

# Press Release

## Contactos

### Juan Giovaneli

Responsable de comunicación  
PricewaterhouseCoopers Argentina  
+54 (11) 4850 0000 int. 4970  
juan.pablo.giovaneli@ar.pwc.com

### Leandro Fogliatti

Asistente de comunicación  
PricewaterhouseCoopers  
+54 11 4850 0000 int. 4967  
leandro.fogliatti@ar.pwc.com

### Fernando Frías

Director Ejecutivo  
RFB Lynch Partners  
+54 11 4813 7550 int. 117  
fernando.frías@rfblynch.com



## Se fortalece la seguridad informática pero aún ocurren incidentes con frecuencia

El 79% de las compañías ha establecido formalmente procesos de seguridad de la información pero sólo el 29% tiene un director a cargo del tema. En 2008, los ataques más comunes fueron la explotación de datos y redes y los incidentes perpetrados a través del correo electrónico. Los empleados fueron la principal fuente de incidentes, seguidos de cerca por los ex-empleados y los hackers.

**Buenos Aires, 26 de mayo de 2009.-** Las empresas en América del Sur empiezan a alinearse con las prácticas de Seguridad de la Información establecidas en Europa y América del Norte, a medida que las inversiones en tecnología siguen creciendo. Sin embargo, todavía algunas áreas de tecnología no pueden precisar cuáles fueron los incidentes de seguridad más comunes sufridos durante el último año, en qué cantidad se produjeron y cuáles fueron sus fuentes de origen, de acuerdo con la Encuesta de Seguridad de la Información 2009, realizada por PricewaterhouseCoopers.

En abril pasado, la consultora internacional Forrester Research nombró a PwC como líder mundial en áreas de Seguridad de la Información y Consultoría de Riesgos de Tecnología. Según mencionó la firma de investigación, "PwC es líder por su superadora

comprensión de los requerimientos del negocio que se combinan con profundas habilidades técnicas; tiene una larga historia de innovaciones en este ámbito y cada vez gana mayor presencia aplicando soluciones pragmáticas”.

“Para capturar los beneficios de la tecnología destinada a cumplir con objetivos relacionados a la seguridad, privacidad, cumplimiento de las políticas organizacionales, y estrategias de continuidad del negocio, se requiere el mayor conocimiento posible sobre el origen de las amenazas a la información, qué impacto tienen sobre la compañía, y cuáles son las metodologías y soluciones existentes en el mercado tecnológico para hacerles frente”, explicó Edgardo Sajón, socio a cargo de la práctica de consultoría tecnológica de PricewaterhouseCoopers.

