RISCCO
Risk & Business Consulting.
Internal Audit.

Moviéndose a la nube con cautela

Estudio sobre Seguridad de Información y Privacidad de Datos

3ra. edición
Junio 2012

Contenido

Introducción	3
Participantes del estudio	4
Resumen ejecutivo	5
Computación en la nube y tecnologías emergentes	7
Protegiendo la información de los clientes	10
Riesgos, desafíos y prioridades en seguridad de información	12
Estrategia y organización de la seguridad de información	16
Tecnologías de seguridad y su administración	18
Sobre RISCCO	22
Contactos	23

Introducción

En la tercera edición del Estudio de Seguridad y Privacidad de Datos, participaron noventa y ocho compañías e Instituciones del Estado, todas panameñas. Esta iniciativa, realizada de manera conjunta entre la Universidad Tecnológica de Panamá y RISCCO, es única en su género en nuestro país y cada año se está consolidando como una referencia para los profesionales de Seguridad de Información, Tecnología de Información y Riesgo Tecnológico.

A pesar de los riesgos de seguridad que implica, globalmente, existe una creciente utilización de la computación en la nube (cloud computing), dispositivos tipo “Tablet PC” y de las redes sociales. Los resultados del presente estudio indican que las organizaciones participantes están adoptando estas tendencias como propias, pero, pareciera que con cierta cautela. Los resultados reflejan que, para algunas tecnologías de seguridad, su adopción parece no ser una prioridad, entre los participantes. Sin embargo, en otras áreas de seguridad de información y gestión de riesgo tecnológico, hay signos positivos de que se está mejorando.

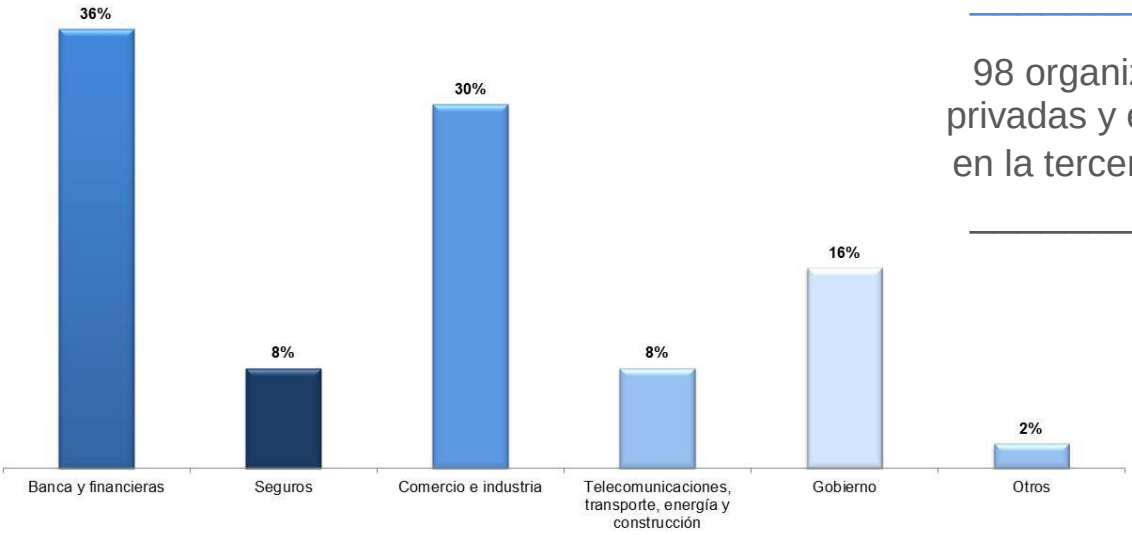
Nuevamente, la Universidad Tecnológica de Panamá y RISCCO, deseamos expresar nuestro agradecimiento a todos los participantes del estudio, por tomarse el tiempo y apoyar esta iniciativa.

Nicolás Samaniego
Decano
Facultad de Ingeniería de Sistemas Computacionales, UTP

Antonio Ayala I.
Vicepresidente Ejecutivo
RISCCO, S. de R. L.

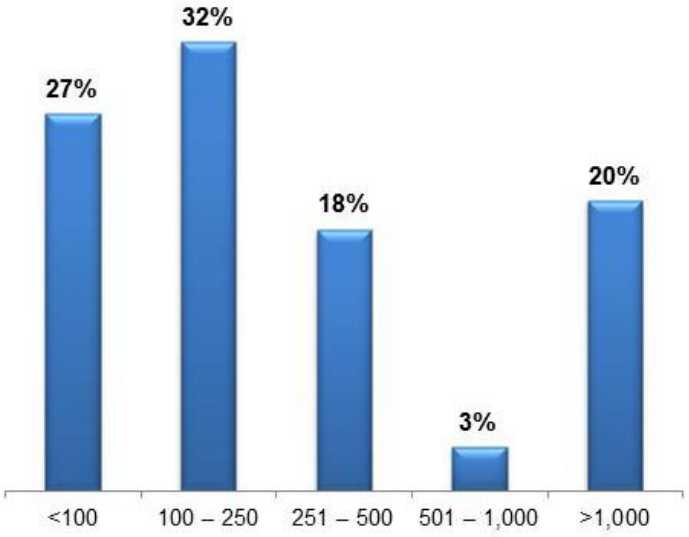
Participantes del estudio

Sector económico al que pertenecen las organizaciones participantes



98 organizaciones panameñas, privadas y estatales, participaron en la tercera edición del estudio.

Número de colaboradores de las organizaciones participantes



Nota: El lector debe tener en cuenta que, en algunas gráficas del estudio, el porcentaje podría no sumar 100, debido al redondeo.

Resumen ejecutivo

1. **La cautela parece ser el denominador común en la adopción de nuevas tecnologías como computación en la nube, uso de "Tablet PC" y acceso a redes sociales.**

   - Sólo un 17% de los participantes informó que está haciendo uso de la computación en la nube.
   - Sólo 24% permite oficialmente, el uso de dispositivos tipo "Tablet PC".
   - 78% restringe o no permite el acceso a las redes sociales.

2. **Frente al aumento de organizaciones afectadas por incidentes de seguridad y a que el riesgo tecnológico es mayor, los esfuerzos para protegerse parecen pocos.**

   - El 61% de los participantes manifestó que el riesgo tecnológico en sus organizaciones hoy día es mayor, debido al incremento de las amenazas externas y el 36% indicó que ha aumentado, debido al incremento de vulnerabilidades internas.
   - Sólo el 17% indicó que cuenta con los conocimientos y herramientas necesarios para hacer las investigaciones forenses que un incidente de seguridad demande.
   - La confirmación de sufrir incidentes de seguridad de información entre los participantes, ha aumentado a través de los años: 29% en 2010; 31% en 2011 y 46% en 2012.
   - Sólo el 9% de los participantes manifestó que su estrategia de seguridad de información, con relación a las amenazas y riesgos tecnológicos actuales, es adecuada.

