RISCO®
Risk & Business Consulting.
Internal Audit.

Estudio sobre Seguridad de Información y Privacidad de Datos

Protegiéndose del riesgo interno

2da. edición
Julio 2011

Contenido

Introducción	3
Participantes del estudio	4
Resumen ejecutivo	6
Riesgos y amenazas	8
Gobernabilidad	13
Operaciones y tecnologías de seguridad	20
Privacidad y protección de datos	26
Sobre RISCCO	30
Contactos	31

Introducción

La necesidad que encaran las organizaciones hoy día para mantener el ritmo de crecimiento de los ingresos y reducir costos, ya sean, privadas o estatales, no puede afectarse por los riesgos tecnológicos a los que están diariamente expuestas.

Con el afán de proteger las redes y datos en un mundo digitalmente riesgoso, las organizaciones tienden, muchas veces, a establecer controles pensando que la amenaza severa provendrá principalmente, de un externo a la organización.

Los resultados de esta segunda edición del estudio, reflejan que, muy probablemente, las organizaciones no están valorando con suficiencia el riesgo interno al que están expuestas. De muy poco ayuda disponer de un equipo que proteja la seguridad perimetral de la red, si internamente, ante la falta de controles, alguien puede copiar en una memoria tipo USB datos confidenciales de clientes o de la propia organización, llevárselos sin autorización y sin que nadie lo advierta oportunamente.

La segunda edición del estudio fue realizada entre febrero y junio de 2011. Participaron 81 organizaciones privadas e Instituciones del Estado en Panamá. Los resultados son una invitación a reflexionar, si en la organización, a la seguridad de información, se le da la importancia que merece.

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.

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

Raúl A. Barahona Barrios
Decano
Facultad de Ingeniería de
Sistemas Computacionales, UTP

© 2009 -2011 RISCCO. Todos los derechos reservados.

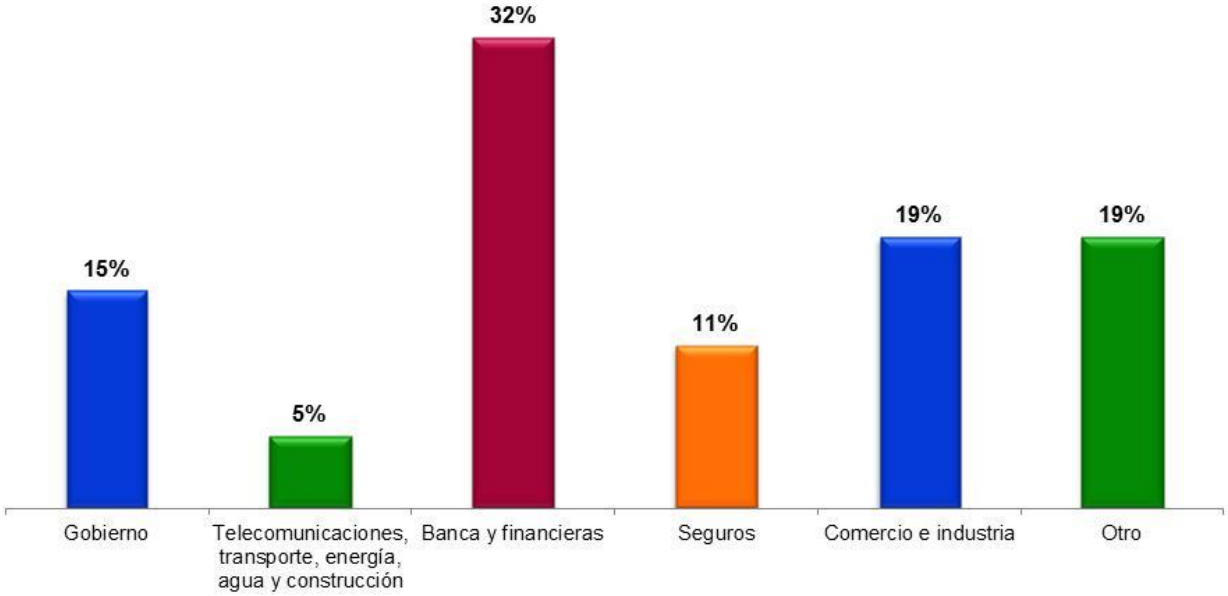
Participantes del estudio

Nos complace afirmar que para la segunda edición del estudio “Estado de la Seguridad de Información y Privacidad de Datos”, participaron 81 organizaciones privadas y estatales, todas con operaciones en Panamá.

Al igual que la primera edición, preservamos el anonimato de las organizaciones participantes, pero los datos demográficos muestran una participación muy balanceada por industria y tamaño.

81 organizaciones privadas y estatales participaron en la segunda edición del estudio. (*)

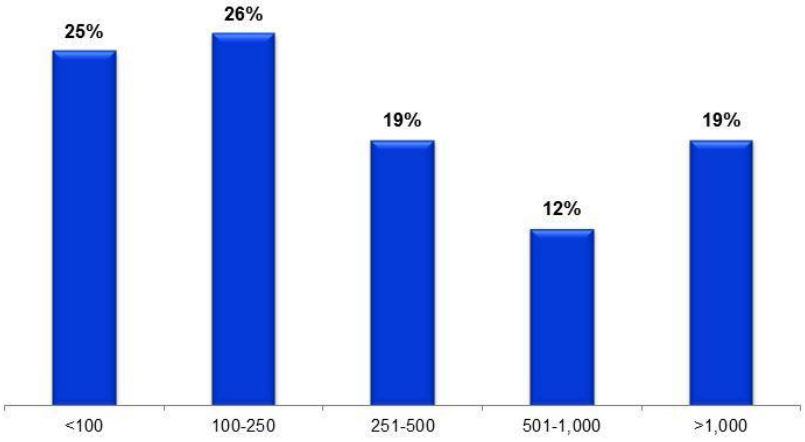
Sector económico al que pertenecen las organizaciones participantes



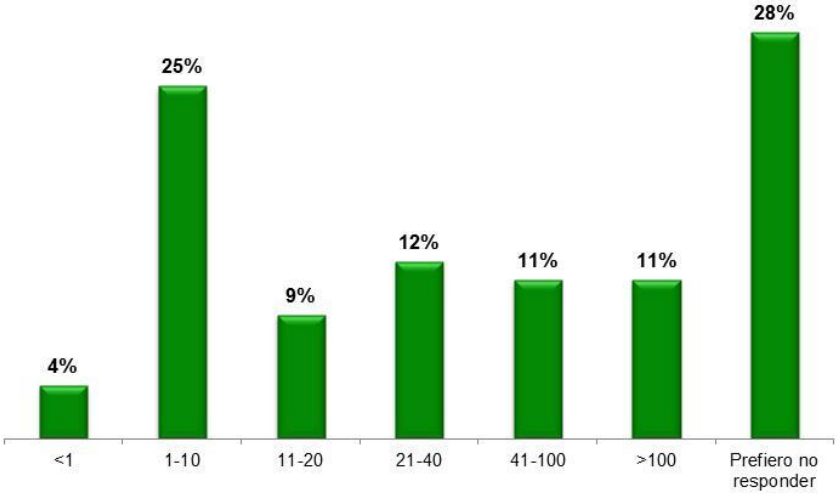
(*) En algunas de las gráficas, la suma de los porcentajes podría no sumar 100% debido al redondeo.

© 2009 -2011 RISCCO. Todos los derechos reservados.

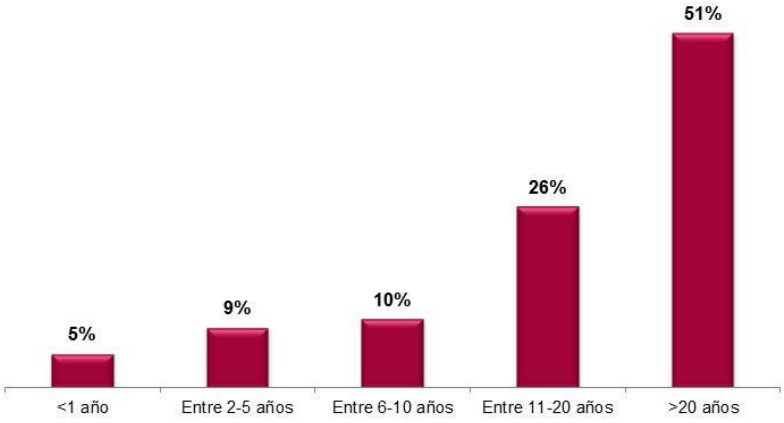
Número de colaboradores de las organizaciones participantes



Ingreso de las organizaciones participantes durante el año 2010 (en millones de Balboas)



Tiempo de operación de las organizaciones participantes



© 2009 -2011 RISCCO. Todos los derechos reservados.

Resumen ejecutivo

1. **Avances en mejorar la seguridad de información en las organizaciones no son evidentes, al comparar los resultados del estudio del 2011 con los del 2010.**

   La situación parece casi estática. Algunos esfuerzos aislados reflejan que los que dirigen algunas organizaciones, han comprendido y están actuando frente a la seriedad y criticidad de los riesgos tecnológicos. Sin embargo, al analizar los resultados en su conjunto, los avances positivos son mínimos y pareciera que a la seguridad de información ni se le da la relevancia que demanda y se continúa pensado que es un tema en el radar del Gerente de Tecnología y/o Gerente de Seguridad, en lugar de ser un punto en la agenda de las reuniones de Junta Directiva.

