Estudio sobre el estado de la Seguridad de Información y Privacidad de Datos en Panamá

1ª. edición

Junio 2010

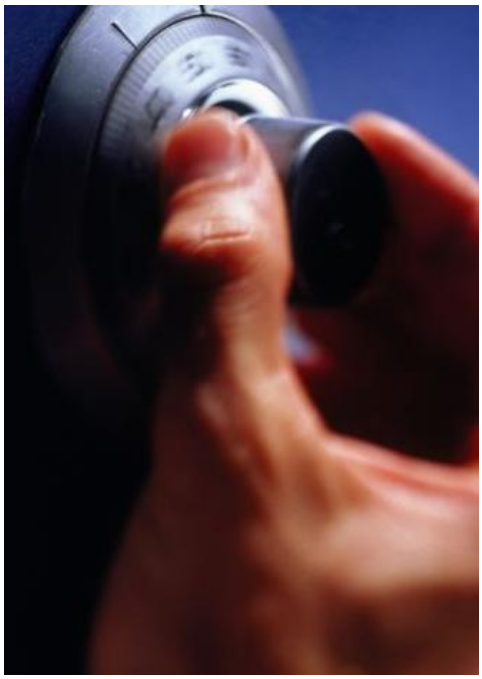
© 2009- 2010 RISCCO

Contenido

Introducción	3
Participantes del estudio	4
Resumen ejecutivo	6
Riesgos y amenazas	8
Gobernabilidad	13
Operación y tecnología de seguridad	20
Privacidad y protección de datos	27
Contactos	29

© 2009- 2010 RISCCO

Introducción



En un momento cuando las organizaciones buscan obtener ventajas competitivas del uso de las redes sociales, computación en la nube (cloud computing) y la virtualización, muchos líderes de tecnología apuestan a estas iniciativas con esperanza. Estar más cerca de los clientes, simplificar las infraestructuras físicas de tecnología y reducir costos, es parte de la apuesta. Si bien es cierto, se reconocen algunas de las implicaciones de seguridad, muchos, sólo ven la punta del "iceberg" de los reales riesgos tecnológicos que su implantación conlleva.

Con esta idea en mente, la Facultad de Ingeniería de Sistemas Computacionales de la Universidad Tecnológica de Panamá y RISCCO, decidieron realizar la primera edición del estudio: *"Estado de la Seguridad de Información y Privacidad de Datos en Panamá".*

El objetivo del estudio fue conocer los desafíos y tendencias que enfrentan los Departamentos de Tecnología en materia de seguridad de información y privacidad de datos.

El estudio fue realizado entre febrero y mayo de 2010. Participaron 73 organizaciones privadas e Instituciones del Estado en Panamá.

Confiamos en que los resultados permitirán a los participantes hacer "Benchmark" frente a sus pares.

Finalmente, queremos expresar nuestro agradecimiento a todos los participantes del estudio, sin los cuales el éxito del mismo no hubiese sido alcanzado.

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

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

© 2009 -2010 RISCCO. Todos los derechos reservados.

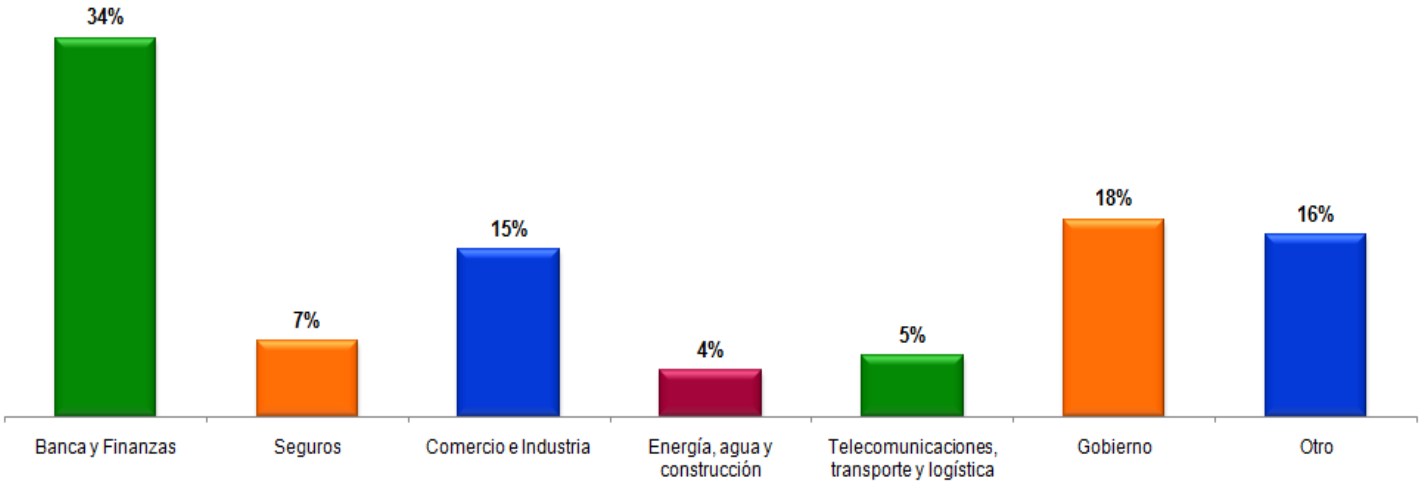
Participantes del estudio

En la primera edición del estudio “Estado de la Seguridad de Información y Privacidad de Datos en Panamá”, participaron 73 organizaciones privadas y estatales, representativas de diferentes sectores económicos.