3. **Se empieza a seguir la tendencia global de dar en outsourcing ciertas actividades de seguridad, usualmente realizadas a lo interno de las organizaciones.**

   Se han incrementado todas las actividades de seguridad abordadas en el estudio, que han sido dadas en outsourcing o que están bajo evaluación de darla. Algunos ejemplos son:

   - BCP/DRP, en 2010, el 21% manifestó que este servicio había sido dado en outsourcing o estaba en evaluación; en 2011, esta cifra fue de 20% pero, en el 2012 fue de 87%.
   - Para pruebas de penetración internas o externas a las redes, en 2010, el resultado fue 36%; en 2011, 62% y en 2012, 77%.
   - Para evaluaciones / auditorías de seguridad, en 2010, esta cifra fue de 33%; en 2011, 34% y en 2012, 63%.

4. La concienciación sobre la importancia de la seguridad de información dentro de las organizaciones, para algunos aspectos, ha evolucionado favorablemente.

- La existencia de un responsable de la seguridad de información dedicado al 100% o parcialmente, fue de 45% en 2010; 57% en 2011 y 63% en 2012.

- Los participantes indicaron que el presupuesto de seguridad de información al compararlo con el año anterior, se ha incrementado. Así lo afirmó un 41% de los participantes en 2010; 52% en 2011 y 54% en 2012.

5. Los desafíos y prioridades en cuanto a seguridad de información, permanecen casi estáticos.

- El principal desafío que experimentarán los participantes en 2012 será la falta de concienciación en cuanto a seguridad de información de los usuarios finales. Este desafío, ha sido también el número uno en la edición de 2010 y 2011.

- Con respecto a las prioridades en materia de seguridad de información, las cuatro primeras no han variado en las ediciones de 2010, 2011 y 2012. Este año al igual que el anterior, la primera es implantar o mejorar las tecnologías y procesos relacionados con la protección de datos. Las tres restantes son:

  - Mejorar los programas de concienciación hacia la seguridad en la organización.
  - Llevar a cabo pruebas de vulnerabilidad a las redes internas/externas.
  - Implantar nuevas tecnologías de seguridad de información.

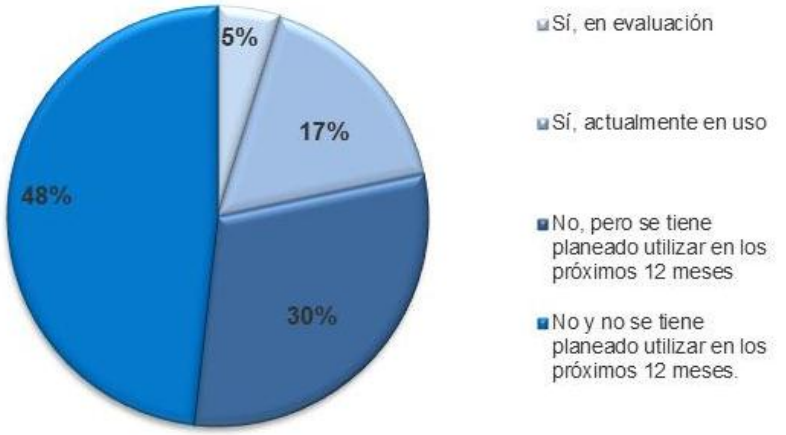
Computación en la nube y tecnologías emergentes

Los participantes del estudio se están moviendo, con cautela, a la utilización de computación en la nube en sus organizaciones, ya que, sólo un 17% indicó que actualmente hace uso de ella. Sin embargo, un 35% fue claro en señalar que en los próximos 12 meses, la utilizaran o bien, que actualmente la están utilizando a manera de prueba.

Para ser una tecnología relativamente reciente con muchos seguidores, pero también, con escépticos en su utilización por los riesgos tecnológicos que conlleva, pareciera que los participantes del estudio han reconocido sus beneficios y la están implantando con cautela.

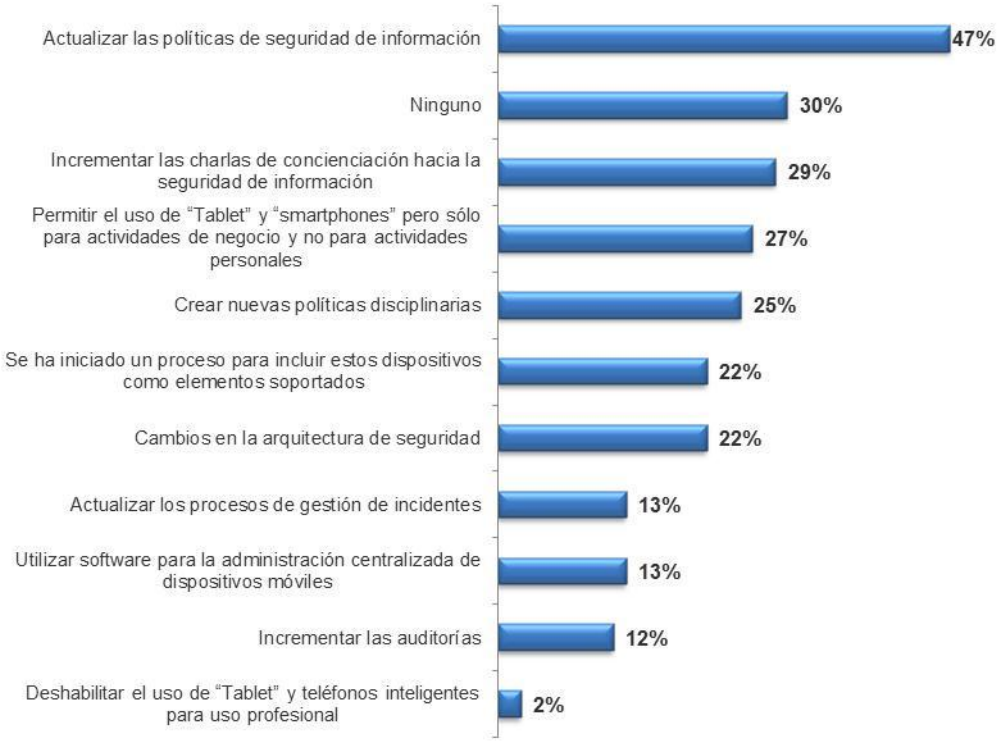
En cuanto a la utilización de computadores tipos “Tablet PC” para actividades de negocio, lleva cierta delantera al compararla con la adopción de computación en la nube, pues, un 24% de los participantes indicó que son ampliamente utilizadas y aprobadas por la organización.

¿Actualmente su organización utiliza servicios de computación en la nube o “cloud computing”?

