de dificultad es una de las razones por las que muchas empresas recurren a tecnologías avanzadas de autenticación para agregar una capa adicional de seguridad y mejorar la confianza entre clientes y socios comerciales. Las tecnologías de autenticación no solo facilitan la identificación y acceso seguro para los usuarios, sino que también ayudan a reforzar la seguridad general de datos.

El 46% de las organizaciones que emplean la autenticación avanzada dicen que han realizado las transacciones en línea más seguras, según los resultados de la encuesta del último año. Los encuestados también informan que las tecnologías de autenticación aumentan sus capacidades de seguridad y privacidad, mejorando la experiencia del cliente y protegiendo la reputación de la marca.

En el pasado, la autenticación avanzada era principalmente el dominio tecnológico de los sistemas gubernamentales y las grandes instituciones financieras; Actualmente, las redes sociales y los proveedores de correo electrónico introdujeron la autenticación multifactor, siendo cada vez más sectores quienes están adoptando este tipo de autenticación.

Más allá de los multifactores, algunas empresas están desarrollando e implementando tecnologías locales más avanzadas tales como un patrón que un usuario debe ingresar, una tarjeta de acceso o una información biométrica tal como huellas dactilares o exploraciones de iris.

A medida que las organizaciones implementan nuevas tecnologías de autenticación, es posible que tengan que replantearse su enfoque de la gestión de identidades para diseñar soluciones que construyan relaciones de confianza de identidad y aseguren la facilidad de uso para los clientes. También es importante asignar la autenticación al nivel de riesgo que el acceso trae al negocio.

Utilizan la biometría para la autenticación

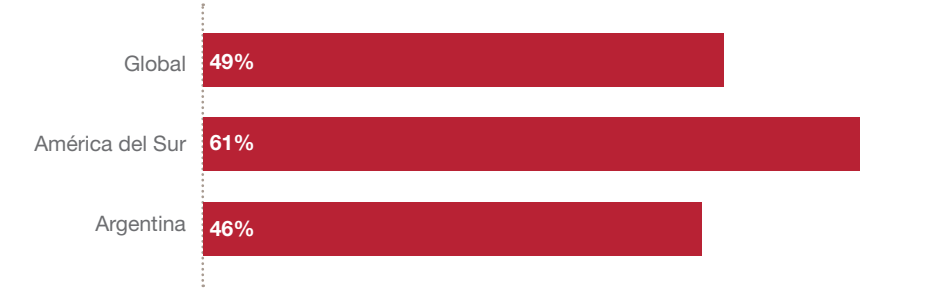
Creando posibilidades con el software de código abierto

La adopción del sofware de código abierto esta proliferando en todas las industrias y representa un gran cambio en la forma en que las organizaciones desarrollan y ejecutan soluciones locales y ofrecen servicios de IT.

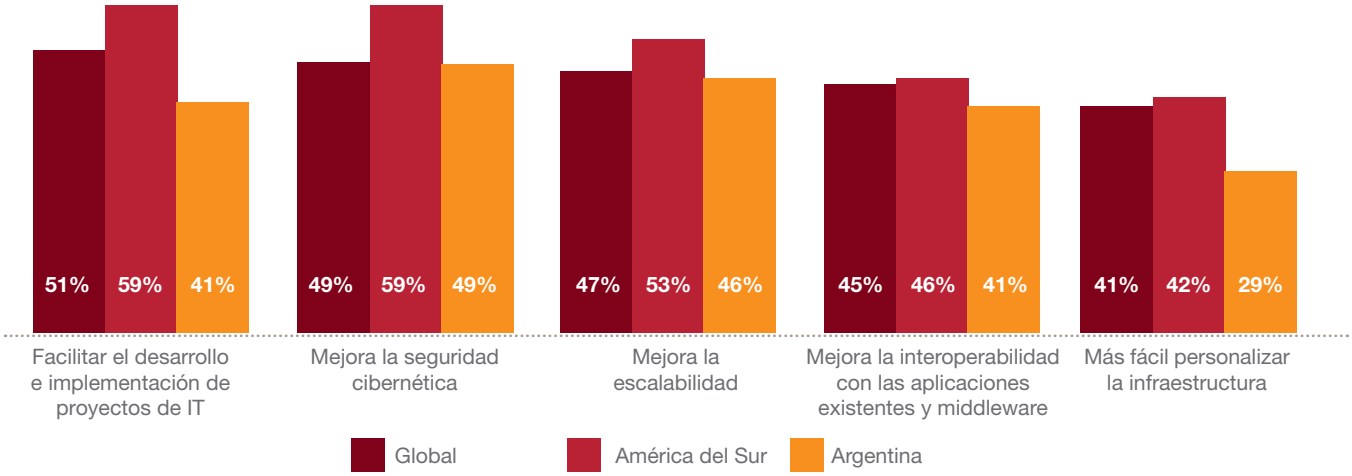
Algunas de las compañías más grandes del mundo están abrazando el movimiento del código abierto, incluyendo el titán del software Microsoft: la compañía ha hecho los componentes de SQL Server, de . NET y de PowerShell disponibles en Linux. El gobierno de los Estados Unidos ha lanzado un programa piloto que requiere que las agencias liberen al menos el 20% del nuevo código para los sitios web con fondos federales, aplicaciones y otros proyectos de software como código abierto. Por lo tanto, no es del todo sorprendente que más de la mitad (53% de los encuestados) utilizan algún tipo de software de código abierto y el 49% de ellos afirma que ha mejorado su postura de ciberseguridad.

El software de código abierto esta disponible a un bajo costo proporcionando un método económico para crear nuevas soluciones. Al combinarse con la nube, las tecnologías de código abierto pueden ayudar a mejorar la interoperabilidad de los sistemas.