2. **En cuanto al responsable de los incidentes de seguridad, todo parece confirmar que el riesgo real, es interno.**

   Un 63% de los participantes indicó que el responsable de los incidentes de seguridad fue personal interno en la organización. Otro 21% confirmó que había sido una combinación de personal interno/externo a la organización. Dicho de otra forma, en el 84% de los incidentes, está involucrado el personal de casa. Para la edición del 2010, solo el 35% indicó que el responsable era personal interno.

   En adición al que comete o es el responsable del incidente de seguridad, somos de la opinión que el “otro” responsable interno es aquel que, pudiendo promover o trabajar en reforzar la seguridad, hace poco o nada. Véalo desde este punto de vista, si en su residencia un ladrón hurta artículos valiosos y luego, usted advierte que fue por su propia negligencia en dejar la ventana de la terraza abierta, al final, ¿Quién es el verdadero culpable?

© 2009 -2011 RISCCO. Todos los derechos reservados.

3. La estructura que debe dar soporte para mantener en un ambiente seguro y controlado las redes, sistemas y datos, permanece en la lista de tareas pendientes.

Un 80% de los participantes indicó no disponer de un Oficial de Seguridad de Información dedicado a tiempo completo. Adicionalmente, un 57% no tiene un modelo de seguridad debidamente documentado e implantado. Por último, un 69% no dispone de un mapa de riesgo que muestre el impacto y probabilidad de los riesgos tecnológicos que podrían afectar a la organización.

Lo anterior es consistente con que solo el 19% de los participantes considera que los controles de seguridad de información implantados y en vigencia, son suficientes para identificar y/o reducir oportunamente los riesgos tecnológicos a los que está expuesta la organización.

4. La privacidad y protección de datos es la prioridad para el 2011.

Un 69% de los participantes confirmó que implantar o mejorar las tecnologías y procesos sobre la privacidad y protección de datos es la prioridad número uno para 2011, en materia de seguridad de información. En los resultados del 2010, esto era la tercera prioridad con un 62%. El ánimo de mejorar en esta área es positivo y necesario, cuando se analizan los siguientes resultados:

- 62% no cuenta con una estrategia para la protección y privacidad de los datos.
- 72% no utiliza ninguna herramienta de software adicional (al sistema operativo y base de datos) para prevenir la pérdida de los datos.
- 80% no dispone de controles efectivos y suficientes para evitar y/o identificar la fuga de datos personales de los clientes.

5. La probabilidad de que datos sensitivos puedan perderse, continúa siendo alta.

Esto se basa en los siguientes resultados:

- No se utiliza cifrado (encriptación) de datos en los siguientes escenarios:
  - En un 77%, en dispositivos USB
  - En un 62%, en tránsito.
  - En un 74%, en los discos fijos de los computadores.
- 71% no dispone de software para prevenir/monitorear la pérdida de datos.

6. Tecnologías de seguridad para enfrentar las nuevas amenazas no están siendo ampliamente utilizadas.

Similar al 2010, los resultados del 2011 indican que los participantes continúan utilizando tecnologías de seguridad tradicionales para protegerse, lo cual es positivo, pero la realidad ha demostrado que ya no son suficientes. Las tres principales tecnologías de seguridad implantadas o en proceso de implantación en 2011 son: antivirus (87%); Firewall (86%); anti-spyware (83%). Sin embargo, con relación al uso de tecnologías más recientes, existe un rezago, ya que:

- El cifrado de datos no es ampliamente utilizado.
- 89% no utiliza técnicas de autenticación fuerte como "one time password", generalmente necesaria en el sector financiero.
- 89% no dispone de tecnología para firmas digitales.
- 74% no utiliza herramientas para la administración y correlación de bitácoras.
- 71% no utiliza software para prevenir/monitorear la perdida de datos.

© 2009 -2011 RISCCO. Todos los derechos reservados.

Riesgos y amenazas

Los cinco incidentes de seguridad que más frecuentemente experimentaron los participantes del estudio en los últimos doce meses fueron:

1. Virus o malware (70%).
2. Accesos no autorizados a recursos de tecnología (30%).
3. Robo de notebook (28%).
4. Robo de contraseñas (19%).
5. Ataques o modificación a la página web (17%).

Cabe resaltar que el incidente No. 4 y No. 5 en los resultados del 2010, aparecían en la última y antepenúltima posición.

Este incremento no puede verse de manera aislada, y en nuestro criterio no es más que el reflejo de que personas o grupo de personas, han advertido que la ausencia de controles de seguridad efectivos en algunas organizaciones, les está haciendo la tarea fácil para acceder datos confidenciales de la organización.

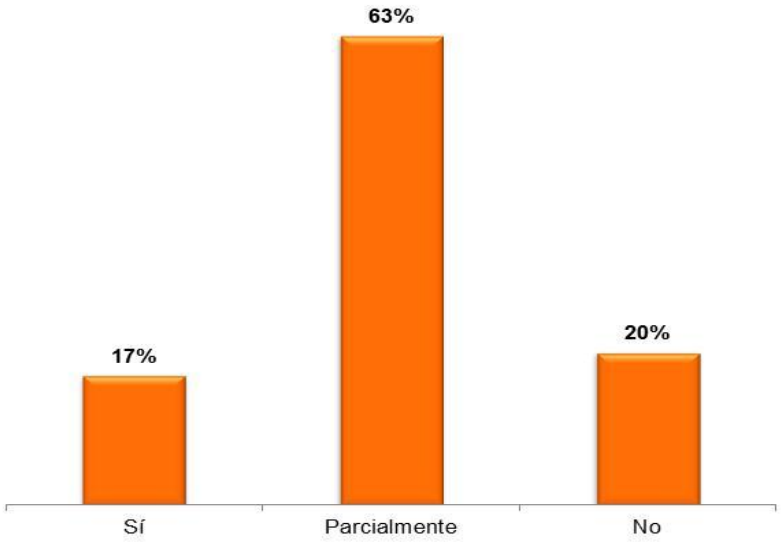
Al preguntar quién era el responsable de los incidentes de seguridad, a diferencia del 2010, para 2011, el personal interno es el principal causante. Los participantes indicaron como responsables a:

- Personal Interno. 63% (2011), 35% (2010).
- Combinación de personal interno y externo. 21% (2011), 27% (2010).
- Personal externo. 16% (2011), 31% (2010).

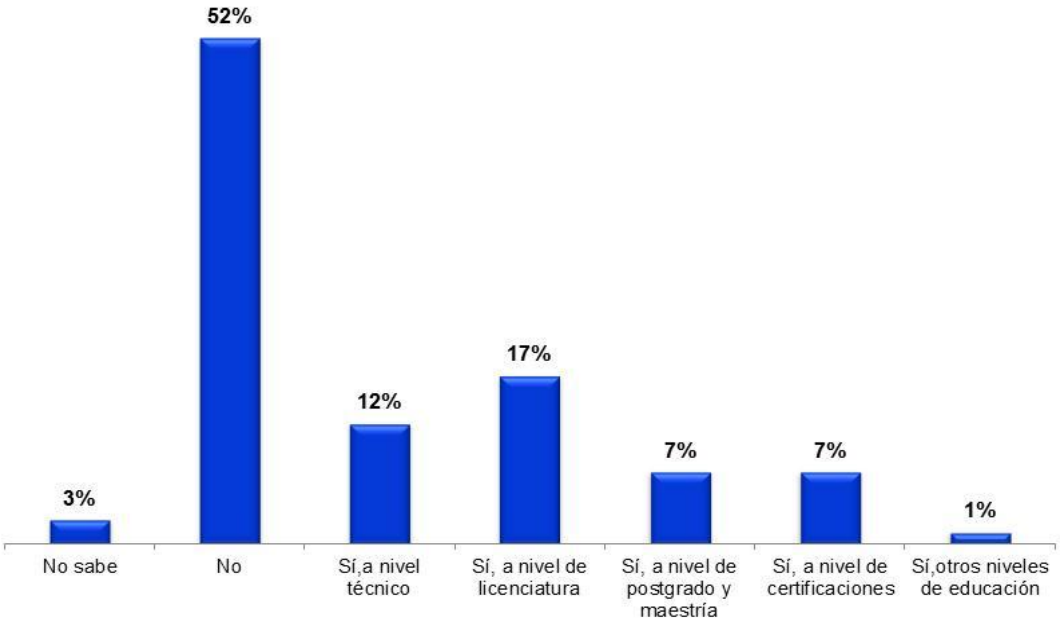
Nuestra lectura de estos resultados es que pareciera que la falta de controles efectivos y suficientes en materia de seguridad informática, está facilitándoles la tarea a algunas personas. La ecuación es simple. ¿A quién considera usted que le sería más fácil sacarle provecho a este hecho? A alguien interno o externo de la organización.

© 2009 -2011 RISCCO. Todos los derechos reservados.

¿La organización cuenta con los conocimientos y herramientas necesarias para hacer las investigaciones forenses si ocurre un incidente de seguridad?

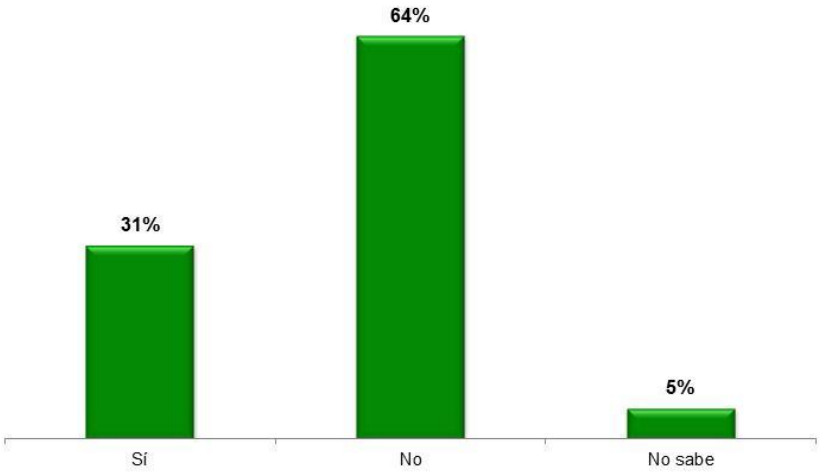


¿La organización cuenta con personal en el Área de Informática Forense y cuál es su nivel educativo?