La información suministrada por los participantes fue tratada con la más estricta confidencialidad, se transmitió en forma cifrada (encriptada) y almacenada en servidores que cuentan con las certificaciones de privacidad y seguridad, preservando el anonimato de las organizaciones participantes.

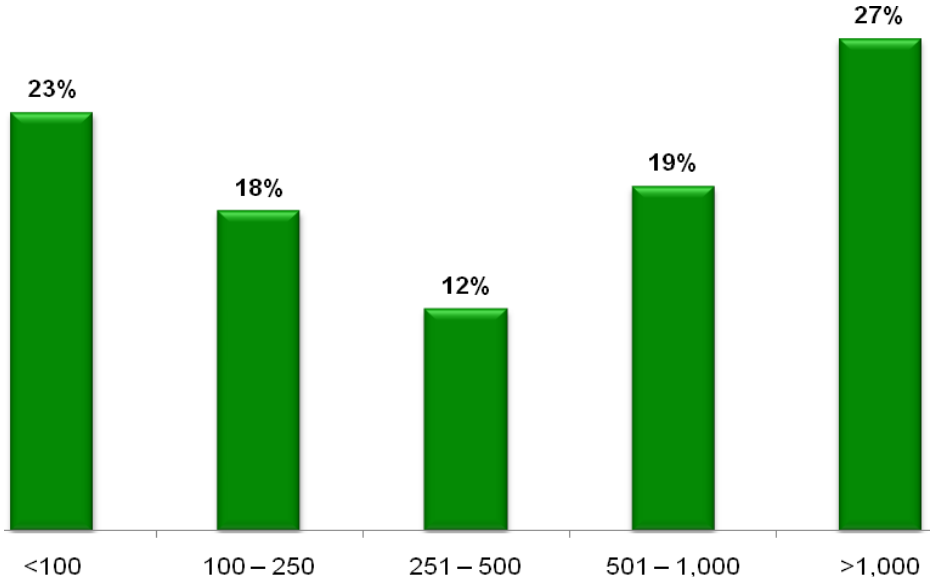
73 organizaciones privadas y estatales participaron en la primera edición del estudio.

Sector económico al que pertenecen las organizaciones participantes

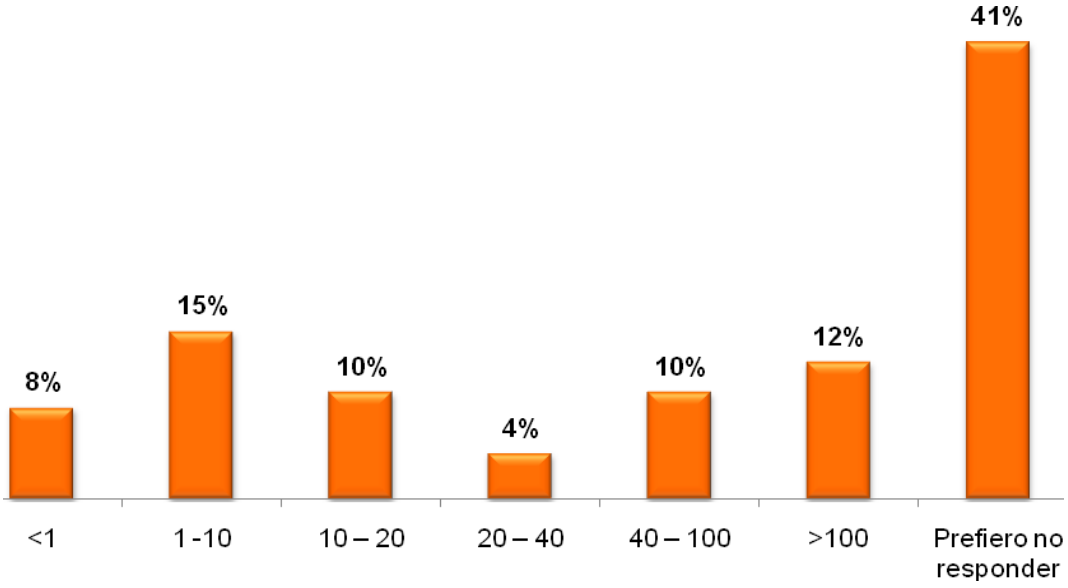


© 2009 -2010 RISCCO. Todos los derechos reservados.

Número de colaboradores de las organizaciones participantes



Ingreso de las organizaciones participantes durante el año 2009
(en millones de Balboas)



© 2009 -2010 RISCCO. Todos los derechos reservados.

Resumen ejecutivo

1. La probabilidad de que las organizaciones pierdan información sensitiva es un riesgo alto.

Esta afirmación la sustentan los siguientes aspectos:

- ✓ 46% de los participantes indicó que el robo de notebooks es el segundo incidente más frecuentemente experimentado.
- ✓ 74% indicó no encriptar los datos de USB y otros medios removibles.
- ✓ 66% indicó no encriptar los datos de los discos fijos de los desktops y notebooks.
- ✓ Solo un 18% indicó que los controles de seguridad de información en su organización son suficientemente fuertes.

2. Las tecnologías de seguridad utilizadas siguen siendo las tradicionales, las cuales poco o nada hacen para mitigar los nuevos riesgos tecnológicos.

Un 93% de los participantes utilizan programas antivirus, un 85% firewall y un 78% programas anti-spyware. Esto es ciertamente positivo, sin embargo, es conocido que este tipo de tecnologías poco ayudan para mitigar ataques tipo “SQL Injection” o “Man in the Middle Browser Trojan Attack”. Solo un 15% dispone de software para la administración y correlación de bitácoras de auditoría. Casi el 90% no utiliza técnicas de autenticación tipo “one time password”. Además, tal como se indica en el punto anterior, la encriptación de datos en medios removibles y discos fijos no es ampliamente utilizada.