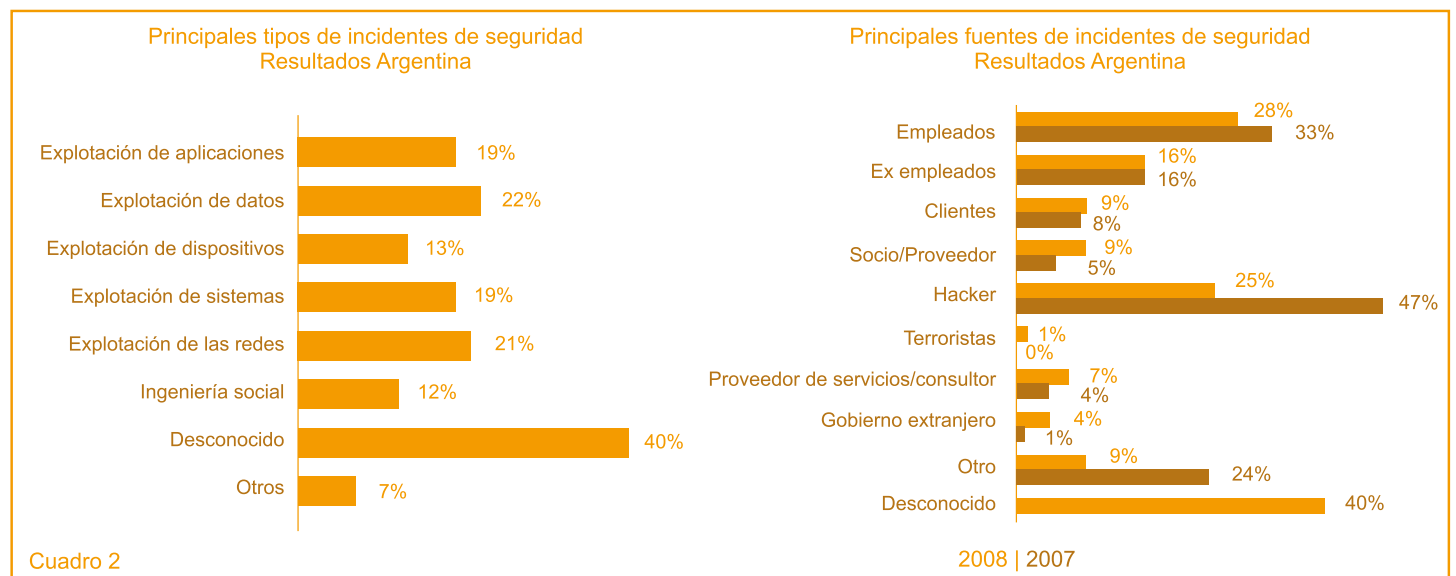
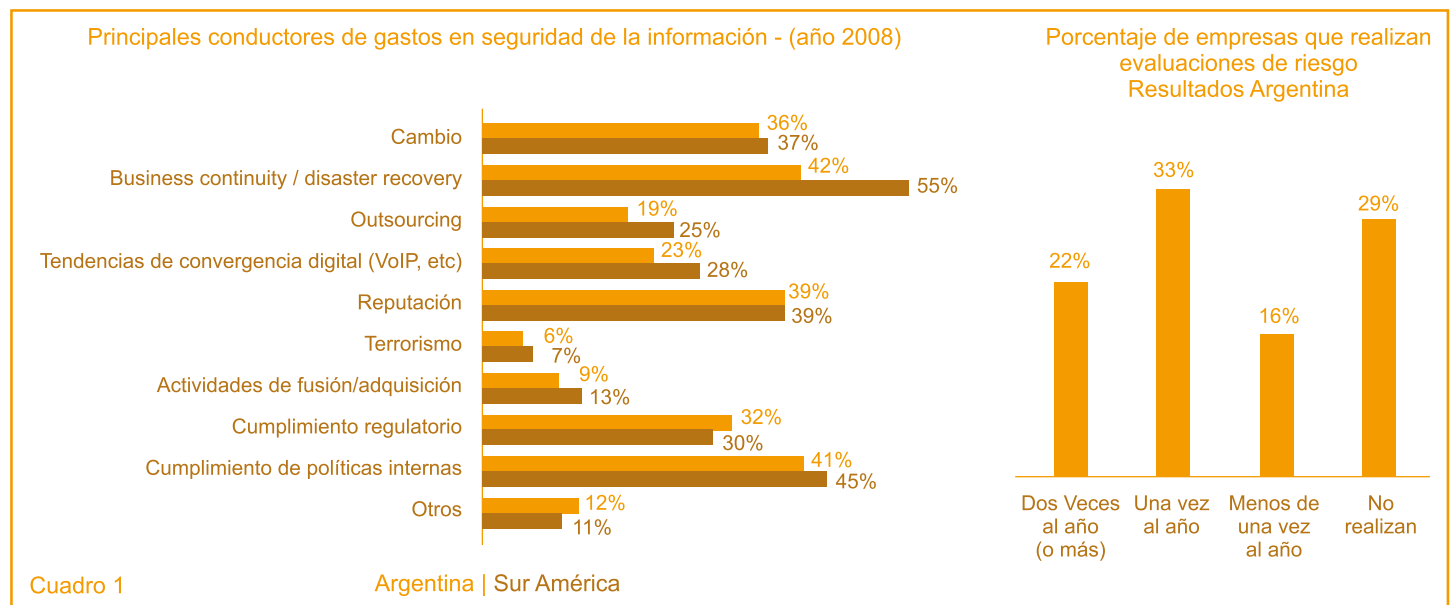
El fraude fue, durante el 2008, una de las principales consecuencias de los incidentes de seguridad sobre los datos de las organizaciones. En nuestro país, el 22% de los encuestados afirmaron haber sufrido algún tipo de fraude a raíz de un incidente de seguridad registrado en sus compañías. Durante el 2007, este índice alcanzaba valores de sólo 7% para la Argentina, lo que significa que el número se triplicó en un año.