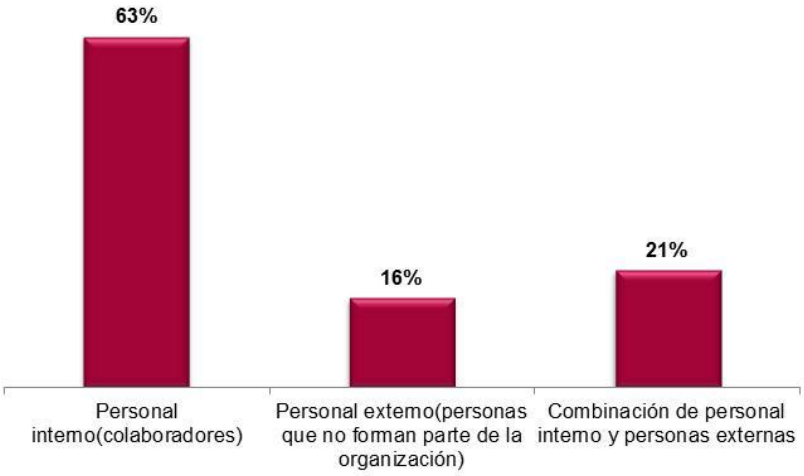


© 2009 -2011 RISCCO. Todos los derechos reservados.

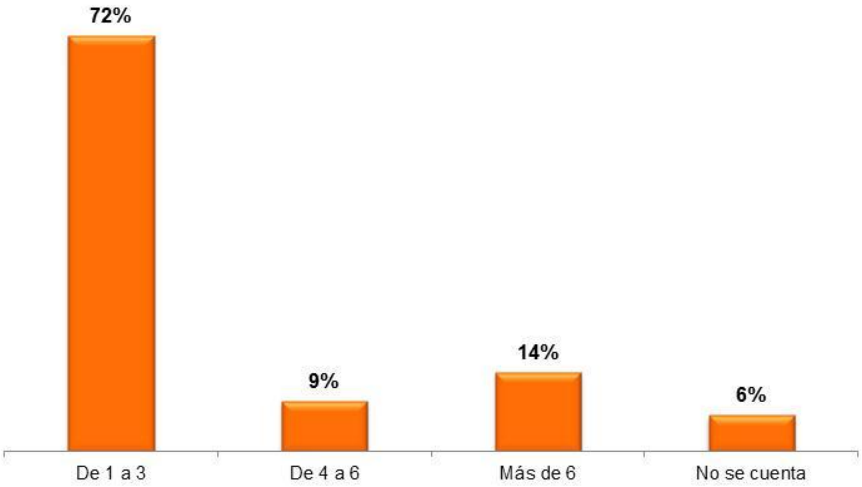
Experimentó incidentes de seguridad de información en los últimos doce meses



Responsable de los incidentes de seguridad de información

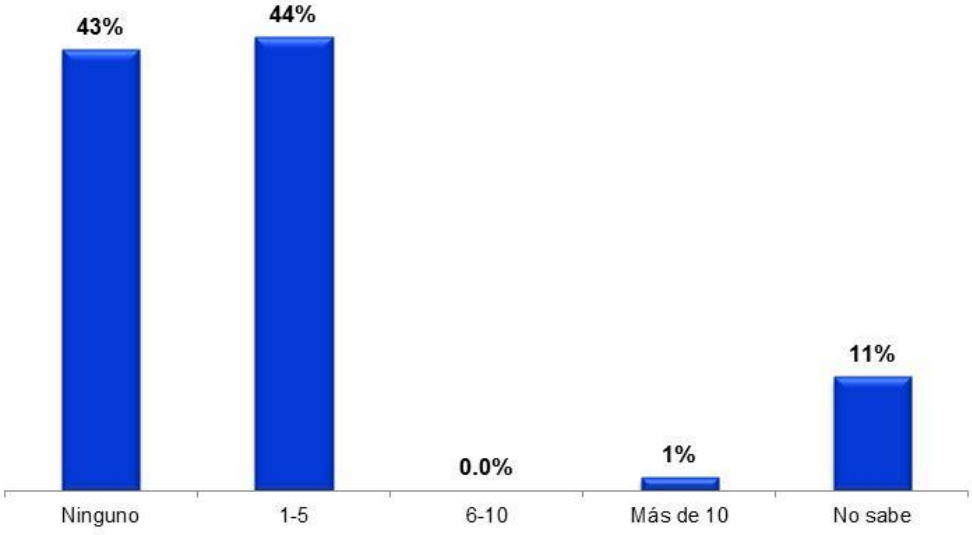


Cantidad de personal con el que cuenta para atender los riesgos y amenazas tecnológicos



© 2009 -2011 RISCCO. Todos los derechos reservados.

Número de incidentes de seguridad de información ocurridos en los últimos doce meses



Tipos de incidentes de seguridad de información ocurridos en los últimos doce meses

© 2009 -2011 RISCCO. Todos los derechos reservados.

Acción que se toma una vez identificado un incidente de seguridad de información

© 2009 -2011 RISCCO. Todos los derechos reservados.

Gobernabilidad

A pesar de que el 76% de los participantes indicó que para la Alta Gerencia los temas de seguridad de información son importantes o muy importantes, los resultados apuntan a que pareciera que existe una contradicción porque:

- 80% no cuenta con un Oficial de Seguridad de Información a tiempo completo.
- 57% no tiene un modelo de seguridad debidamente documentado e implantado.
- 74% no cuenta, en ejecución plena, de un programa permanente para la concienciación hacia la seguridad de usuarios finales.
- 69% no dispone de un mapa de riesgo que muestre el impacto y probabilidad de los riesgos tecnológicos que podrían afectar a la organización.

En cuanto a los desafíos en materia de seguridad de información experimentados en 2010 y que se esperan experimentar en 2011, prácticamente son los mismos:

- Falta de concienciación de los usuarios finales (68% y 54%).
- Disponibilidad de recursos (49% y 44%).
- Falta de un Oficial de Seguridad (49% y 35%).
- Presupuesto muy limitado (38% y 35%)

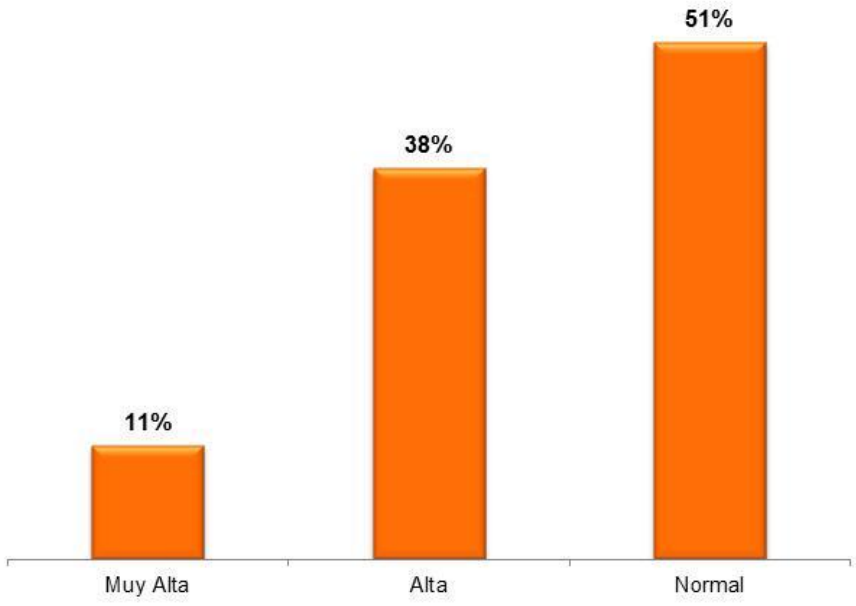
Con relación a las tres principales prioridades sobre seguridad de información que para 2011 tendrán las organizaciones, éstas son:

- 69%, implantar o mejorar las tecnologías y procesos sobre la privacidad y protección de datos.
- 61%, mejorar los programas de concienciación hacia la seguridad, en la organización.
- 58%, llevar a cabo pruebas de vulnerabilidad a las redes internas/externas.