Utilizan software de código abierto y afirman que ha mejorado su programa de ciberseguridad



Beneficios del software de código abierto



Aumento del riesgo global en la privacidad de datos

Mientras que los ecosistemas digitales están interconectados, las amenazas que se generan están impulsando cambios en la ciberseguridad y los avances tecnológicos están creando marcos regulatorios en todo el mundo. Este año se implementarán nuevos requisitos, uno de los más importantes es el ***Reglamento General de Protección de Datos*** de la UE (GDPR), que entrará en vigor en abril de 2018 y se centrará en la privacidad de datos para las empresas que ofrecen bienes y servicios a los ciudadanos de la Unión Europea.

Cabe destacar que el Reglamento se aplicará al procesamiento de datos de europeos por entidades establecidas en Europa, pero también por aquellas empresas situadas fuera de la Unión Europea que realicen actividades dentro de la UE y que impliquen el tratamiento de datos personales, incluso aunque no tengan presencia física en dicho territorio de la Unión.

Las empresas que no cumplan con GDPR se enfrentarán a multas de hasta el 4% de los ingresos anuales globales de la compañía.

Cómo abordan las organizaciones los desafíos regulatorios

Las regulaciones de privacidad de datos crean nuevos desafíos para las organizaciones, y generan preocupación entre los ejecutivos.

Entre los encuestados, la prioridad más citada en los próximos 12 meses es la formación y concientización en materia de políticas y procedimientos de privacidad.

Más allá de estas medidas, las organizaciones deben desarrollar y actualizar metodologías para administrar la privacidad así como también implementar o actualizar un marco de gobierno, realizar evaluaciones de impacto y garantizar un programa de privacidad de datos.

Prioridades de privacidad para los próximos 12 meses

Las oportunidades a futuro

El progreso tecnológico y cibernético en la última década se ha acelerado. Consideremos, por ejemplo, que hace sólo 10 años Amazon lanzó sus Servicios Web de Amazon (AWS) para entregar IT a las empresas. Hoy en día, la mayoría de las organizaciones de todo el mundo (el 63% de los encuestados) ejecutan servicios de IT en la nube.

Por otro lado, el 59% de encuestados dicen que están aumentando su gasto en seguridad como resultado de la digitalización de los sistemas. Por este motivo, las empresas están optimizando los modelos de negocios para la era digital.

Por último, la capacidad de entender la ciberseguridad y las amenazas a la organización. En 2008, el 42% de los encuestados no conocía la fuente de detección de incidentes de seguridad. Este año, sólo el 13% de los encuestados no pudo identificar qué tipo de actores -como empleados, socios comerciales, hackers, hacktivistas y estados nacionales- eran responsables de intrusiones.

Acerca de nuestros servicios en Seguridad de la Información

Forrester Research reconoció en 2009 a PwC como líder mundial en áreas de Seguridad de la Información y Consultoría de Riesgos de Tecnología:

"PwC ofrece una práctica de seguridad madura, que se encuentra integrada con la privacidad y la gestión de los riesgos en una sola estructura. La compañía tiene una fuerte presencia global. En nuestra evaluación, PwC ha obtenido los mejores puntajes en materia de administración de clientes y cuentas".

The Forrester Wave™: Security Consulting.

En PwC Argentina, contamos con una práctica que tiene más de 15 años en el mercado. La misma está compuesta por profesionales con vasta experiencia y diversidad de conocimientos en materia de seguridad de la información, especializados por industria, plataforma y aplicación.

Contamos además con un laboratorio de seguridad especialmente diseñado para llevar a cabo estudios de seguridad y análisis.

Asimismo, asistimos a nuestros clientes en:

- Cyber-security: Modelado de ciber-amenazas, Ejecución de Cyber-ejercicios, Cyber-intelligence
- Servicios gestionados de detección y respuesta a incidentes en activos de la red
- Pruebas de intrusión (Ethical Hacking)
- Implantación de soluciones de gestión de identidades y accesos
- Investigaciones forenses en el campo de la seguridad informática
- Cumplimiento normativas: PCI DSS, SOX, Ley de protección de datos personales y BCRA 4609/A
- Alineación con estándares ISO 27001, BS25999, ISO22301, COBIT e ITIL
- Revisiones de seguridad de sitios web, aplicaciones, tecnologías de base, seguridad física y patrimonial
- Estudios de vulnerabilidades de plataformas
- Testeo de seguridad de soluciones específicas
- Implantación de esquemas de seguridad para diversas tecnologías y plataformas
- Simulación de ambientes informáticos
- Pruebas de software y herramientas de seguridad
- Desarrollo de infraestructuras PKI
- Implantación de VPNs
- Definición de planes de respuesta ante incidentes
- Desarrollo e implantación de planes de continuidad del negocio
- Elaboración de estrategia y plan de seguridad

Contactos

Enzo Taibi **| Socio**
(54 11) 4850 - 6819
enzo.i.taibi@ar.pwc.com

Diego Taich **| Director**
(54 11) 4850-6811
diego.taich@ar.pwc.com

Oficinas

Buenos Aires
Bouchard 557, Piso 7°
(C1106ABG) Buenos Aires
Tel.: (54 11) 4850-0000
Fax: (54 11) 4850-1800

Córdoba
Av. Colón 610, Piso 8°
(X5000EPT) Córdoba
Tel.: (54-351) 420-2300
Fax: (54-351) 420-2332

Mendoza
9 de Julio 921, Piso 1°
(M5500DOX) Mendoza
Tel.: (54-261) 429-5300
Fax: (54-261) 429-5300
(int. 1116)

Rosario
Madres de Plaza 25 de Mayo
3020, Piso 3°
(S2013SWJ) Rosario
Tel.: (54-341) 446-8000
Fax: (54-341) 446-8016