www.pwc.com/ar

Resultados de la Encuesta Global de Seguridad de la Información

Advisory

pwc

Auditoría. Asesoramiento Impositivo y Legal. Consultoría.

Introducción

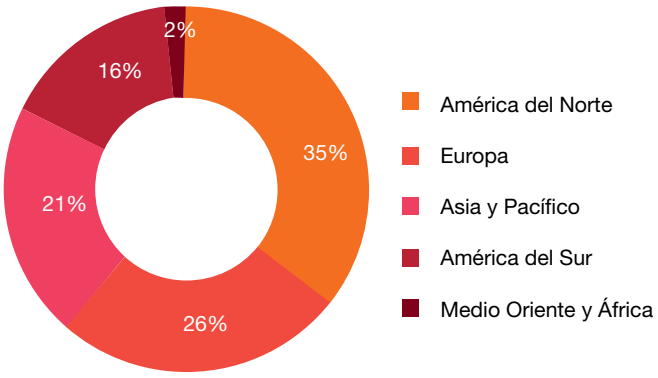
Nos complace presentarles los resultados de la encuesta que PwC realiza anualmente: Global State of Information Security Survey (Encuesta global sobre Seguridad de la Información).

Contenidos

Participación y metodología

La Encuesta global de Seguridad de la Información 2014 es un estudio mundial realizado por PwC y las revistas CIO Magazine y CSO Magazine. La misma se llevó a cabo en forma online del 1 de febrero de 2013 al 1 de abril de 2013. Los resultados presentados en este informe se basan en las respuestas de más de 9600 ejecutivos, incluyendo CEOs, CFOs, CIOs, CISOs, CSOs, Vicepresidentes y Directores de TI y Seguridad de la Información de 115 países. El 36% de los encuestados provienen de América del Norte, 26% de Europa, 21% de Asia y Pacífico, 16% de América del Sur y el 2% de Medio Oriente y África. Del total, el 3% de las repuestas fueron obtenidas de Argentina.

Figura 1. Porcentaje de encuestados



El centro de la cuestión

Si bien los riesgos en materia de seguridad de la información han evolucionado y se han incrementado, las estrategias de seguridad no le han seguido el ritmo. En base a esto, muchas organizaciones aún confían en estrategias de seguridad poco aptas para afrontar las amenazas existentes hoy en día.

Como agravante de la cuestión, el espectro de ataque se expandió (a socios, proveedores, clientes, y otros), dado que cada vez hay un mayor volumen de datos que viajan a través de canales digitales.

Dada esta situación, la seguridad de la información se ha convertido en una disciplina que exige tecnologías innovadoras, procesos y habilidades basadas en técnicas de contrainteligencia, y el apoyo de los altos ejecutivos.

Por consiguiente y de acuerdo a los resultados de la Encuesta global de Seguridad de la Información 2014, los ejecutivos están prestando mayor atención a la necesidad de financiar las actividades de seguridad.

> Los resultados arrojan que los incidentes de seguridad detectados han aumentado un 25% respecto al año anterior, mientras que los costos financieros de los incidentes se han incrementado un 18%.

También revela que muchas organizaciones no han implementado tecnologías para detectar vulnerabilidades y amenazas a las que sus entornos se encuentran expuestos, así como identificar y proteger activos claves del negocio.

Hoy en día las empresas están cada vez más interconectadas e integradas. Emplean la tecnología y la conectividad para compartir un volumen sin precedentes de activos de información con los clientes, proveedores, socios y empleados. Pero este sistema de negocios avanzado también las pone en peligro, debido a que aumentan los riesgos de seguridad.

Para evaluar las prioridades de los encuestados en la preparación para abordar las amenazas, se fijaron las prioridades de ejecución de procesos y tecnología de seguridad de los próximos 12 meses.

> “No se puede luchar contra las amenazas de hoy con estrategias de ayer”

La seguridad efectiva hoy requiere que las organizaciones identifiquen y den prioridad a la protección de los activos más críticos. En este sentido, el 25% de los encuestados manifiesta que priorizará la implementación de un programa para identificar los sensitivos, mientras que un 17% priorizará el uso de herramientas de gestión de activos.