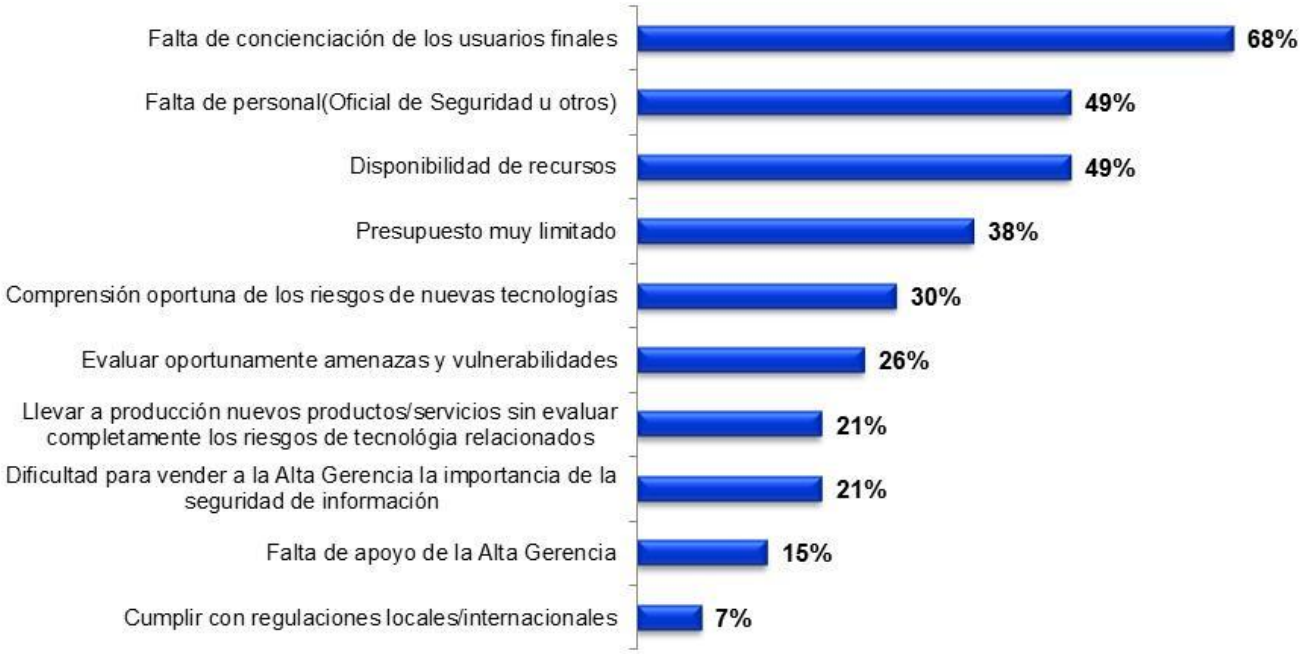
Cuando hablamos de gobierno de seguridad de información, la implantación de un marco normativo o modelo de seguridad es fundamental. Para 2011, implantar un marco normativo no está entre las prioridades, ya que se encuentra en la antepenúltima posición, algo casi idéntico a los resultados del 2010.

© 2009 -2011 RISCCO. Todos los derechos reservados.

Nivel de complejidad de las redes, sistemas, aplicaciones e infraestructura tecnológica en su organización



Principales desafíos relacionados con la seguridad de información, experimentados en el año 2010



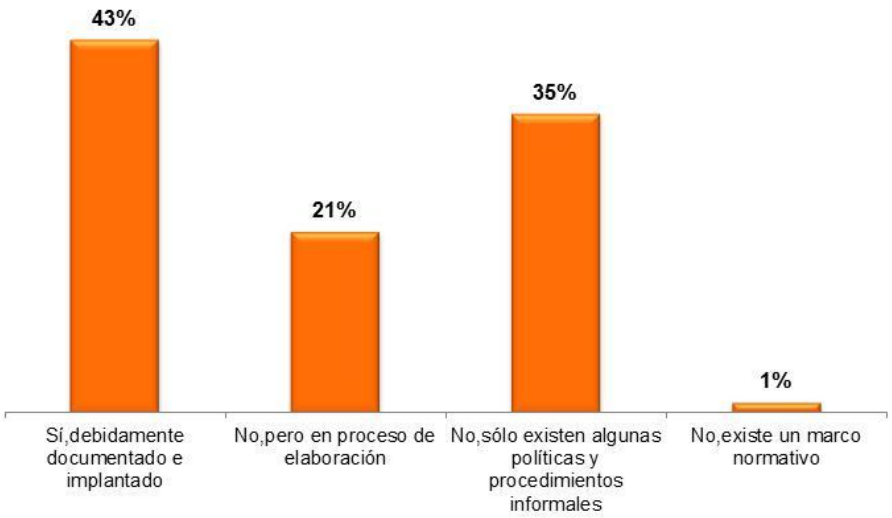
© 2009 -2011 RISCCO. Todos los derechos reservados.

Principales prioridades en el 2011 en cuanto a seguridad informática en su organización

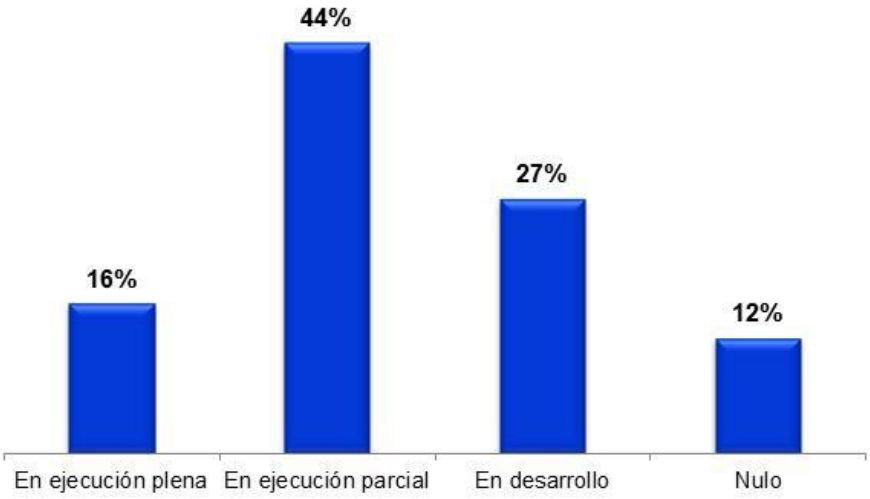
Principales desafíos en el 2011 para mejorar la seguridad de la información en las organizaciones

© 2009 -2011 RISCCO. Todos los derechos reservados.

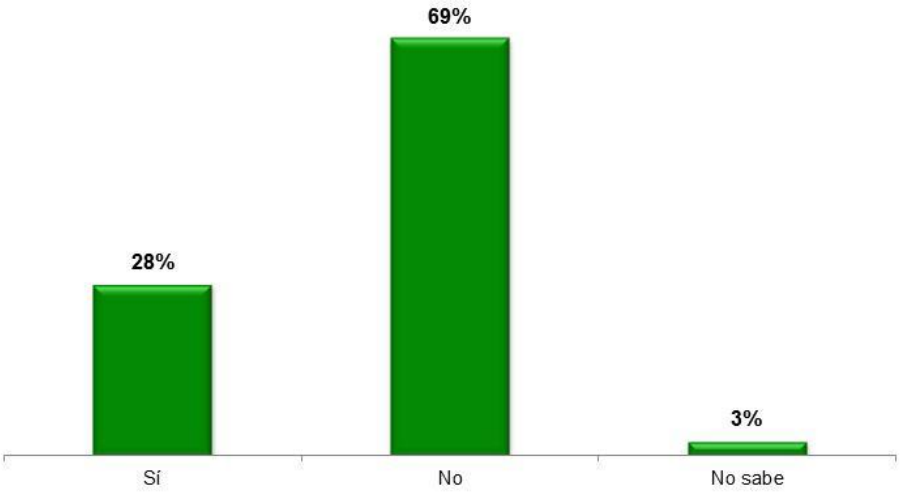
Existe un marco normativo (políticas, procesos y procedimientos) para administrar la seguridad de información



Existe un programa permanente y formal de concienciación hacia la seguridad de información para los usuarios

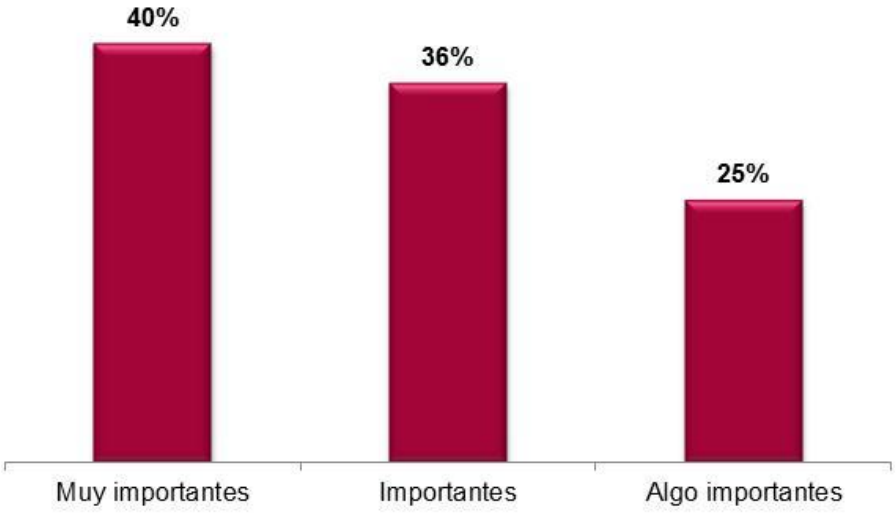


Cuenta la organización con un mapa de riesgos que muestre el impacto y la probabilidad de los riesgos tecnológicos

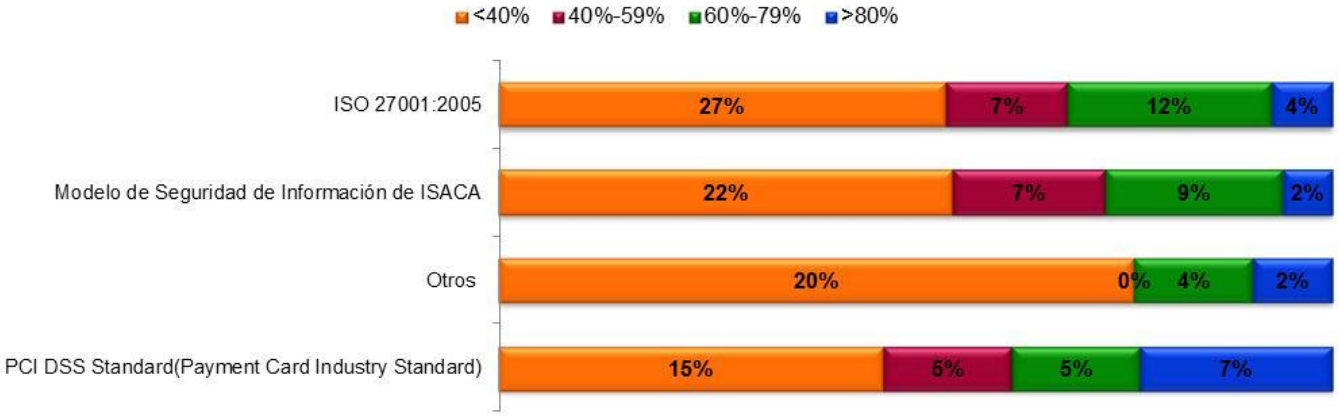


© 2009 -2011 RISCCO. Todos los derechos reservados.