© 2009 -2010 RISCCO. Todos los derechos reservados.

3. La seguridad de información no se está tomando seriamente. Existe una contradicción entre el discurso y las acciones concretas para proteger las redes, datos y sistemas de las organizaciones.

Los participantes reconocen que la complejidad de sus infraestructuras tecnológicas es alta. Además la Alta Gerencia considera importante los temas de seguridad de información. Los presupuestos de seguridad de información no disminuirán de manera importante para 2010. Sin embargo, solo un 16% tiene un oficial de seguridad a tiempo completo. Un 52% no cuenta con un modelo de seguridad implantado. El 60% no dispone de un Auditor Interno de Sistemas. Sólo un 29% indicó tener un mapa de riesgo tecnológico actualizado.

4. La privacidad y protección de datos pareciera no ser una preocupación importante y sigue siendo una responsabilidad del Gerente de Sistemas y no del área de riesgo y/o Alta Gerencia.

El 44% de los participantes no tiene un proceso para la clasificación de datos personales de los clientes. El 61% indicó que el responsable en definir la estrategia de privacidad y protección de datos es el área de tecnología y seguridad de información, cuando debería ser el área de riesgo y/o la Alta Gerencia. Sólo un 23% indicó tener controles efectivos para evitar y/o identificar la fuga de datos personales de los clientes. Menos de una tercera parte (29%) indicó disponer de herramientas de software para prevenir la pérdida de datos. Un 48% afirmó disponer de una estrategia a nivel directivo para proteger los datos personales de los clientes.

En cuanto al cumplimiento del estándar internacional PCI DSS (Payment Card Industry Data Security Standard), solo un 22% conoce qué es y están trabajando en cumplir con sus requerimientos.

5. La falta de concienciación sobre seguridad de información hacia los usuarios finales fue, en el 2009 y será en el 2010, el principal desafío.

Los tres desafíos más importantes en 2009 para los participantes del estudio fueron: falta de concienciación hacia la seguridad de los usuarios finales (60%), poca disponibilidad de recursos (personal y económico) un 45%, y falta de personal (oficial de seguridad u otros) en un 45%.

Para 2010 es: falta de concienciación hacia la seguridad de los usuarios finales (47%), poca disponibilidad de recursos (personal y económico) un 45%, y presupuesto limitado en un 45%.

6. En el 2010, implantar un modelo de seguridad de información, no está en la agenda de las prioridades.

Para un 64% de los participantes, la prioridad número uno es realizar pruebas de vulnerabilidad externas/internas a las redes, mientras que igual porcentaje de participantes desea implantar nuevas tecnologías de seguridad. La tercera, con un 62%, es mejorar las tecnologías para la protección de datos.

No obstante, en la posición nueve con un 32% está implantar marcos normativos internacionales como ISO/IEC 27001 o COBIT. La norma ISO 27001 es un sistema de gestión de seguridad de la información para evaluar el riesgo e implantar controles apropiados, para preservar la confidencialidad, la integridad y la disponibilidad de la información.

© 2009 -2010 RISCCO. Todos los derechos reservados.

Riesgos y amenazas

El estudio revela que un 63% de las organizaciones participantes no experimentó incidentes de seguridad de información en los últimos doce meses. Un 8% indicó que desconoce si fue víctima. Los incidentes identificados siguen siendo los comunes como virus y robo de notebooks. Esto pudiese no ser cónsono con lo indicado por el 55% de los participantes en cuanto a que el grado de complejidad de la infraestructura tecnológica de la organización es muy alto o alto. Esto puede concluirse al observar los datos que siguen:

- ✓ 29% indicó haber sufrido algún incidente de seguridad. De este 29%, el 81% indicó haber sufrido entre 1 y 5 incidentes de seguridad en los últimos doce meses.
- ✓ Los tres incidentes más frecuente en los últimos doce meses fueron: 54% virus, 46% robo de notebooks y un 27% alteración no autorizada de datos en las aplicaciones.
- ✓ El responsable de los incidentes es, en un 35%, personal interno y 31%, personal externo.

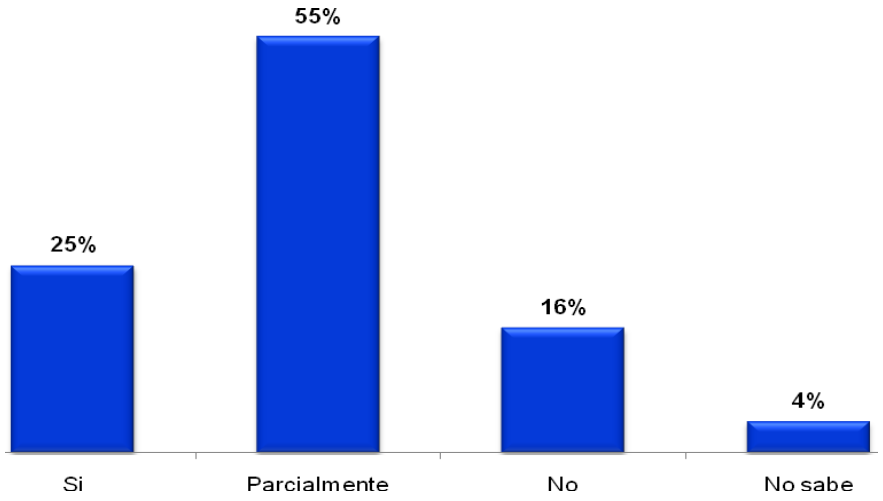
A pesar de la relevancia de los incidentes de seguridad de información reportados, sólo el 25% de los participantes considera que cuenta con los conocimientos y herramientas necesarios para hacer las investigaciones forenses en caso de ocurrir un incidente de seguridad de información en su organización.