Las compañías que brindan servicios financieros son las más susceptibles de ser víctimas de algún tipo de fraude como consecuencia de incidentes de seguridad de la información.

A pesar de que el soporte tecnológico provisto fue mucho mayor que en años anteriores, el 35% de los encuestados a nivel local no supo responder cuántos incidentes de seguridad ocurrieron en el último año en sus organizaciones; el 44% no pudo informar qué tipo de incidentes de seguridad representa la mayor amenaza a la información de su compañía; y 42% de los encuestados no pudo confirmar la fuente más probable de ataques realizados contra los activos de información de su compañía.

Los resultados de Argentina se alinean con los globales: el 30% afirmó desconocer el número de eventos de seguridad ocurridos en los últimos 12 meses; cerca del 40% no conoce el tipo de incidente ocurrido; y el 39% de los encuestados desconoce la fuente de incidentes de seguridad. (CUADRO 1)

Los más comunes incidentes de seguridad conocidos durante el 2008 fueron la explotación de datos (22%), la explotación de redes (21%), y los incidentes perpetrados



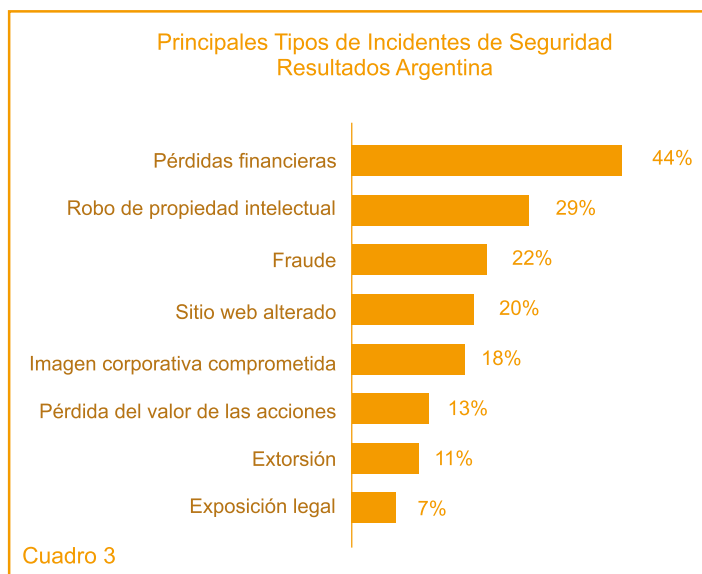
a través del correo electrónico como método principal (79 por ciento).

Este año los encuestados fueron a nivel global menos proclives a considerar a su propio staff como la fuente probable de incidentes de seguridad (34% vs. 48% en 2007). Sin embargo, en la Argentina, las fuentes más importantes de incidentes fueron los empleados en el 28% de los casos; ex-empleados, con 16%; y las amenazas de hackers (25% vs. 47% en el 2007).

(CUADRO 2)

### Factores determinantes de los gastos en Seguridad de la Información

Al consultar respecto a los gastos en materia de Seguridad de la Información, los encuestados globales apuntaron principalmente a procesos críticos como la continuidad del negocio y la recuperación de desastres (57%), pero también citaron cuestiones como la gestión del cambio (40%), el cumplimiento regulatorio (44%) y



las políticas internas (46 por ciento).

Los resultados fueron similares para Argentina y América del Sur, ya que la principal motivación para invertir en seguridad informática fue la continuidad del negocio y la recuperación de desastres (55% y 42% para América del Sur y Argentina, respectivamente). Luego, aparecen las inversiones en imagen de la compañía (39% tanto para América del Sur como para Argentina); y la gestión del cambio (37% y 36% América del Sur y Argentina, respectivamente). (CUADRO 3)

Existen distintas formas de distribuir los fondos del presupuesto de Seguridad, pero no todas están igualmente alineadas con la dirección estratégica del negocio. Los CISOs (Chief Information Security

Officers) perciben aún una brecha significativa entre el gasto en materia de seguridad y los objetivos del negocio. Solo el 29% de las organizaciones a nivel global afirmaron tener actualmente cubierto el puesto de CISO.