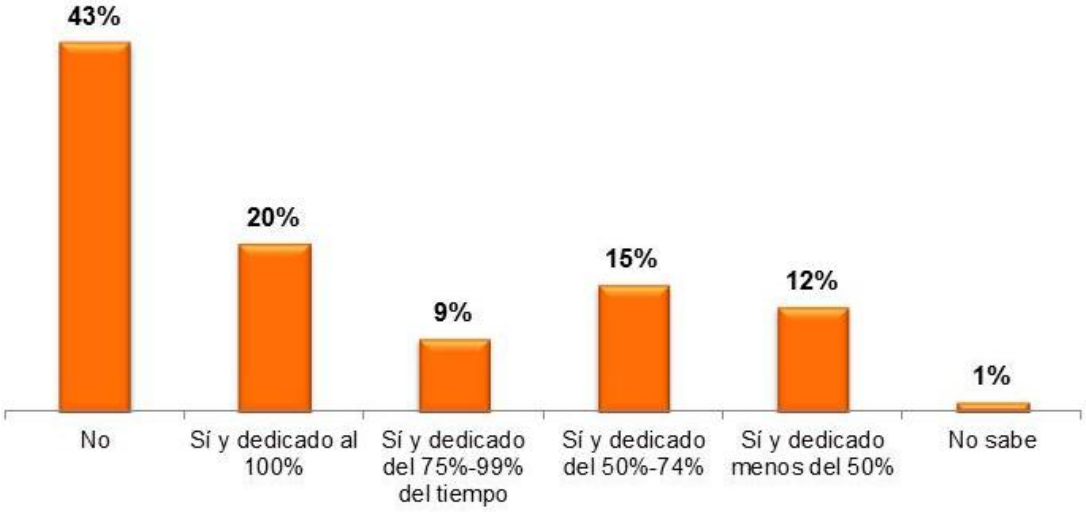
Cómo considera la Alta Gerencia los temas de seguridad de Información



Porcentaje de adopción de estándares internacionales de seguridad de información implantados en la organización

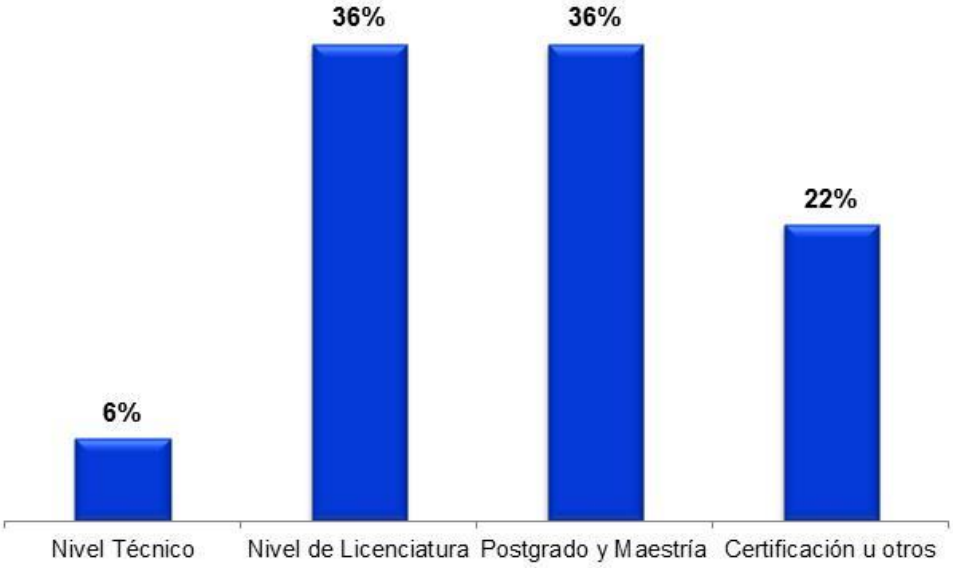


Cuenta la organización con un Oficial de Seguridad



© 2009 -2011 RISCCO. Todos los derechos reservados.

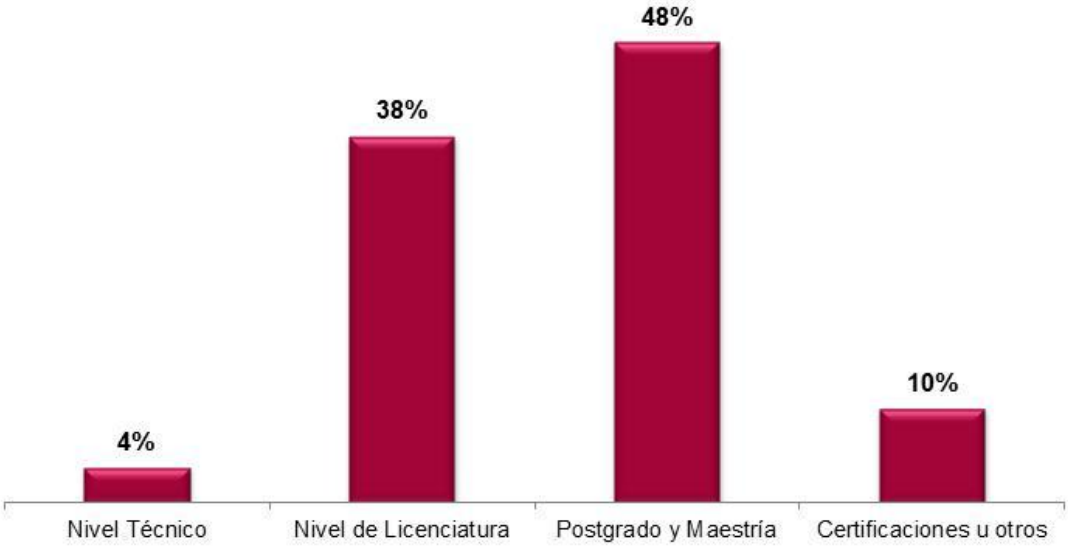
La formación académica del Oficial de Seguridad



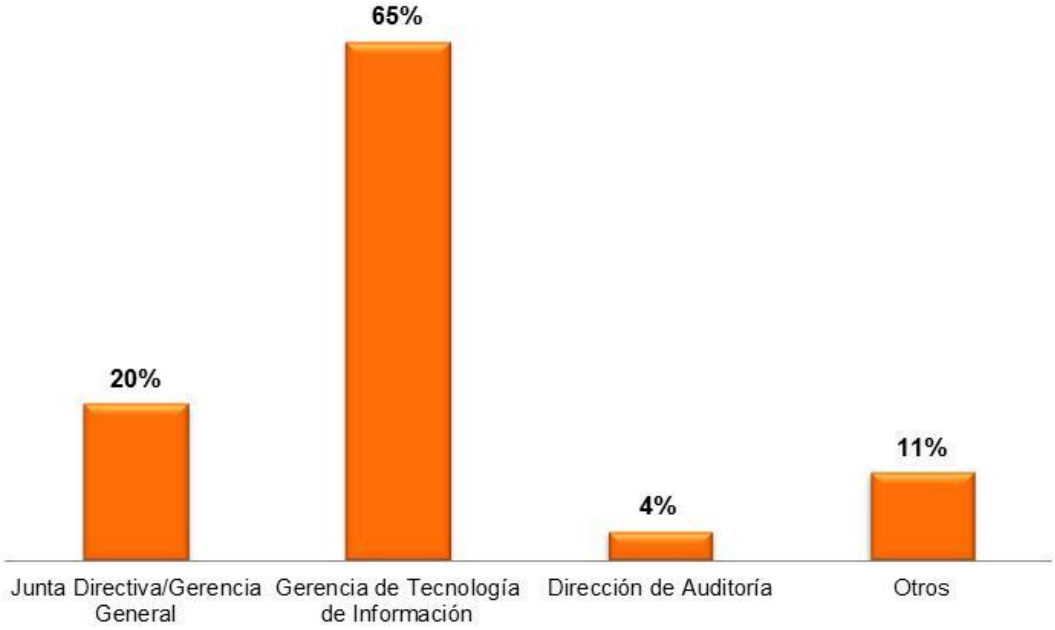
Las áreas que son responsabilidad del Oficial de Seguridad

© 2009 -2011 RISCCO. Todos los derechos reservados.

La formación académica del Auditor de Sistemas



A quién reporta el Oficial de Seguridad



© 2009 -2011 RISCCO. Todos los derechos reservados.

Operaciones y tecnologías de seguridad

Muy positivo, al igual que la edición 2010 del estudio, los presupuestos para temas de seguridad en el Departamento de Tecnología parecieran no ser el problema, ya que, para 2011:

- 89% afirmó que el presupuesto se incrementará o mantendrá al compararlo con el año 2010.
- 68% indicó que el presupuesto de seguridad, como porcentaje del presupuesto total del Departamento de Tecnología, es igual o mayor al 3%. En 2010, este valor era 52%.