Para mejorar la seguridad de la infraestructura, el 24% de los encuestados dicen que aplicarán normas de seguridad para los socios externos, proveedores, vendedores y clientes. Esto es importante en la medida que más organizaciones abren sus redes, aplicaciones y datos a terceros. Además, las tecnologías como la virtualización y servicios en la nube han ampliado las posibilidades de que un usuario con altos privilegios comprometa la información. En consecuencia, el seguimiento y la gestión de usuarios privilegiados es ahora un desafío clave, en este sentido encontramos que el 17% de los encuestados planea agregar herramientas de gestión de acceso para los usuarios privilegiados en los próximos 12 meses.

Figura 2. Principales medidas de protección para los próximos 12 meses

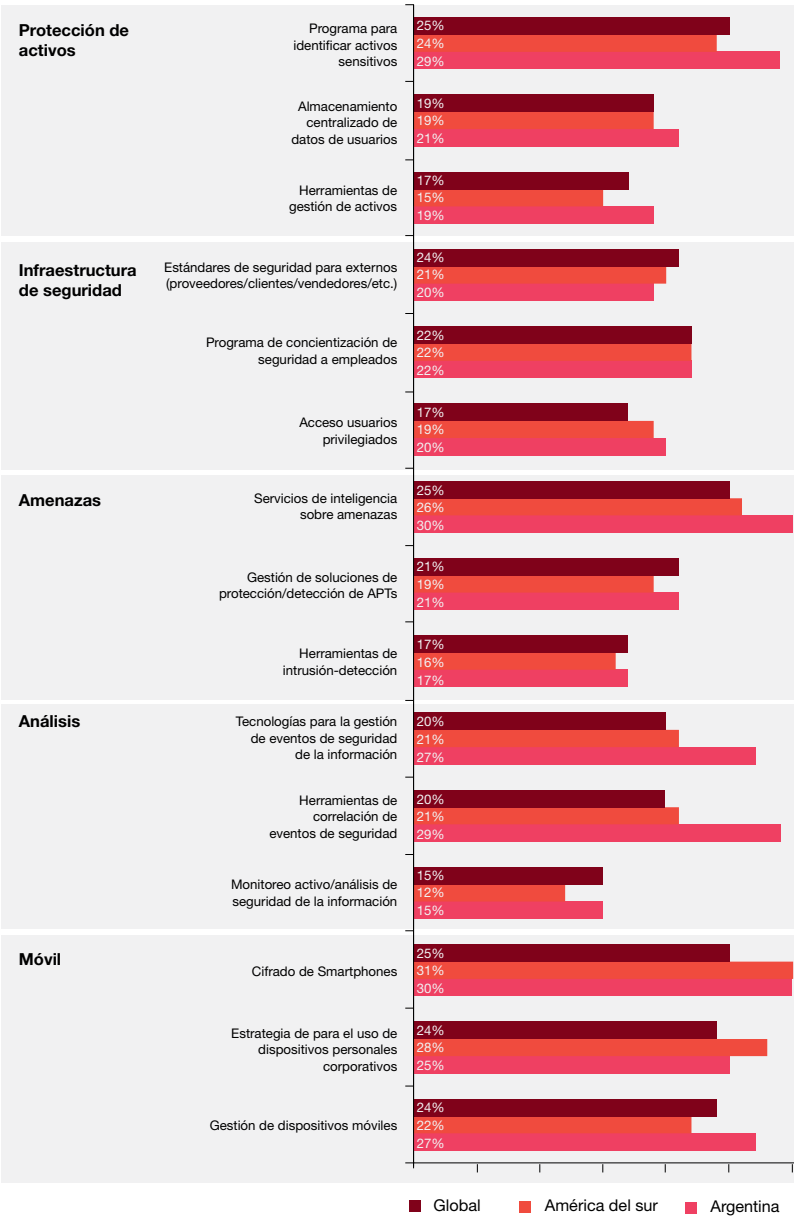
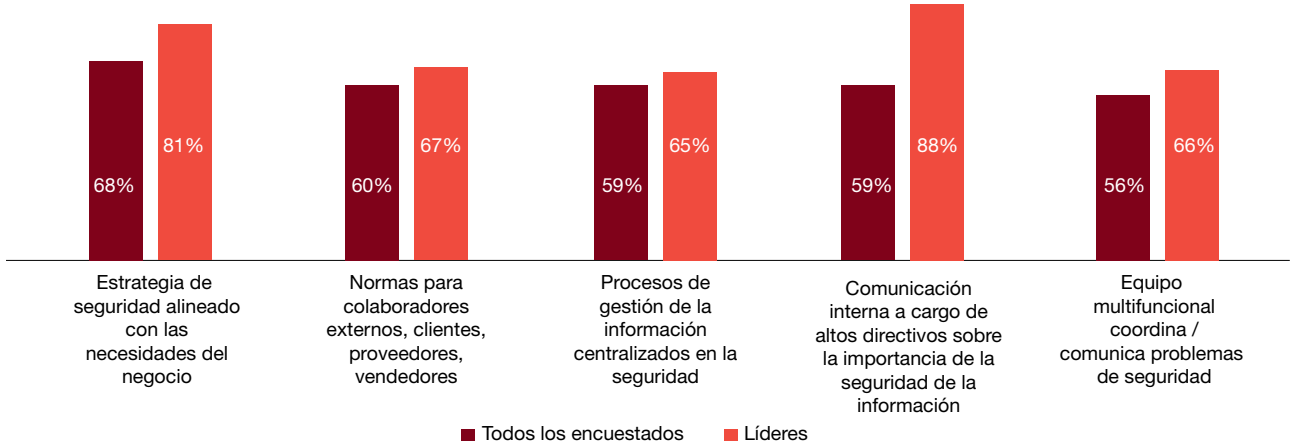