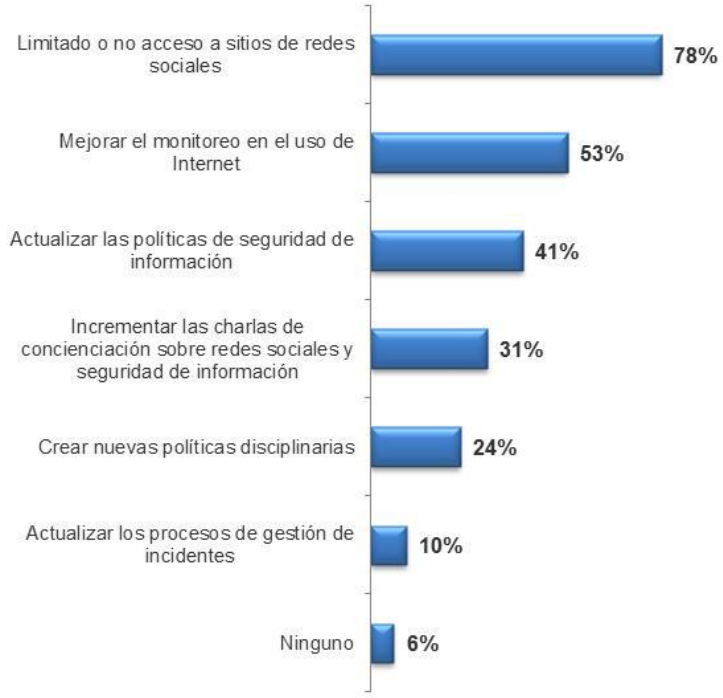


¿Actualmente en su organización se permite el uso de computadores tipo “Tablet PC” (por ejemplo, IPAD 2 o Samsumg Galaxy), para actividades de negocios?

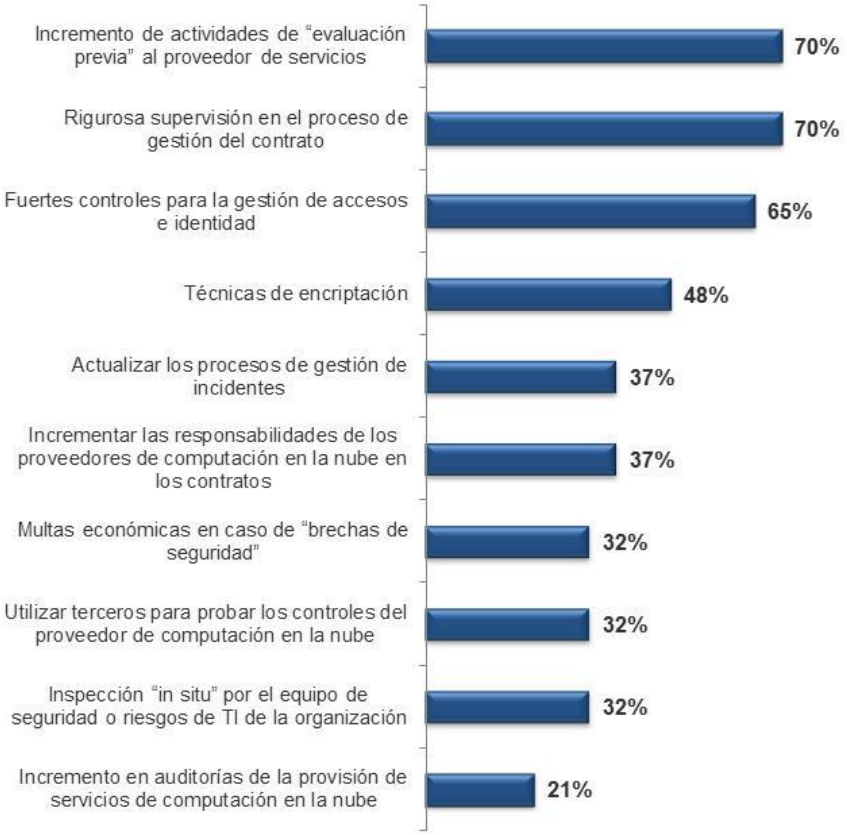
¿Cuáles de los siguientes controles ha implantado su organización para mitigar los nuevos riesgos relacionados con el uso de computación móvil (ejemplo, smarthphones, IPAD 2 o Samsumg Galaxy), para actividades de negocio?



¿Cuáles de los siguientes controles ha implantado su organización para mitigar los nuevos riesgos relacionados con el uso de redes sociales?



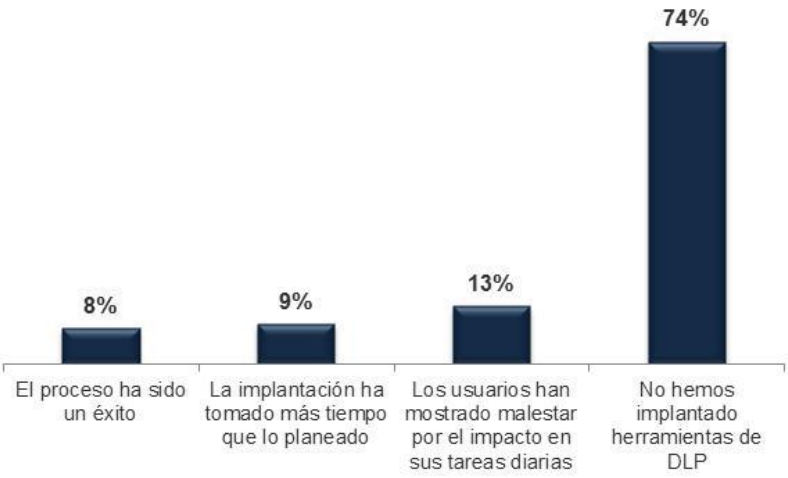
¿Cuáles de los siguientes controles ha implantado su organización para mitigar los nuevos riesgos relacionados con el uso de computación en la nube o "cloud computing"?



Protegiendo la información de los clientes

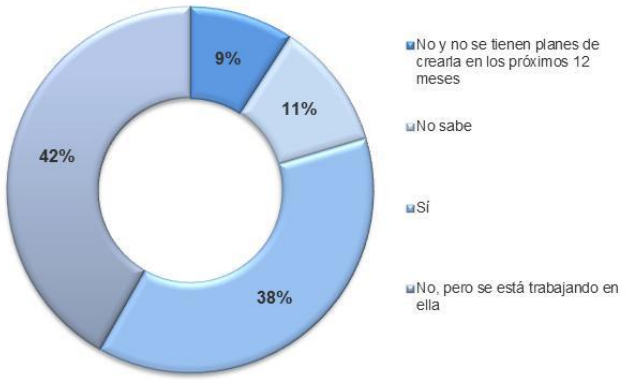
Las organizaciones hoy día, a diferencia del pasado, enfrentan el problema de la ubicuidad de los datos. Antes, la mayoría de los datos de los clientes y de la organización se encontraban "dentro" de las redes y computadores. Esto hacía relativamente simple proteger los datos. En la actualidad, los datos están, al menos en: servidores, computadores, proveedores de servicio, "Tablet PC", correos electrónicos, cintas de backup y teléfonos tipo "smartphones".