A pesar de que el dinero para invertir en tecnologías de seguridad no es el problema, los resultados indican, al igual que en 2010, que las inversiones se hacen a tecnologías tradicionales de seguridad, ya que, para 2011:

- Las tres principales tecnologías de seguridad implantadas o en proceso de implantación son: antivirus (87%); Firewall (86%); anti-spyware (83%).

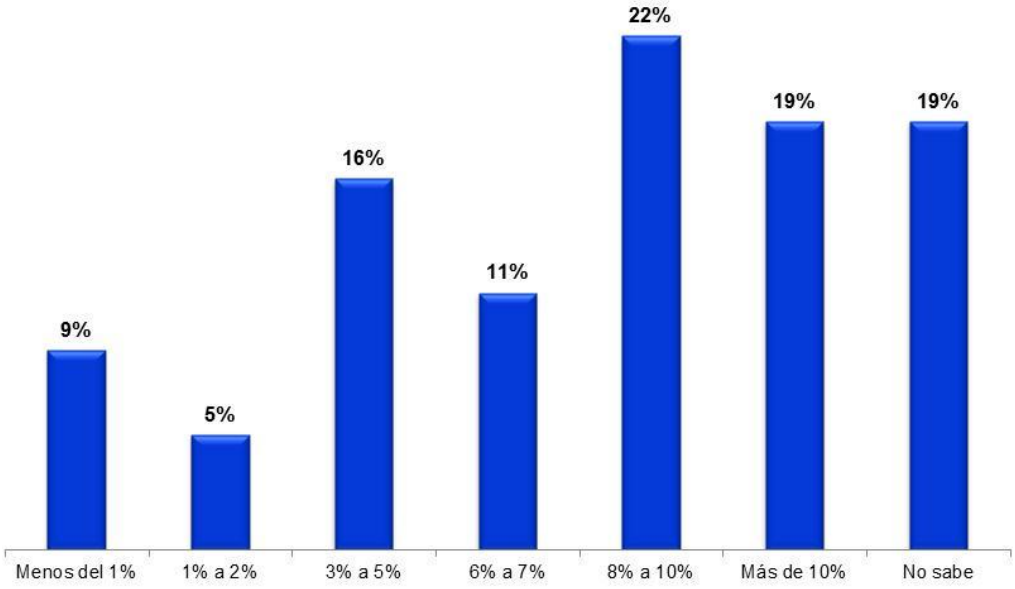
Con relación a otras tecnologías de seguridad, de importancia, el nivel de implantación para 2011 entre los participantes parece baja, ya que:

- 77% no utiliza encriptación para datos en dispositivos USB y 62% para datos en tránsito.
- 74% no encripta los datos de los discos fijos de los computadores.
- 71% no dispone de software para prevenir/monitorear la perdida de datos.
- 89% no utiliza técnicas de autenticación fuerte como “one time password”, generalmente utilizada en el sector financiero.

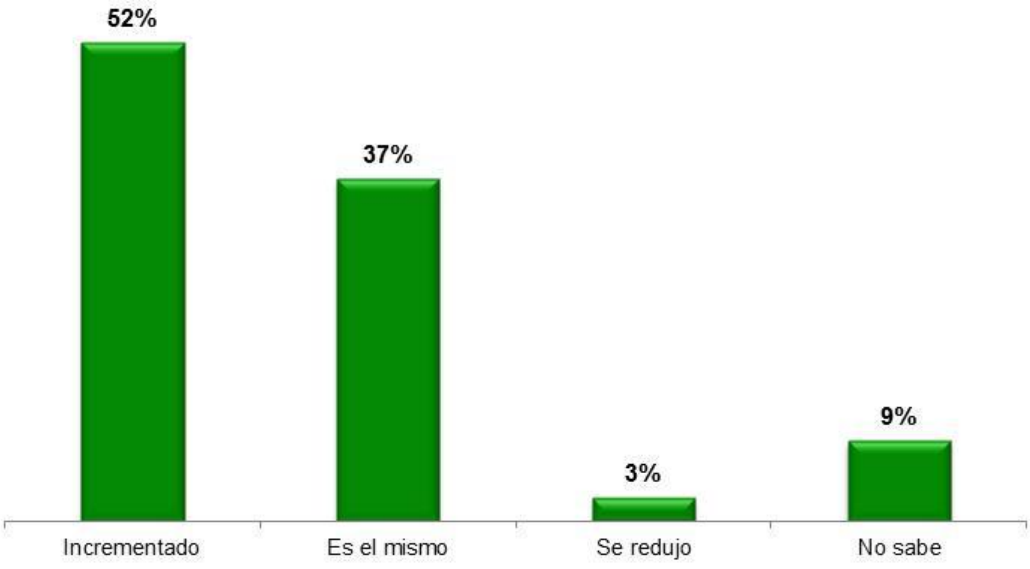
Un elemento final en esta sección, es que, casi igual que los resultados del 2010, solo un 19% de los participantes considera que los controles implantados son suficientes para identificar y/o reducir oportunamente los riesgos tecnológicos a los que está expuesta la organización.

© 2009 -2011 RISCCO. Todos los derechos reservados.

Porcentaje del presupuesto de tecnología asignado a la seguridad de información



Presupuesto de seguridad de información del 2011 con relación al presupuesto del 2010

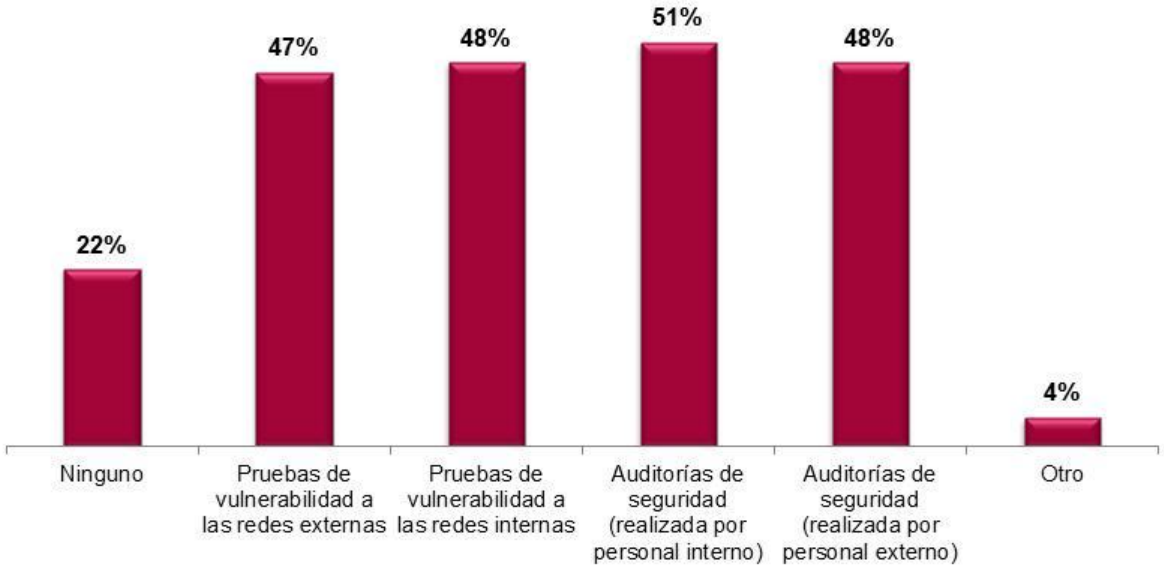


© 2009 -2011 RISCCO. Todos los derechos reservados.

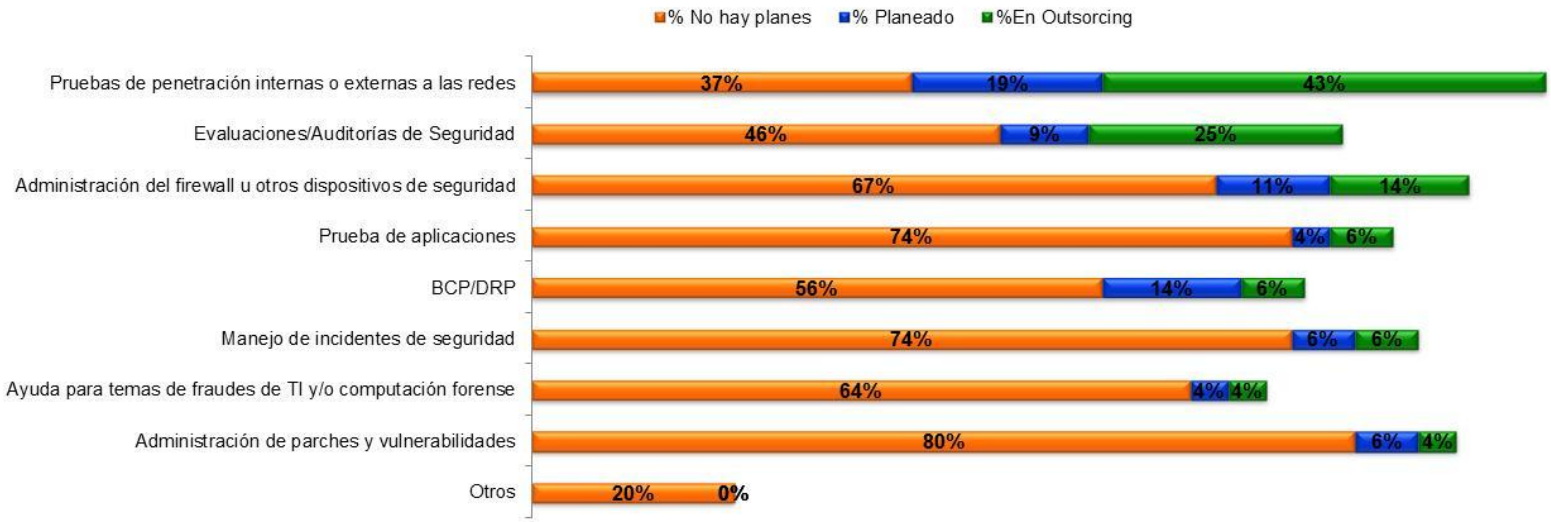
Tipos de tecnologías de seguridad de información implantadas o en proceso de implantación

© 2009 -2011 RISCCO. Todos los derechos reservados.