Figura 3. Principales medidas de protección y políticas de seguridad actuales



Fuerte confianza en las prácticas de seguridad actuales

Cabe destacar que, incluso en un clima de riesgos crecientes y constantes, los ejecutivos siguen mostrando confianza en las capacidades y acciones de seguridad de su organización. A nivel global, el 74% de los encuestados consideran que sus actividades son eficaces.

Entre los encuestados, el 50% fueron identificados como pioneros o asumen que su "organización tiene una estrategia eficaz y es proactiva en la ejecución del plan", el 26% se define como estrategas ya que considera que "son mejores para definir la estrategia que para llevarla a cabo", mientras el 13% se considera como tácticos debido a que son "mejores para hacer las cosas que en definir una estrategia efectiva". En cuanto al 11% restante, admite un rol de bombero ya que no tienen una estrategia eficaz y por lo general actúa de un modo reactivo. (Figura 3)

En Argentina se identificaron un 44% como pioneros y como estrategas un 27%. En cuanto a los denominados tácticos, fue identificado un 18%, y un 11% los llamados bomberos.

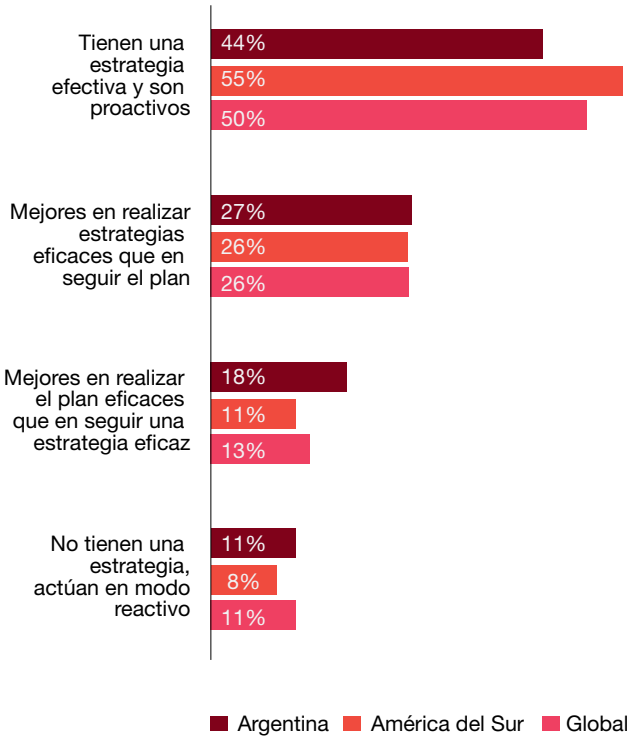
Pero, ¿son realmente pioneros?, medimos las autoevaluaciones en cuatro criterios clave que se utilizan para definir el liderazgo.