¿Con relación a la implantación de herramientas de Data Loss Prevention (DLP) en su organización, cómo describiría usted dicho proceso?



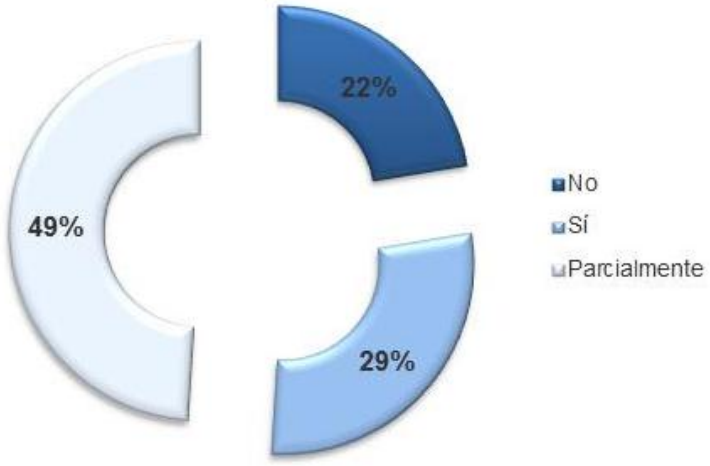
En esta línea de ideas, disponer de herramientas de software para la prevención de pérdida de datos (DLP por sus siglas en inglés) hoy día es vital. Pareciera que este tema, es un área con espacios importantes de mejora, ya que un 74% de los participantes indicó no disponer de herramientas tipo DLP. Además, sólo un 38% dispone de alguna estrategia para establecer controles para proteger los datos personales de sus clientes.

¿Existe alguna estrategia formal a nivel directivo, para establecer controles y procedimientos para proteger los datos personales de sus clientes?



¿Quién en la organización es el responsable de definir la estrategia para la privacidad y protección de los datos personales de los clientes a nivel corporativo?

¿Existe algún proceso para la clasificación de datos (público, confidencial, etc.) que permita definir los mecanismos de control para proteger los datos personales de los clientes?



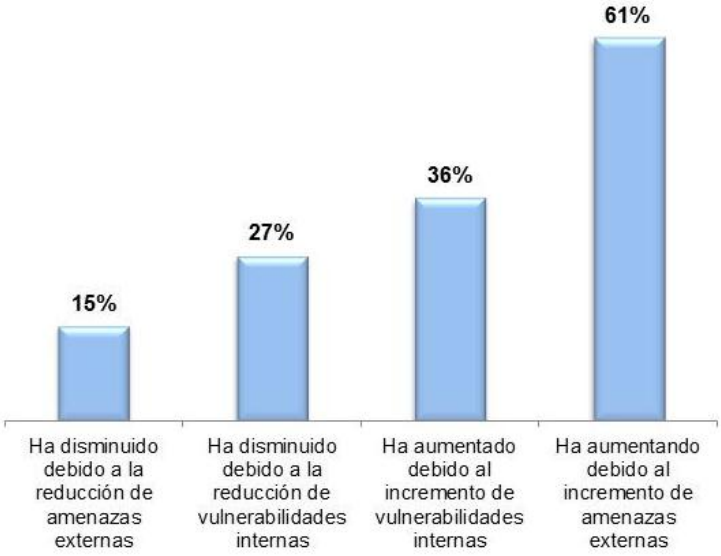
Riesgos, desafíos y prioridades en seguridad de información

Los participantes del estudio fueron claros en afirmar que, en los últimos doce meses, el riesgo tecnológico relacionado con la operación ha aumentando, a causa de amenazas externas y vulnerabilidades internas (61% y 36 % respectivamente).

Estos resultados son consecuentes con lo que experimentan otras organizaciones en otras latitudes. El riesgo tecnológico aumenta. Mucho más que una reflexión fría, debe ser un llamado de atención a los que dirigen las organizaciones en Panamá; al revisar los resultados del presente estudio, hay señales muy claras de que algunos parecieran no estar atendiendo con la suficiencia requerida, la seguridad de información y el riesgo tecnológico.

Este hecho no se puede ver de manera aislada, pues, al preguntar a los participantes si han sufrido algún incidente de seguridad en los últimos doce meses, el 46% contestó afirmativamente. Al analizar la respuesta anterior versus la misma pregunta del estudio de 2010 y 2011, es claro, que el incremento de los incidentes de seguridad de información en las organizaciones panameñas está ganando terreno.

¿Cómo el riesgo tecnológico relacionado a la operación de la organización, ha cambiado en los últimos 12 meses?



¿ Ha experimentado incidentes de seguridad en los últimos doce meses ?	2012	2011	2010
Sí	46%	31%	29%
No	54%	64%	63%
No sabe	-	5%	8%

Con respecto a las principales prioridades en seguridad de información, las tres primeras, para la edición de 2012 son las mismas que en el 2011. Al analizar los resultados (ver gráfica adjunta) para los años 2010, 2011 y 2012, las cuatro primeras prioridades no han variado. Resulta interesante destacar que implantar estándares de seguridad de información como ISO 27001, ha sido la antepenúltima prioridad de un número de doce, en las tres ediciones.

¿ Cuáles considera serán las principales prioridades, en cuanto a seguridad de información, el presente año?	2012	2011	2010
Implantar o mejorar las tecnologías y procesos relacionados con la protección de datos	78% (1)	69% (1)	62% (3)
Mejorar los programas de concienciación hacia la seguridad en la organización	69% (2)	61% (2)	55% (4)
Llevar a cabo pruebas de vulnerabilidad a las redes internas/externas	68% (3)	58% (3)	64% (1)
Implantar nuevas tecnologías de seguridad de información	52% (4)	48% (4)	64% (2)

Nota: El número entre paréntesis significa la posición de dicha prioridad entre todas las indicadas ese año.