En materia de seguridad de información resulta difícil proteger las redes, datos y sistemas si se desconoce a qué riesgos tecnológicos se está expuesto. Un mapa de riesgo tecnológico es vital para esto. ¿Cómo podemos proteger las redes, datos y sistemas de la organización con efectivos controles si desconocemos los riesgos a los que estamos expuestos?

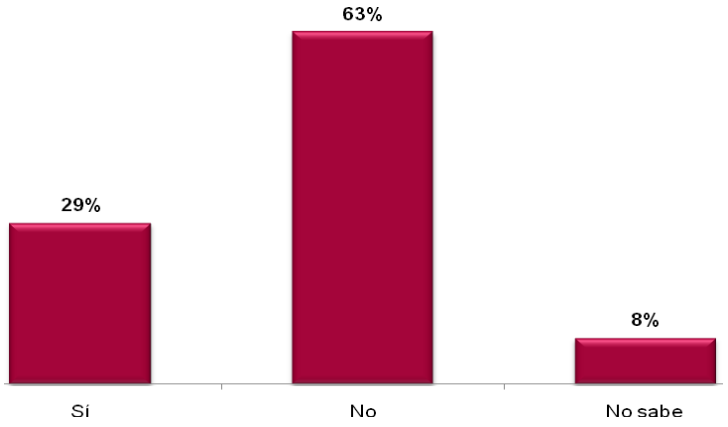
En cuanto a la existencia de un mapa de riesgo tecnológico actualizado, solo un 29% de los participantes del estudio indicó disponer de uno.

© 2009 -2010 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

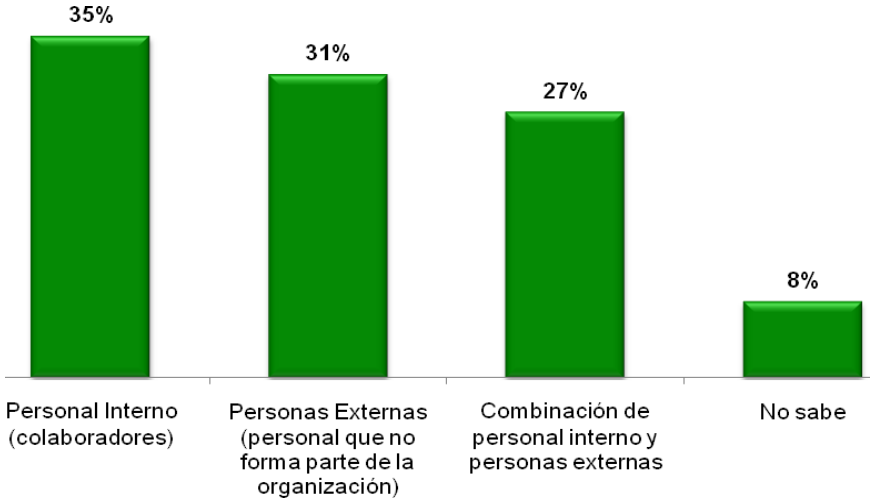


Experimentó incidentes de seguridad de información en los últimos doce meses

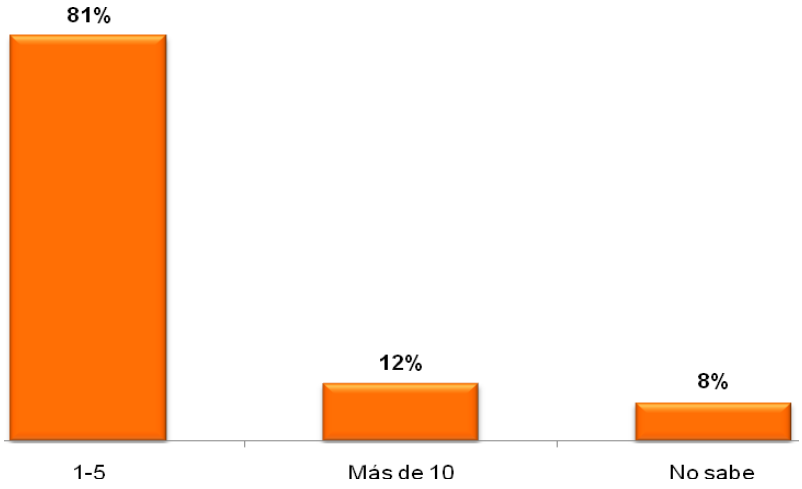


© 2009 -2010 RISCCO. Todos los derechos reservados.

Responsable de los incidentes de seguridad de información

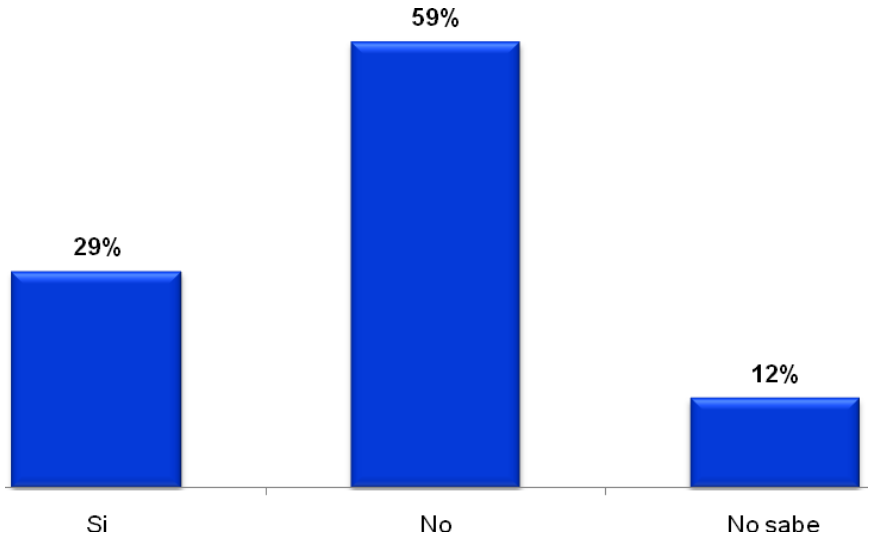


Número de incidentes de seguridad de información ocurridos en los últimos doce meses