Los verdaderos líderes deben:

- Tener una estrategia de seguridad de la información;
- Contar con la función de un CISO o equivalente que informe "a la alta dirección";
- Evaluar, cuantificar y monitorear la eficacia de la seguridad de la información en el último año;
- Comprender los eventos de seguridad de la información ocurridos en el último año.

En base a estos requisitos, nuestro análisis revela que sólo el 17% de los encuestados realiza las acciones.

Figura 4. Cómo caracterizan a su organización en relación a la seguridad de la información



Incidentes de hoy, estrategias del ayer

Los resultados de la encuesta corroboran algunos datos relativos a los incidentes de seguridad.

En 2013, el 24% de los encuestados informó que sufrió pérdidas de datos como consecuencia de los incidentes de seguridad, un aumento del 16% respecto a 2012. En relación a los tipos de datos explotados, se revela que los registros de los empleados (35%) y de los clientes (31%) encabezan la lista en cuanto a la información más dañada.

Figura 5. Cifras promedio de los incidentes de seguridad

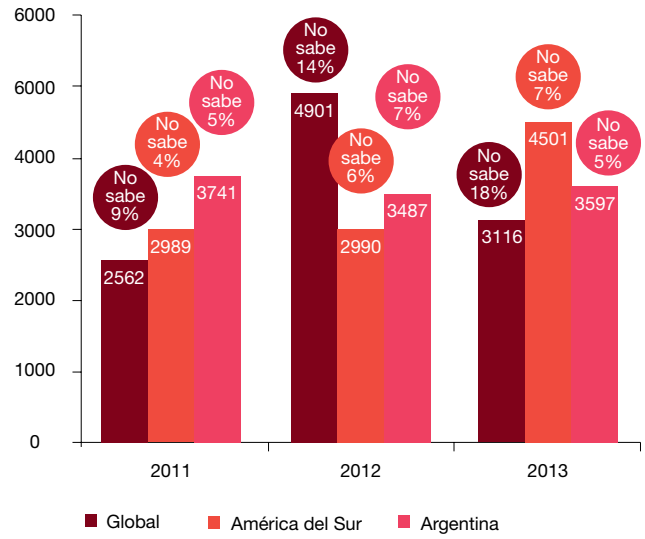
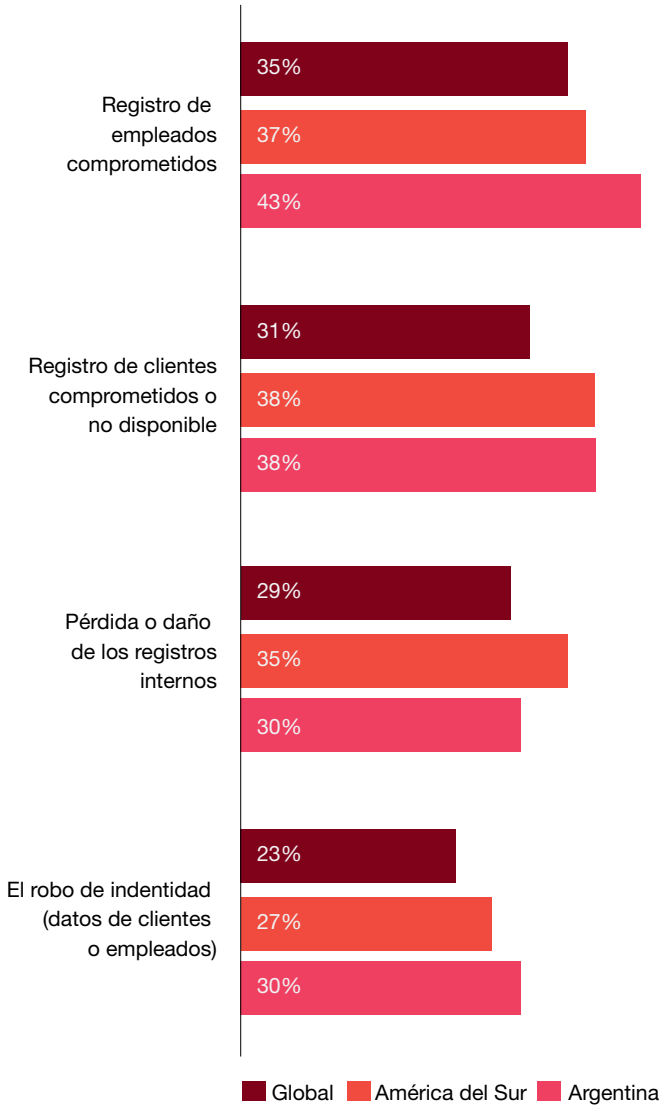


Figura 6. Impacto de los incidentes de seguridad



Los encuestados han reportado un incremento del 25% en los incidentes detectados en comparación con el año 2012. Este resultado también podría significar que las organizaciones han mejorado en cuanto a las tareas de identificación de los incidentes.