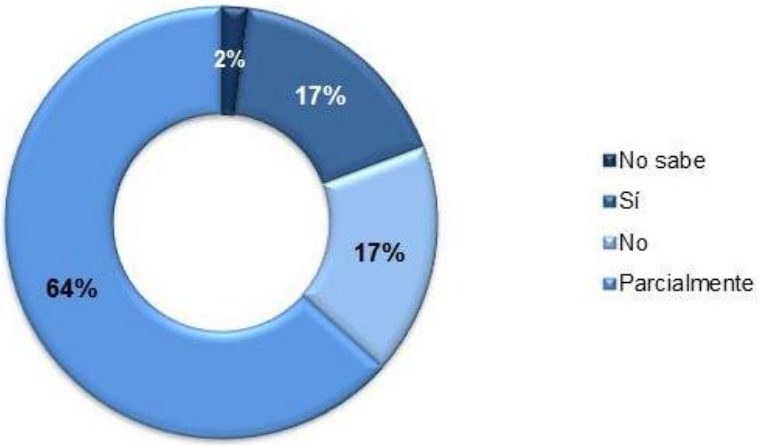
De manera similar, en cuanto a los desafíos en materia de seguridad de información, ha sido una constante para las tres ediciones, que el primer desafío es la falta de concienciación de los usuarios finales hacia la seguridad de información (ver gráfica adjunta). Los programas de concienciación toman un rol crítico en esto, ya que, como es conocido, el eslabón más débil en la cadena de seguridad de información es el usuario final.

Algo interesante entre los desafíos para la presente edición del estudio, es ver, que “cumplir con regulaciones locales o internacionales” ha escalado para estar entre las cuatro primeras posiciones. Probablemente, esto sea el reflejo de recientes regulaciones emitidas en esta materia, por entes reguladores como la Superintendencia de Bancos de Panamá o regulaciones internacionales como PCI-DSS.

¿ Cuáles considera serán las principales desafíos, en cuanto a seguridad de información, el presente año?	2012	2011	2010
Falta de concienciación de los usuarios finales	50% (1)	54% (1)	47% (1)
Evaluar oportunamente amenazas y vulnerabilidades	40% (2)	41% (3)	40% (4)
Disponibilidad de recursos	40% (3)	44% (2)	45% (2)
Cumplir con regulaciones locales/internacionales	35% (4)	16% (9)	22% (8)

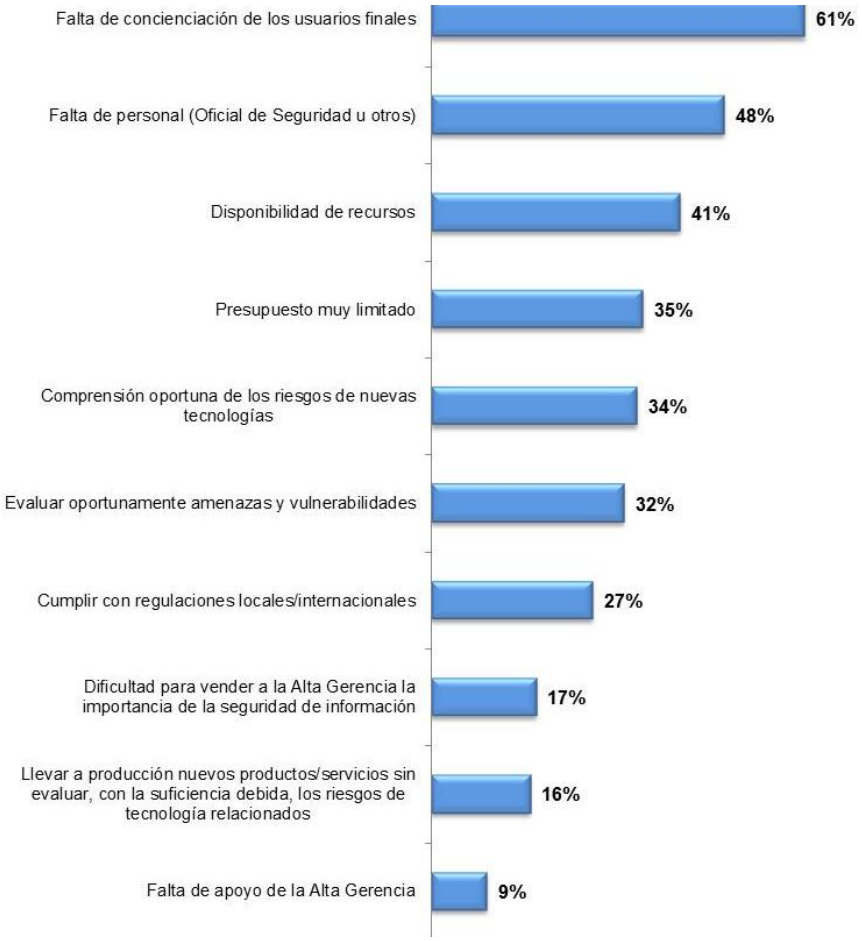
Nota: El número entre paréntesis significa la posición de dicho desafío entre todos los indicados ese año.

En caso de que ocurra un incidente de seguridad, ¿cuenta su organización con los conocimientos y herramientas necesarias para hacer las investigaciones forenses que demande el incidente?

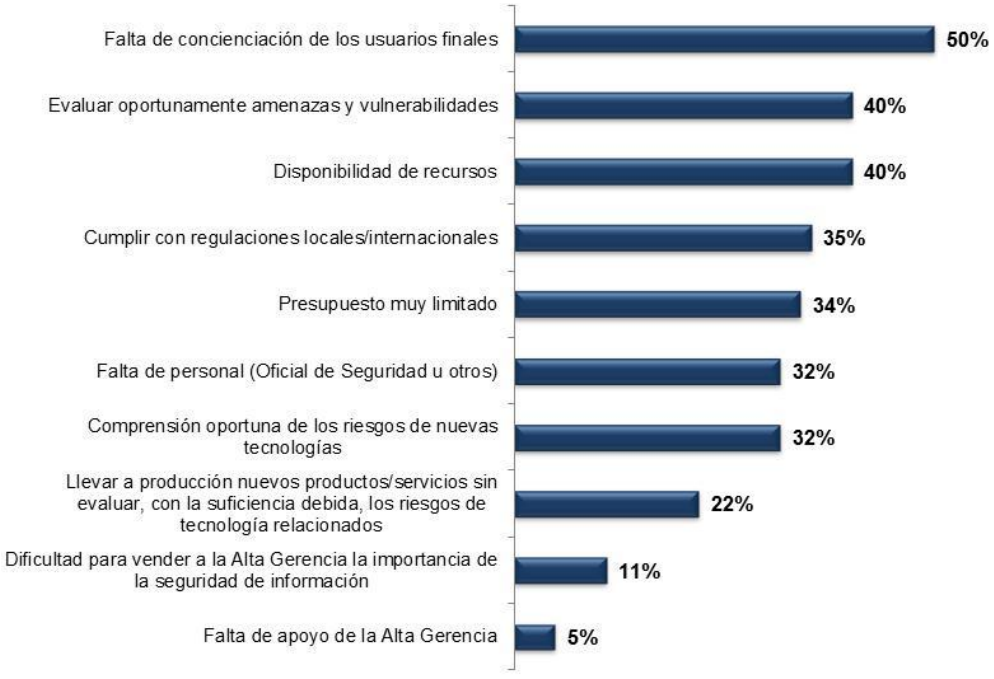


En el 2012, ¿cuáles considera usted serán las principales prioridades, en cuanto a seguridad de información, en su organización?