Mecanismo utilizado para evaluar la efectividad de la seguridad de la información

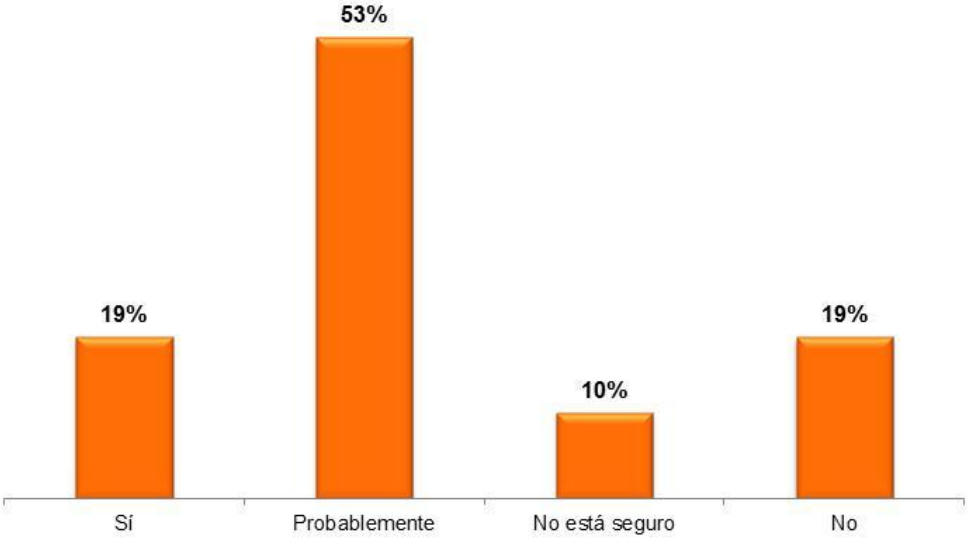


¿Qué actividades de seguridad de información han sido dadas o se tiene planeado o no hay planes de darlas en outsourcing?

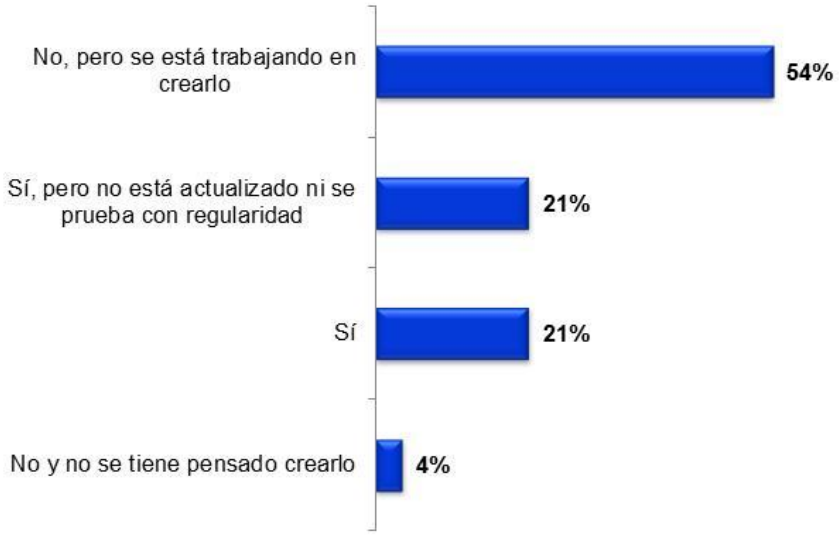


© 2009 -2011 RISCCO. Todos los derechos reservados.

Considera que los controles de seguridad de información implantados en la organización son suficientes para identificar y/o reducir oportunamente los riesgos de tecnología

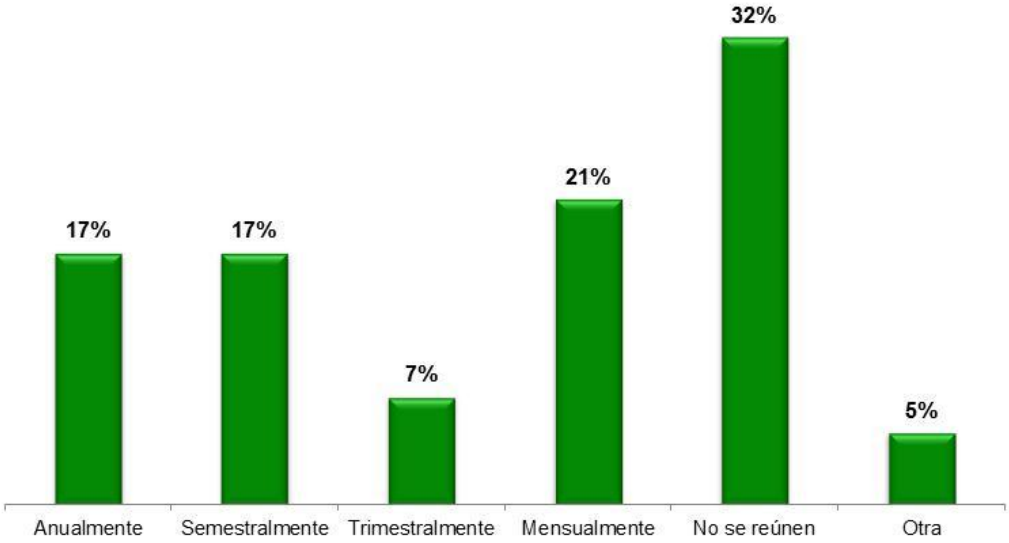


Dispone su organización de un plan de recuperación ante desastres debidamente documentado y probado con regularidad

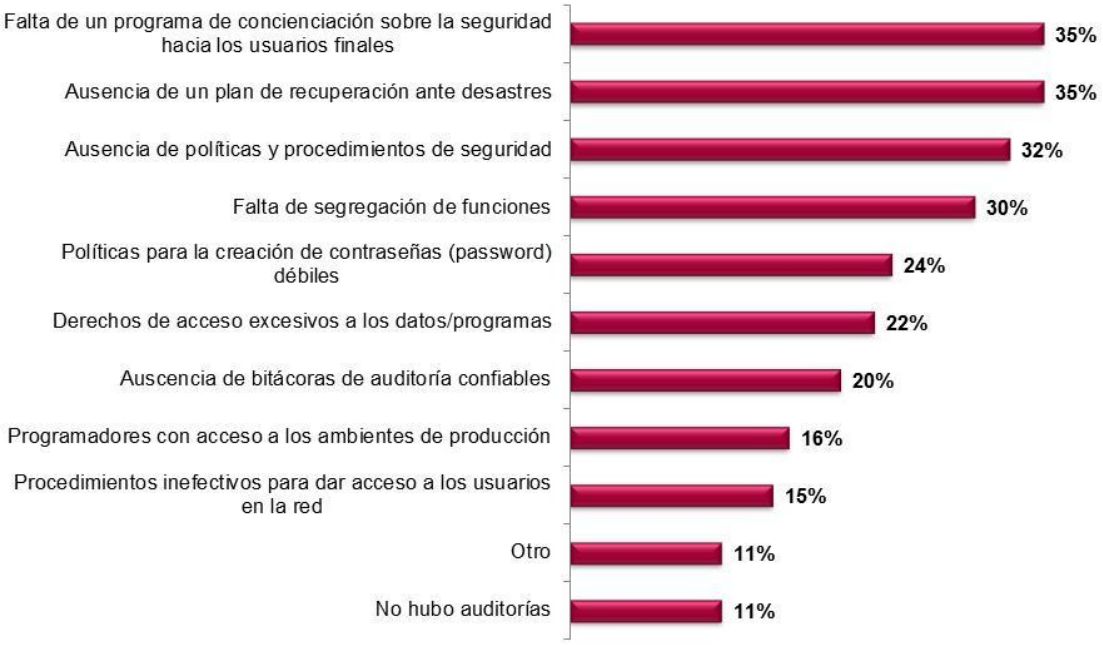


© 2009 -2011 RISCCO. Todos los derechos reservados.

Frecuencia con que se reúnen la Alta Gerencia, Comité de Seguridad o el Departamento de Riesgo o Tecnología para tratar temas de seguridad de información



Principales hallazgos plasmados en las auditorías internas/externas de seguridad durante el 2010



© 2009 -2011 RISCCO. Todos los derechos reservados.

Privacidad y protección de datos

Si existe un elemento que, globalmente, cada día toma mayor relevancia en materia de seguridad de información es la privacidad y protección de datos. Hace mucho tiempo los datos dejaron las fronteras de las redes de la organización y están desde, el teléfono inteligente hasta las convenientes memorias tipo USB. Internacionalmente y localmente las regulaciones que exigen a las compañías establecer controles para proteger los datos personales de los clientes, aumenta.