> "El aumento en la detección de incidentes de seguridad debe ser visto como un avance positivo."

Sin embargo, el número de encuestados que desconoce la frecuencia de incidentes aumenta anualmente y esto parece contradecir la afirmación que dice que las organizaciones han mejorado en la detección de aquellos. Esto último, sugiere que los modelos de seguridad en uso ya no son eficaces.

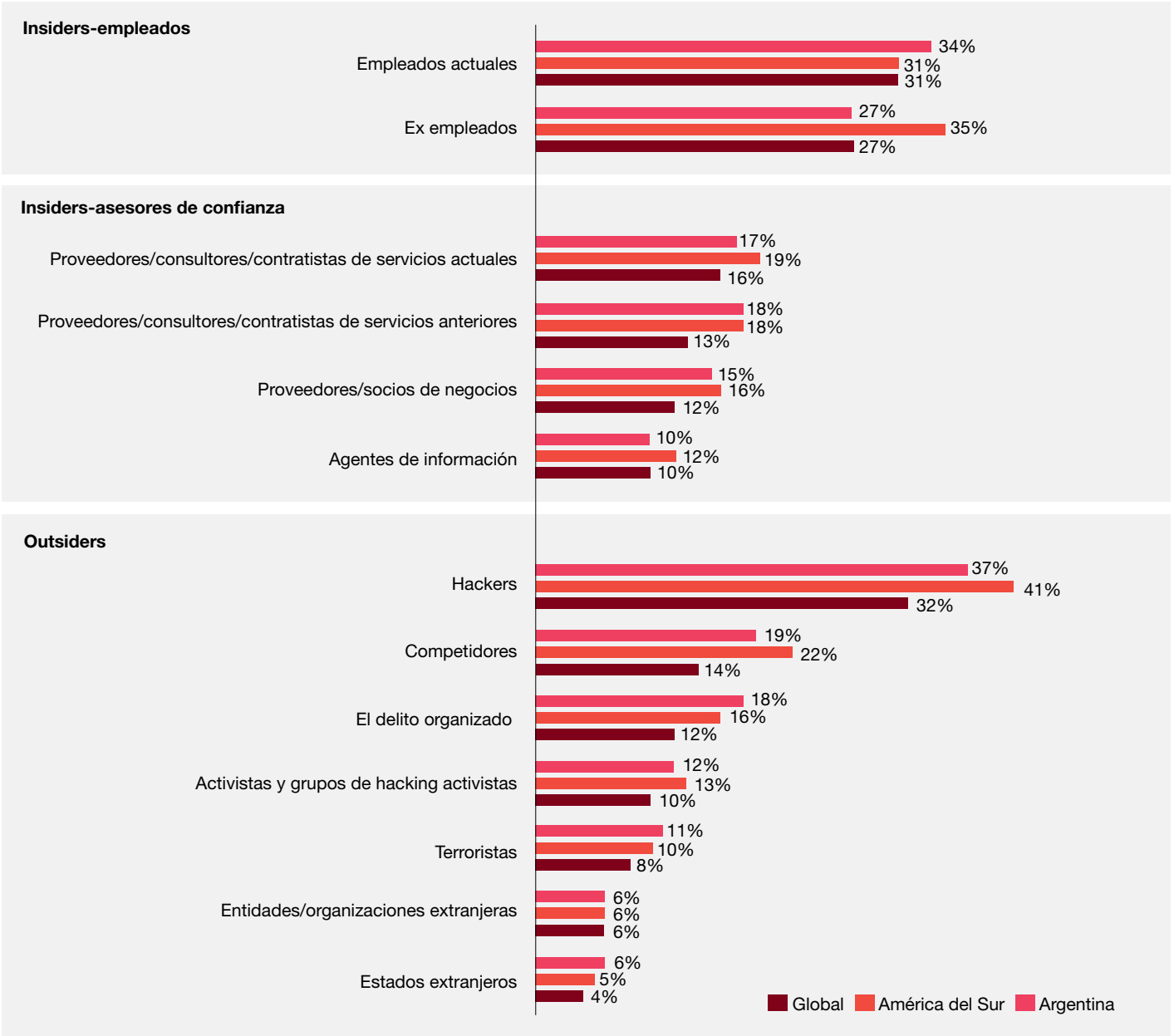
El promedio de pérdidas financieras asociadas con los incidentes de seguridad aumentaron un 18% respecto al año pasado. Desde el 2011 las pérdidas financieras han incrementado un 51%.