¿Cuáles fueron los principales desafíos experimentados en el 2011 con relación a la seguridad de la información en su organización?



En el 2012, ¿cuáles considera usted serán los principales desafíos para mejorar la seguridad de información en la organización?



Estrategia y organización de la seguridad

El eje fundamental para que el incremento de los riesgos tecnológicos afecte lo menos posible las operaciones de la organización y sus clientes, es disponer de una estrategia adecuada de seguridad de información. Sólo un 9% de los participantes indicó que la suya lo es.

Adicionalmente, muy relacionado con lo anterior, un 63% de los participantes confirmó que la función de seguridad de información no está cubriendo las necesidades de su organización.

Si bien es cierto lo anterior pudiese no ser alentador, los resultados del presente año, comparados con los resultados del 2010 y 2011 para los tema de oficial de seguridad de información y disponibilidad de un mapa de riesgo tecnológico, muestran signos favorables.

Con relación al oficial de seguridad de información, a pesar de que, aquellos dedicados al 100% no han variado significativamente (sólo 6 puntos porcentuales), lo cierto es que su ausencia se ha reducido de un 55% en 2010 a 37% en 2012.

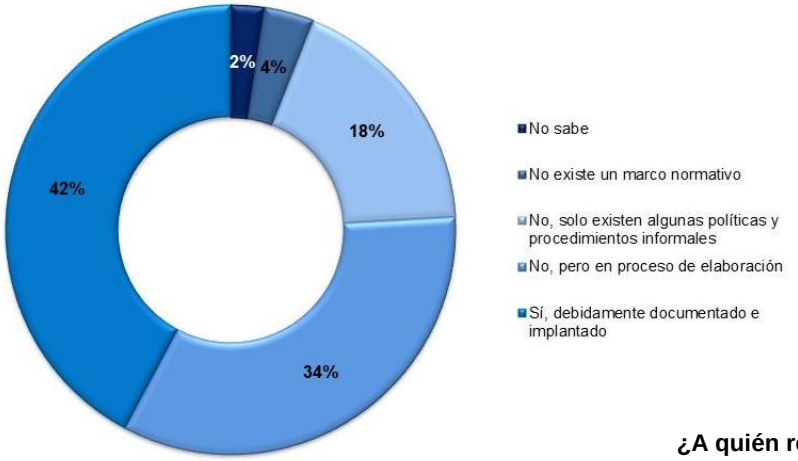
¿Cuál de los siguientes enunciados describiría es la mejor forma de estrategia de seguridad de información de su organización, en relación a las amenazas y riesgos tecnológicos actuales?

¿ Cuenta la organización con un oficial de seguridad de información ?	2012	2011	2010
Sí, dedicado al 100%	22%	20%	16%
Sí, dedicado parcialmente	41%	37%	29%
No	37%	43%	55%

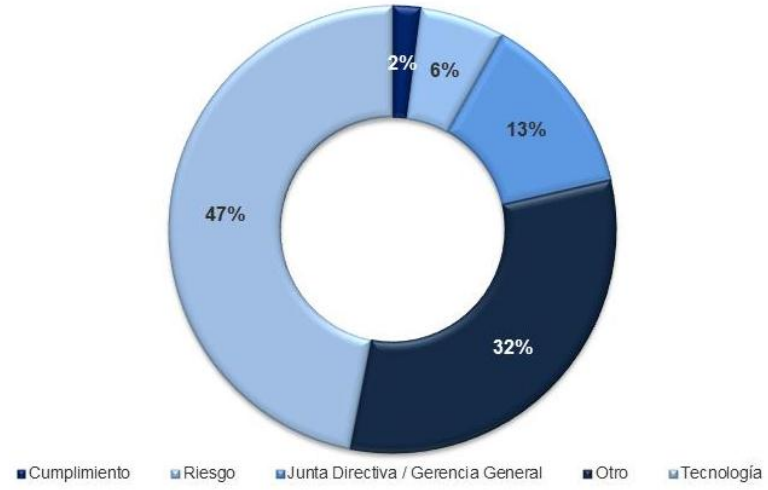
¿ Cuenta la organización con un mapa de riesgos tecnológicos?	2012	2011	2010
Sí	35%	29%	28%
No	59%	69%	69%
No sabe	6%	3%	3%

¿Considera que la función de seguridad de información está cubriendo las necesidades de su organización?

¿Dentro de su organización existe un marco normativo (políticas, procesos y procedimientos), para administrar la seguridad de información a fin de mitigar los riesgos derivados del uso de tecnología de información?



¿A quién reporta el Oficial de Seguridad de Información?



Tecnologías de seguridad y su administración

En cuanto a la utilización de tecnologías de seguridad, los resultados para los años 2010, 2011 y 2012 muestran que las tres más utilizadas son: antivirus; firewall y anti-spyware. Hay mayor utilización de herramientas para la correlación de bitácoras y para la gestión de parches. Las tarjetas inteligentes o tecnologías tipo "one time passwrod", parecieran no ser una prioridad al momento de adquirir nuevas tecnologías de seguridad.

Algo muy positivo en este estudio, al igual que los resultados del 2010 y 2011, es que, todo parece indicar que el presupuesto asignado a la seguridad de información no es el problema.

La afirmación anterior se basa en que, para los resultados del 2010, 2011 y 2012, el presupuesto asignado a la seguridad de información se incrementará o será el mismo. Esto ha sido una constante que consideramos favorable.

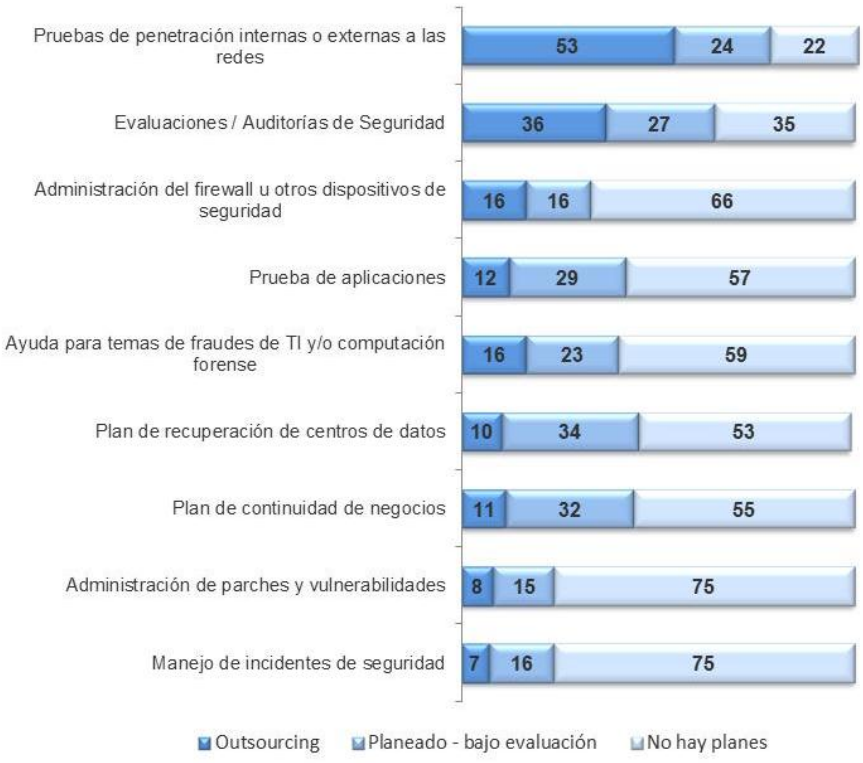
Otro aspecto interesante de los resultados al comparar el comportamiento de la adopción del outsourcing para los años 2010, 2011 y 2012, es que cada día, esta herramienta gerencial es más aceptada (ver gráfica en la siguiente página).