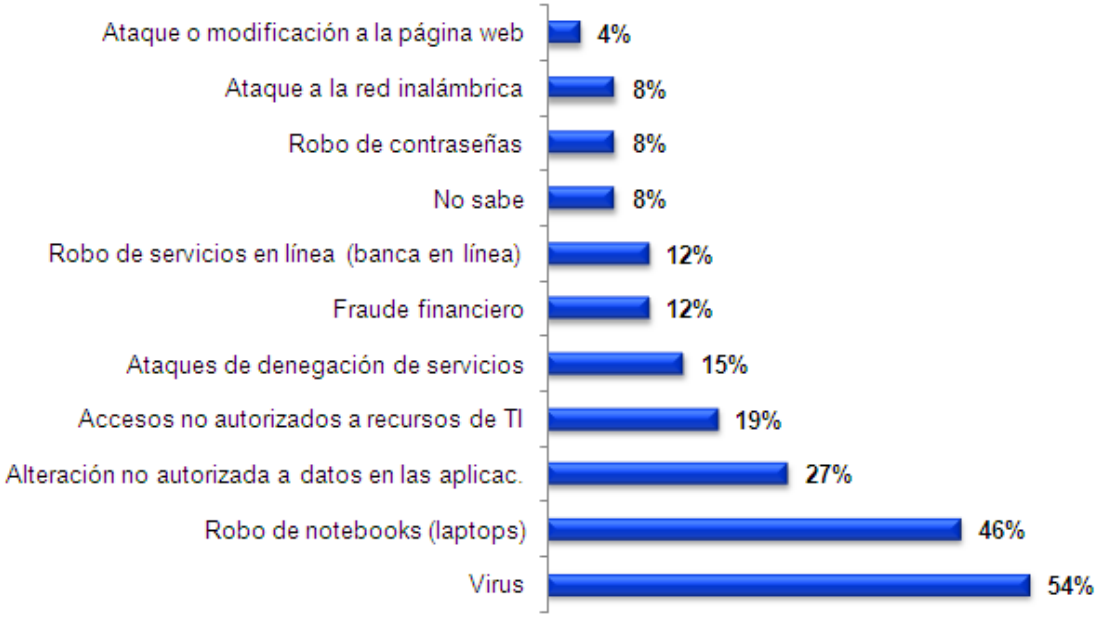
© 2009 -2010 RISCCO. Todos los derechos reservados.

Existe en la organización un de mapa de riesgos tecnológicos actualizado

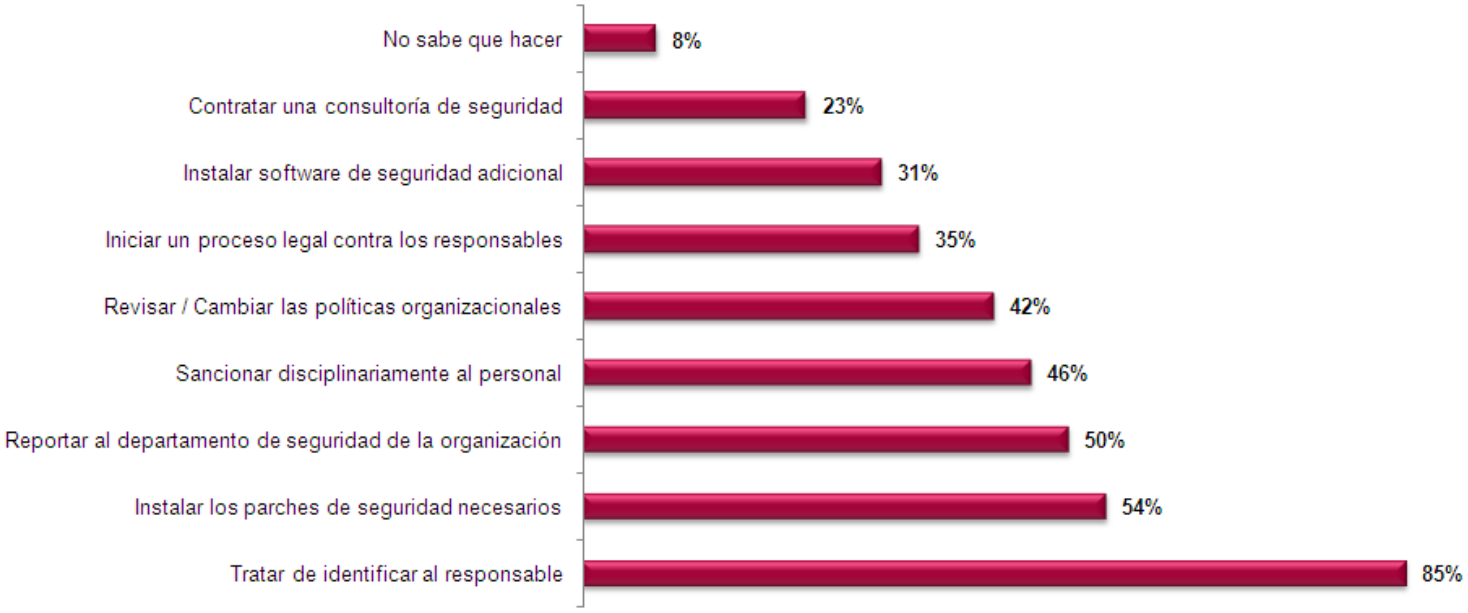


© 2009 -2010 RISCCO. Todos los derechos reservados.