Insiders, outsiders y hackers

La mayoría de los encuestados atribuye los incidentes de seguridad a los accesos a la información privilegiada por los empleados actuales (31%) o ex empleados (27%).

> "Es importante destacar que las amenazas internas no provienen necesariamente de un "Hacker" o de un "usuario malintencionado", sino que podría ser el perfil de un buen empleado que hace el trabajo justo de manera insegura".

Figura 7. Fuentes probables de incidentes



Si bien hay una prevalencia de riesgos en relación a los empleados, hay que destacar que muchas organizaciones no están preparadas para administrar las amenazas internas. Asimismo, entre los factores de riesgo externos, el 32% de los encuestados atribuye los incidentes de seguridad a los hackers, un aumento del 27% respecto al año anterior.

Mientras que las "amenazas persistentes avanzadas" (APT, son aquellas que se refieren a grupos organizados y financiados para atacar determinados blancos) presentan un riesgo potencial a distancia, el seguimiento de la rápida evolución de las amenazas informáticas es una prioridad para las grandes organizaciones.

Obstáculos al avance de la seguridad

Aunque la mayoría de los referentes de seguridad coinciden en que debe haber mayor colaboración entre las partes, para que puedan tomarse nuevas medidas para mejorar la seguridad de la información, parece que hay poco consenso sobre los desafíos de hacerlo.

En general, los encuestados afirman que los obstáculos más importantes incluyen falta de presupuesto, falta de comprensión de las necesidades futuras del negocio que podrían afectar la seguridad de la información y la falta de una estrategia acorde.

La carrera global en materia de defensa

Desde hace varios años, Asia Pacífico se ha puesto a la cabeza de la inversión en tecnologías de seguridad, procesos y gastos. Aún ocupa el primer puesto, aunque por primera vez América del Sur parece a punto de tomar la delantera en las inversiones en información de seguridad, políticas y protección.

Qué significa para su negocio

Los resultados de la encuesta demuestran que la seguridad de la información está en un momento incierto, situada de forma simultánea en el umbral del cambio y el estancamiento en la situación vigente. Los encuestados muestran el progreso en la implementación de nuevas e importantes medidas de seguridad, por un lado, y la falta de atención a las estrategias clave como la protección de la propiedad intelectual, por el otro. Se identifica un renovado compromiso de invertir en seguridad junto a incertidumbre sobre la forma de mejorar las prácticas.

Acerca de los servicios de Advisory 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 las gestión de los riesgos en una sola estructura. La compañía tiene una fuerte presencia global de empleados y clientes, focalizándose generalmente en emprendimientos de gran escala. En nuestra evaluación, PwC también 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 de actividad 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, y con el aval y sustento que le brinda un programa de capacitación especializado.

Contamos además con un laboratorio de seguridad especialmente diseñado para llevar a cabo estudios de seguridad y análisis. Es un centro de instalación, prueba y operación sobre servicios y soluciones de seguridad informática para cualquier tecnología o plataforma.

Asimismo, asistimos a nuestros clientes en:

- 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.
- Medición de Audiencia Online.
- 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

Jesús M. Estévez | Socio | (54 11) 4850-6819 | jesus.m.estevez@ar.pwc.com

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

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

Rosario
Madres de Plaza 25 de Mayo 3020, Piso 3
(S2013SWJ) Rosario
Tel.: (54 341) 446-8000 | Fax: (54.341) 446-8016

@PwC_Argentina /PwCArgentina YouTube /PwCArgentina