Tecnologías de seguridad utilizadas o en proceso de implantación (se muestran sólo algunas)	2012	2011	2010
Antivirus	96%	97%	93%
Firewall	93%	96%	85%
Anti-spyware	83%	83%	78%
Redes privadas virtuales (VPN)	78%	70%	68%
Software para monitoreo de redes	66%	70%	64%
Software para administración de parches/vulnerabilidades	53%	47%	45%
Cifrado - datos en tránsito	33%	38%	36%
Cifrado - datos almacenados (discos fijos)	31%	26%	34%
Software para la administración y correlación de bitácoras	27%	26%	15%
Cifrado - datos almacenados en medios removibles (USB)	27%	23%	26%
Tarjetas inteligentes u otro medio de one-time passwords	13%	11%	10%

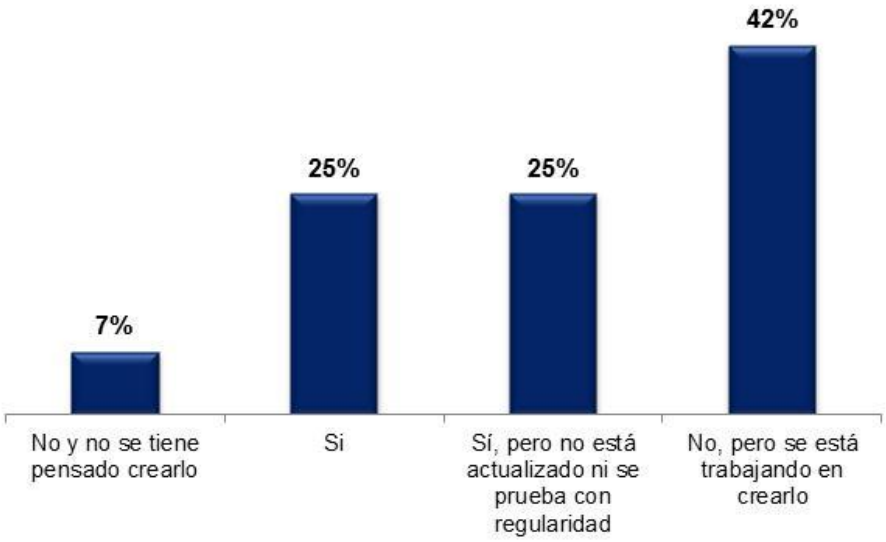
¿El presupuesto asignado a la seguridad de información para el año 2012 y comparado con el del año 2011 va a?	2012	2011	2010
Incrementar	54%	52%	41%
Será el mismo	27%	37%	40%
No sabe	17%	9%	15%
Se reducirá	2%	3%	4%

Actividades relacionadas con seguridad de información dadas en outsourcing o bajo evaluación de darla.	2012	2011	2010
Pruebas de penetración internas o externas a las redes	77%	62%	36%
Evaluaciones / Auditorías de Seguridad	63%	34%	33%
BCP / DRP	87%	20%	21%
Prueba de aplicaciones	41%	10%	14%
Ayuda para temas de fraudes de TI y/o computación forense	39%	8%	13%
Administración del firewall u otros dispositivos de seguridad	32%	25%	19%
Manejo de incidentes de seguridad	23%	12%	13%
Administración de parches y vulnerabilidades	23%	10%	13%

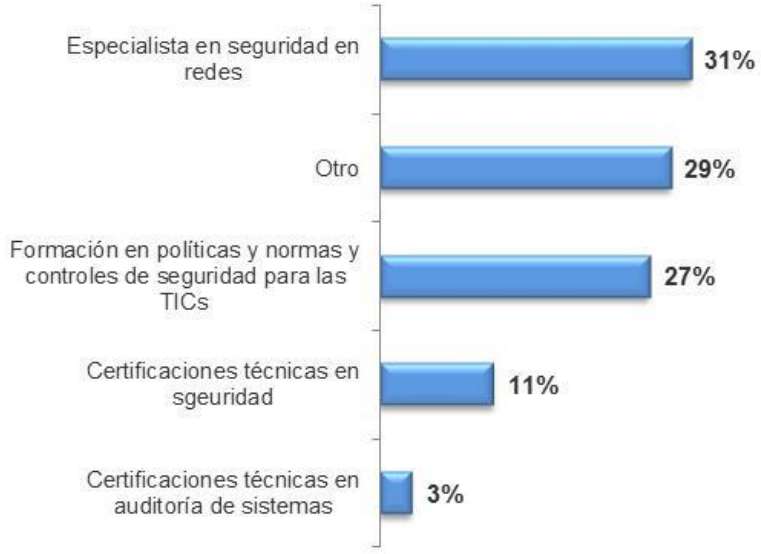
¿De las siguientes actividades relacionadas con seguridad de información, han sido o están siendo consideradas para darlas en outsourcing?