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



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



© 2009 -2010 RISCCO. Todos los derechos reservados.

Gobernabilidad

Existe una aparente contradicción entre el discurso y la acción. Por un lado los participantes reconocen como alta la complejidad de sus infraestructuras tecnológicas y que la Alta Gerencia considera importantes los temas de seguridad de información. Pero, por otro lado, no se tiene un oficial de seguridad, un modelo de seguridad no ha sido ampliamente implantado y la concienciación de los usuarios finales hacia la seguridad, es muy baja. Estos análisis se basan en los siguientes resultados:

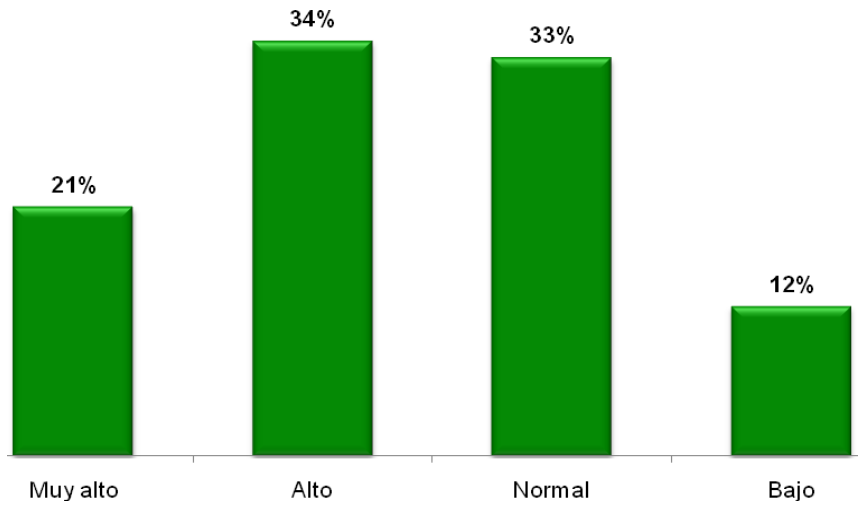
- ✓ 55% considera que la complejidad de la infraestructura tecnológica es muy alta o alta.
- ✓ 69% considera que, para la Alta Gerencia, los temas de seguridad de información son muy importantes o importantes.
- ✓ 55% no cuenta con un oficial de seguridad de información y, de aquellos que tienen uno, sólo un 16% de éstos está dedicado al 100% a tan importante labor.
- ✓ 60% no cuenta con un Auditor Interno de Sistemas.
- ✓ 52% no tiene un modelo de seguridad debidamente documentado e implantado.

En cuanto a los desafíos en materia de seguridad de información experimentados en 2009 y que se esperan experimentar en 2010, prácticamente son los mismos:

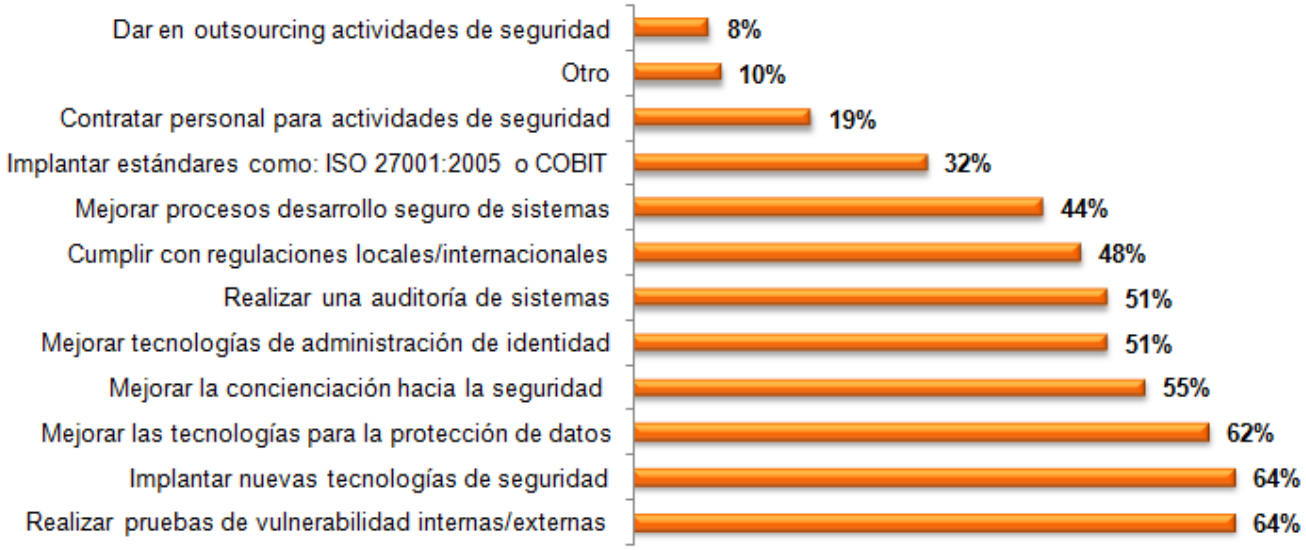
- ✓ Falta de concienciación de los usuarios finales (60% y 47%).
- ✓ Disponibilidad de recursos (45% en ambos años).
- ✓ Falta de un oficial de seguridad (45% y 29%).
- ✓ Presupuesto muy limitado (44% y 45%)

© 2009 -2010 RISCCO. Todos los derechos reservados.