Al igual que otras secciones del presente estudio, al comparar los resultados de las ediciones 2010 y 2011, se refleja que no hay variaciones favorables de importancia en cuanto a la privacidad y protección de datos. Si bien es cierto que el 89% afirmó no haber sufrido ningún incidente relacionado con la pérdida de datos, los siguientes resultados podrían hacer pensar que al tema no se le está dando la relevancia que merece:

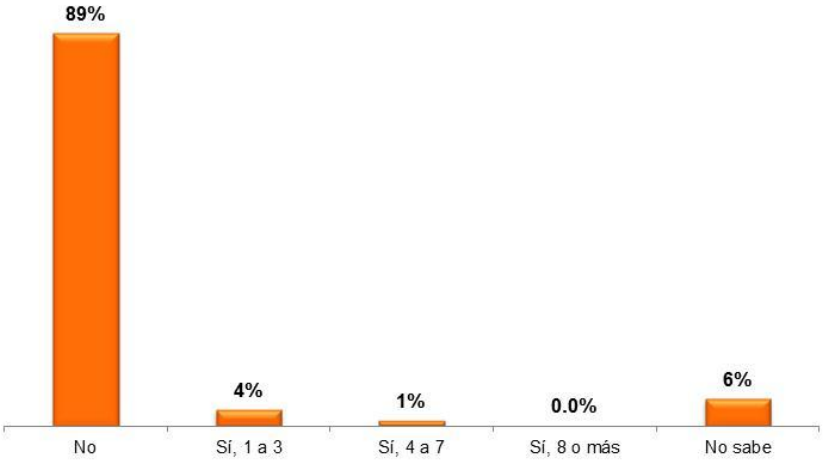
- 62% no cuenta con una estrategia para la protección y privacidad de los datos.
- 72% no utiliza ninguna herramienta de software adicional (al sistema operativo y base de datos) para prevenir la perdida de los datos.
- 83% no cuenta con un proceso para la clasificación de los datos que defina controles para protegerlos.
- 80% no dispone de controles efectivos y suficientes para evitar y/o identificar la fuga de datos personales de los clientes.

El 66% de los participantes indicó que el responsable en definir la estrategia para la protección y privacidad de datos es el Gerente de Tecnología y Gerente de Seguridad. Si bien es cierto que el Departamento de Tecnología juega un rol clave en establecer los controles para proteger los datos, los temas sobre privacidad y protección de datos deben recaer sobre las áreas de riesgo y/o cumplimiento en las organizaciones.

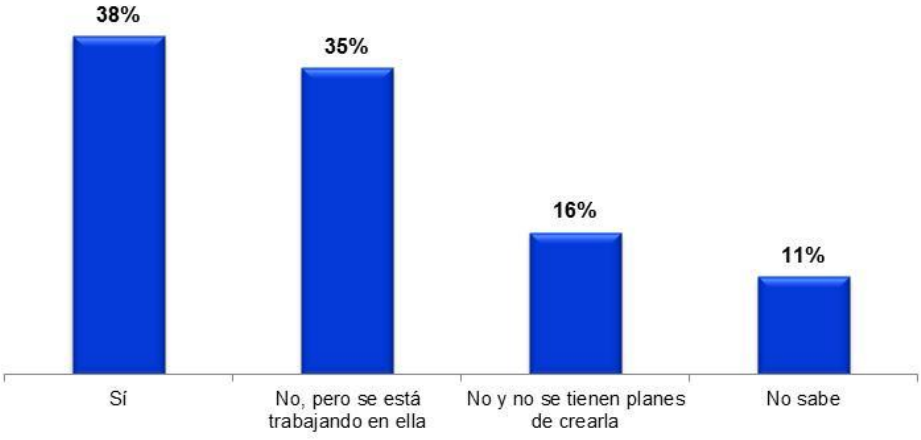
Un 42% indicó que el estándar PCI DSS (Payment Card Industry Data Security Standard) no aplica en su organización. Esto resulta interesante, pues el estándar aplica a cualquier organización que procese, transmita o almacene datos sobre tarjetas de crédito. Pensamos que muchas organizaciones en Panamá tienen que cumplir con PCI DSS. Probablemente muchas desconozcan del alcance de la norma.

© 2009 -2011 RISCCO. Todos los derechos reservados.

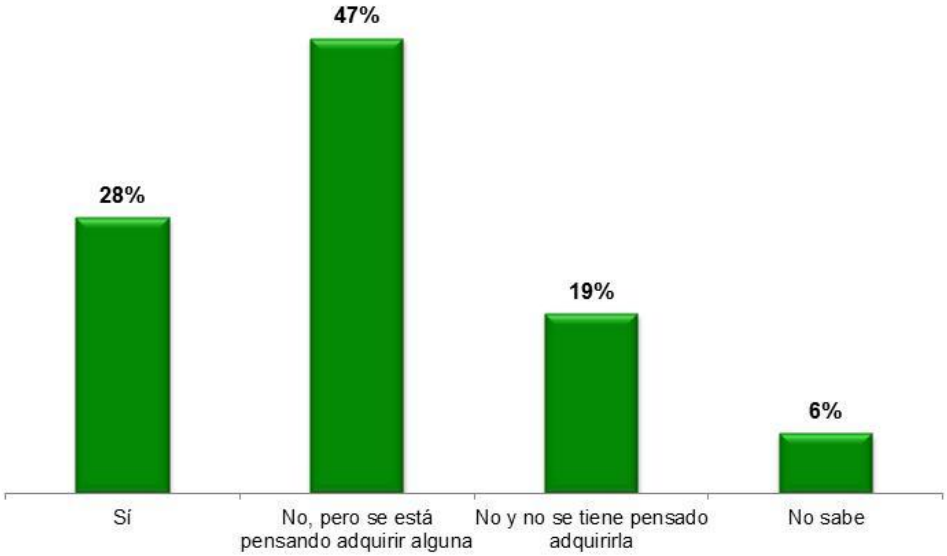
Ha ocurrido algún incidente relacionado con la pérdida o robo de datos personales de sus clientes.



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

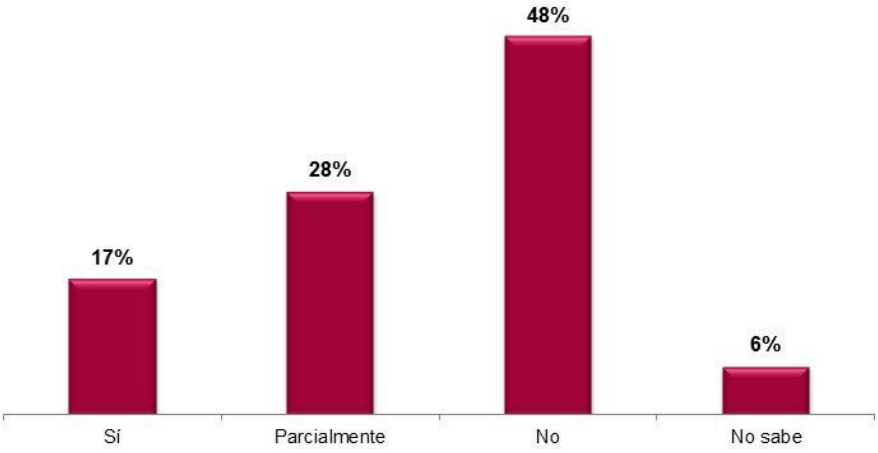


Utiliza alguna herramienta de software para prevenir la pérdida de los datos adicional a las opciones de seguridad de los sistemas operativos y bases de datos

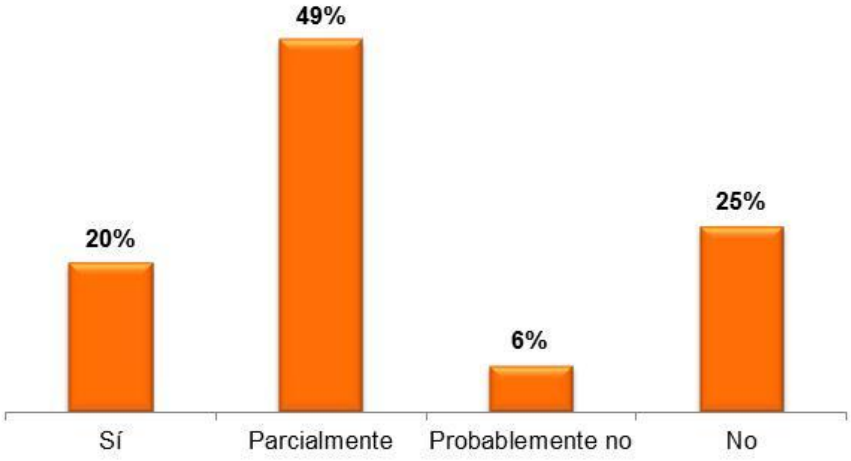


© 2009 -2011 RISCCO. Todos los derechos reservados.

Existe un proceso para la clasificación de datos que defina controles para proteger los datos personales de los clientes



Existen controles efectivos y suficientes para evitar y/o identificar la fuga de datos personales de los clientes por medios removibles y correo electrónico



Quién es el responsable de definir la estrategia para la privacidad y protección de los datos de los clientes

© 2009 -2011 RISCCO. Todos los derechos reservados.

Conoce si su organización debe cumplir con el estándar PCI DSS (Payment Card Industry Data Security Standard)

© 2009 -2011 RISCCO. Todos los derechos reservados.

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 necesaria para traducir aspectos muy técnicos a un leguaje simple y con sentido de negocio.

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

Los profesionales que dirigen RISCCO cuentan 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

© 2009 -2011 RISCCO. Todos los derechos reservados.

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

Raúl A. Barahona Barrios
Decano
raul.barahona@utp.ac.pa

© 2009 -2011 RISCCO. Todos los derechos reservados.

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 - 2011 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 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.