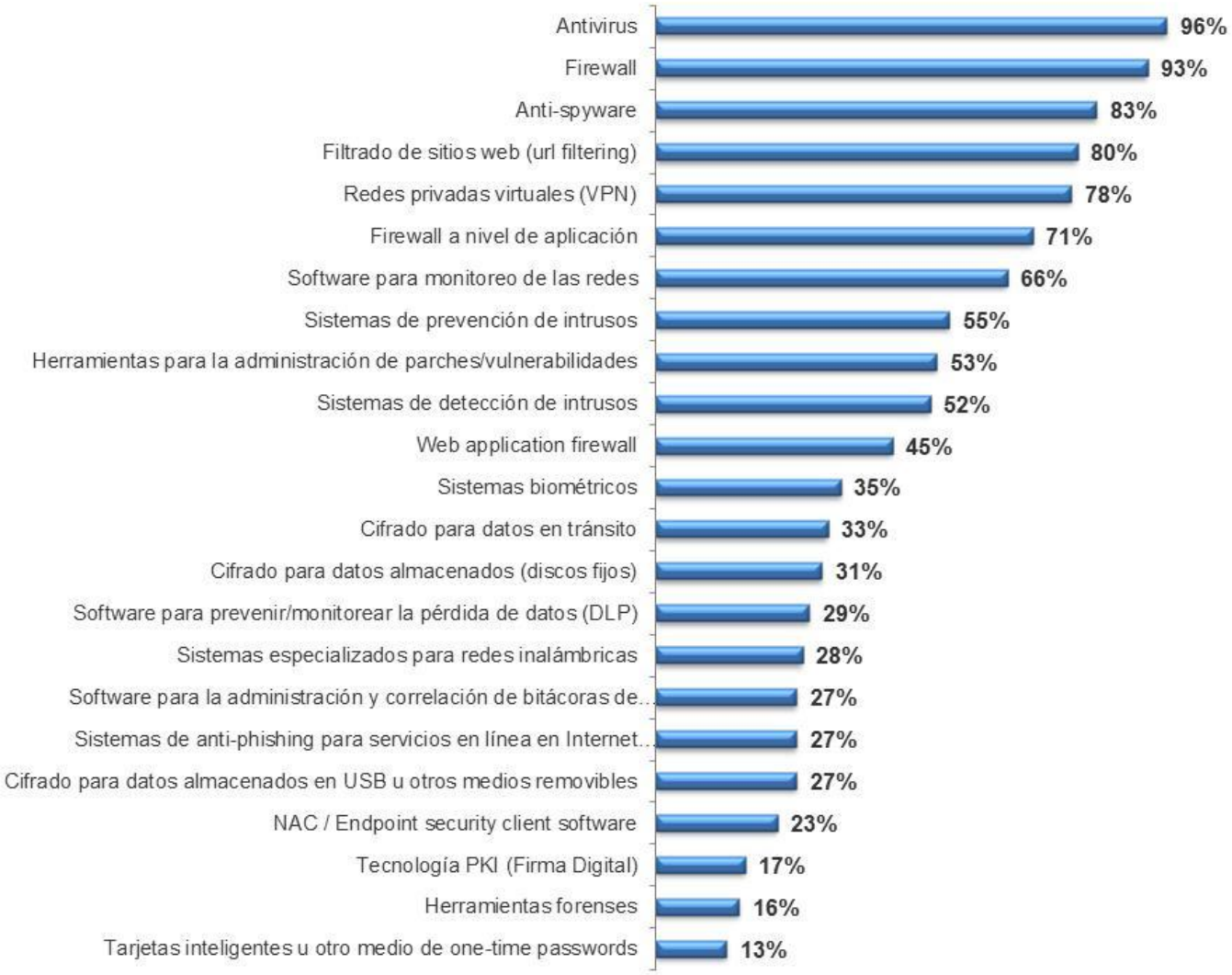
¿Dispone la organización de un plan de recuperación ante desastres que esté debidamente documentado y revisado con regularidad?



¿Cuál es el perfil solicitado por usted para contratar personal en el área de TIC?



¿Qué tipo de tecnologías de seguridad de información tiene implantado o está en el proceso de implantar?



Sobre RISCCO

RISCCO es una compañía panameña dedicada a la consultoría en riesgo tecnológico y auditoría interna, compuesta por profesionales con el conocimiento y credibilidad necesarios, para traducir aspectos muy técnicos a un leguaje simple y con sentido de negocio.

Con poco más de tres años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías e Instituciones del Estado Panameño, líderes en su ramo.

Los profesionales que dirigimos RISCCO contamos con muchos años de experiencia local e internacional, lo cual nos permite identificar problemas de manera rápida, pero sobre todo, recomendar soluciones prácticas y no teóricas. RISCCO se distingue de otras alternativas del mercado por:

- Tener la capacidad de responder con prontitud y rapidez a las necesidades de los clientes.
- Ofrecer servicios y soluciones sin mayores restricciones de independencia.
- Ofrecer recursos, competencias y conocimientos, como las grandes compañías de consultoría, sin las restricciones regulatorias o de mercado por conflicto de intereses.
- Brindar soluciones con calidad, pero con un nivel de inversión accesible.

Para conocer más sobre cómo estamos ayudando a organizaciones a encarar sus desafíos en materia de riesgo tecnológico y auditoría interna, llámenos al teléfono 279-1410 o visítenos en www.riscco.com

Contactos

RISCCO

Consultores en Riesgos y Auditoría Interna

Antonio Ayala I.
Vicepresidente Ejecutivo
RISCCO, S. de R. L.
+507 279-1410
aayala@riscco.com

Benildo Vergara
Gerente
RISCCO, S. de R. L.
+507 279-1410
bvergara@riscco.com

Félix Olivares C.
Gerente
RISCCO, S. de R. L.
+507 279-1410
folivares@riscco.com

Universidad Tecnológica de Panamá

Facultad de Ingeniería de Sistemas Computacionales

Nicolás Samaniego
Decano
+507 560-3616
nicolas.samaniego@utp.ac.pa

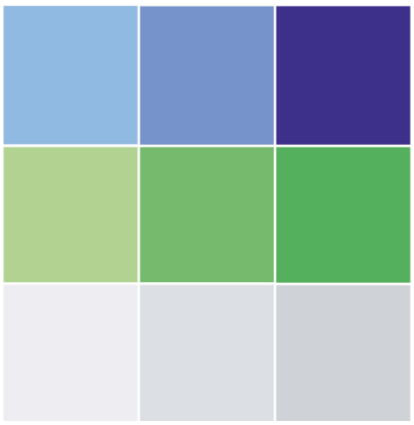
Independencia. Integridad. Conocimiento. Credibilidad.

RISCCO es una compañía independiente dedicada de manera exclusiva a la consultoría en riesgo, negocios y auditoría interna.

Para mayor información sobre el contenido de este estudio o conocer más sobre la forma cómo estamos ayudando a las organizaciones a enfrentar sus desafíos en materia de administración de riesgo, riesgos de tecnología o auditoría interna, por favor contáctenos.

info@riscco.com

Teléfono: +507 279-1410



www.riscco.com

© 2009 - 2012 RISCCO. Todos los derechos reservados. RISCCO y su logo son una marca registrada de RISCCO, S. de R. L. RISCCO no está registrada ni licenciada como una firma de contadores públicos y no emite opinión sobre estados financieros u ofrece servicios de atestación.

Los participantes del estudio fueron corporaciones e Instituciones del Estado establecidas en la República de Panamá. Los lectores del presente estudio deben tener presente que RISCCO, S. de R.L. no ha intentado validar la certeza de las respuestas proporcionadas. Además, los resultados podrían no necesariamente cubrir todos los aspectos relacionados con Seguridad de Información, que sean de interés para su organización.