Al consultar respecto a la realización de evaluaciones de riesgo, sólo el 33% de los encuestados afirmó estar llevando a cabo este tipo de actividades al menos una vez al año, mientras que un porcentaje similar (29%) declaró que no las realizan en absoluto.

### Procedimientos críticos de Seguridad

Los resultados de la encuesta indican que las compañías requieren prestar mayor atención a los procesos críticos de Seguridad de la Información y a la selección y entrenamiento del personal que ejecuta dichos procesos.

Este año, aquellos que contestaron nuestra encuesta, informaron un avance de diez puntos respecto al año anterior en la implementación de algunos procesos críticos, como ser: el establecimiento de estándares de seguridad para el manejo de dispositivos móviles (42% vs. 32% en 2007), celulares/PCS/wireless (40% vs. 29% en el 2007), y la utilización de distintos niveles de autorización (30% vs. 20% en el 2007).

En nuestro país los resultados de la encuesta muestran que la mayoría de las empresas logró avances respecto al 2007 en establecimiento de estándares de seguridad para el manejo de dispositivos móviles como Celular/PCS/wireless (30% vs 22% en el 2007), el proceso centralizado de Seguridad de la información (44% vs 37% en el 2007) o monitoreo de los activos de Internet (54% vs. 41% en el 2007).

El porcentaje de compañías que no ha establecido formalmente procesos de seguridad de la información alcanza el 21 por ciento. Seleccionar y entrenar al personal a fin de mantener adecuados niveles de seguridad, también es un desafío y requiere establecer procedimientos detallados. En este sentido es necesario resaltar que sólo la mitad de las compañías cuenta con un procedimiento para controlar los antecedentes de los empleados (32%) y sólo el 46% ha implementado programas de entrenamiento sobre seguridad de la información.

El 54% de las organizaciones tiene personal dedicado a monitorear el uso de Internet/activos informáticos por parte de los usuarios.

## Control de acceso y privacidad

Los resultados muestran que sólo el 41% de las compañías afirma tener una estrategia de gestión de identidad y control para los accesos. El 52% explica que mitiga los riesgos sobre datos y robo de identidad implementando herramientas de monitoreo de las actividades de usuarios, y el 73%, aplicando aprovisionamiento automático de cuentas.

La encuesta revela que son pocas las compañías que están preparadas en forma adecuada para proteger la privacidad de los datos. Las inversiones en protección de la privacidad no se han incrementado en la medida necesaria a pesar de las numerosas noticias de violaciones a los datos de los clientes y organizaciones.

Resulta llamativo el bajo porcentaje de empresas (27% y 29% América del Sur y Argentina respectivamente), que afirmó llevar a cabo un entrenamiento sobre políticas y prácticas de privacidad para sus empleados. Por otra parte, sólo el 28% de ellas requieren que sus proveedores (terceros) adhieran por escrito a las políticas de privacidad de la organización.

Si bien es cierto que a nivel global, las compañías están más predispuestas a revisar sus políticas de privacidad anualmente (47% vs. 44% en el 2007), en Argentina este índice ha disminuido respecto al año pasado (32% vs. 35% en el 2007).

Los resultados en este aspecto también denotan que hay espacio de mejora en la Argentina: sólo un 38% de los encuestados dice haber establecido lineamientos de seguridad para proveedores y terceros; el 28% exige que los terceros adhieran por escrito a las políticas de seguridad de la organización, y sólo un 15% afirmó mantener un inventario de aquellos terceros que manejan datos de sus clientes o proveedores.

## Prevención de la pérdida de Datos

Cuando la pérdida de datos ocurre, se hace sentir fundamentalmente en términos de imagen y/o pérdidas económicas. Este año, un porcentaje significativo de los encuestados que acusó un impacto negativo en el negocio por pérdida de datos, apuntó a las pérdidas financieras (39%), robo de propiedad intelectual (30%), compromiso de ciertas marcas o de la imagen corporativa (27%), y fraude (21%), entre otros.

En nuestro país, al igual que en el resto del mundo, la pérdida de datos tuvo mayor impacto sobre las pérdidas financieras (44%), la propiedad intelectual (29%), la imagen de la organización (18%), y el fraude (22 por ciento). Pero el uso de soluciones para evitar las capturas no autorizadas de datos, sólo alcanza a un 28% de las organizaciones consultadas.