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

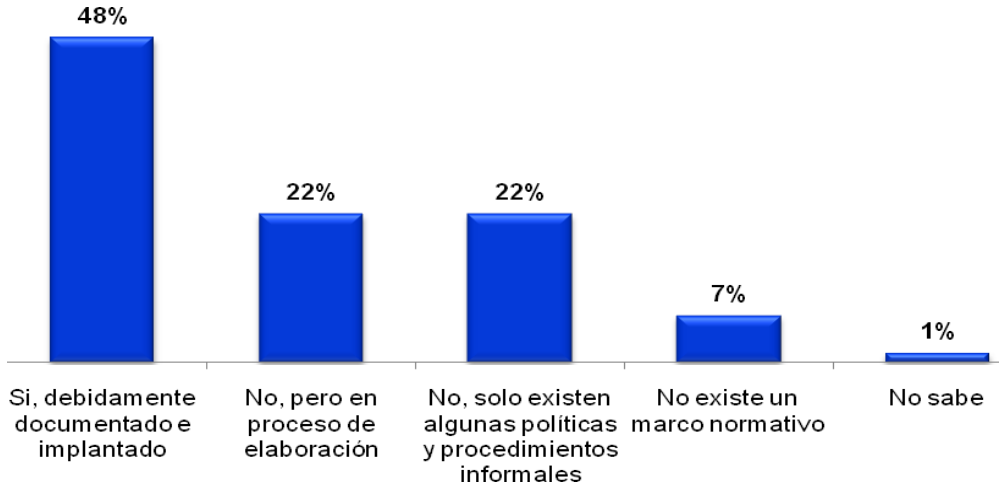


Orden de prioridades en cuanto a seguridad de información en el año 2010



© 2009 -2010 RISCCO. Todos los derechos reservados.

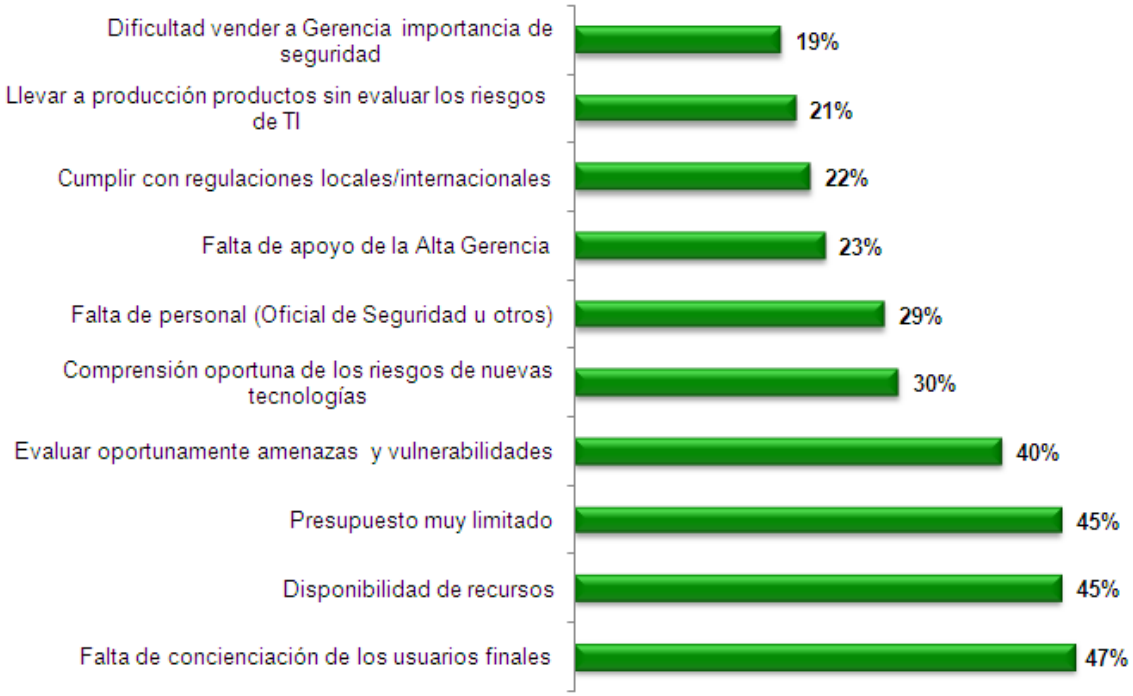
Existe un marco normativo (políticas, procesos y procedimientos) para administrar la seguridad de información



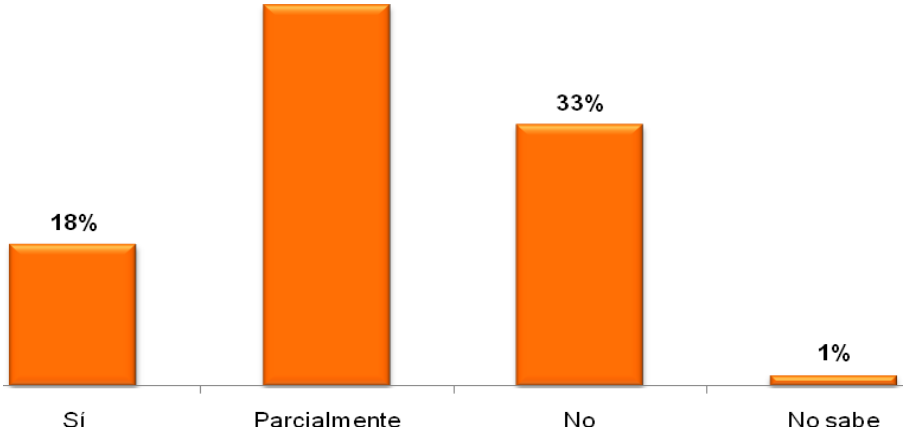
Principales desafíos relacionados con la seguridad de información, experimentados en el año 2009

© 2009 -2010 RISCCO. Todos los derechos reservados.

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

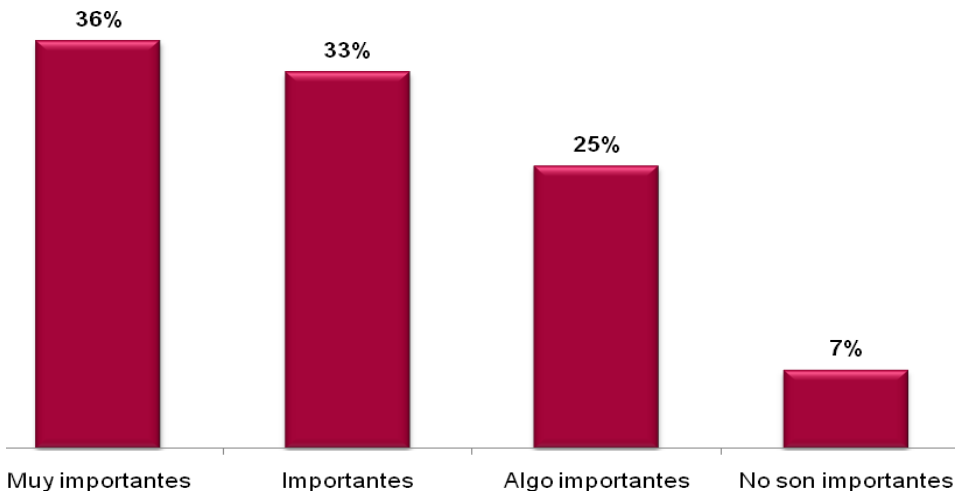


Existe un programa permanente y formal de concienciación hacia la seguridad de información para los usuarios



© 2009 -2010 RISCCO. Todos los derechos reservados.

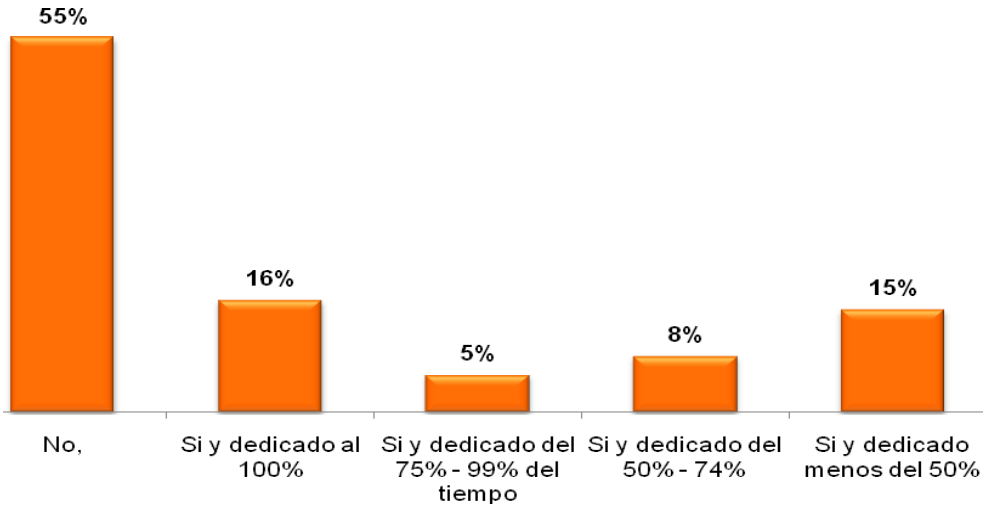
Cómo considera la Alta Gerencia los temas de seguridad de Información



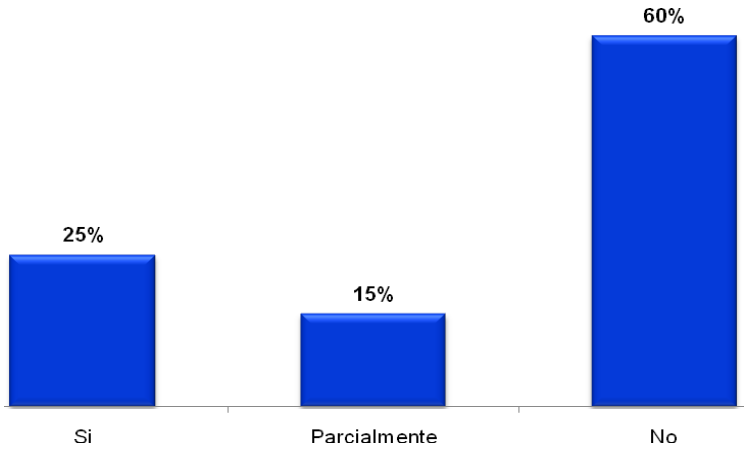
Estándares internacionales de seguridad de información adoptados en la organización

© 2009 -2010 RISCCO. Todos los derechos reservados.

Cuenta la organización con un Oficial de Seguridad

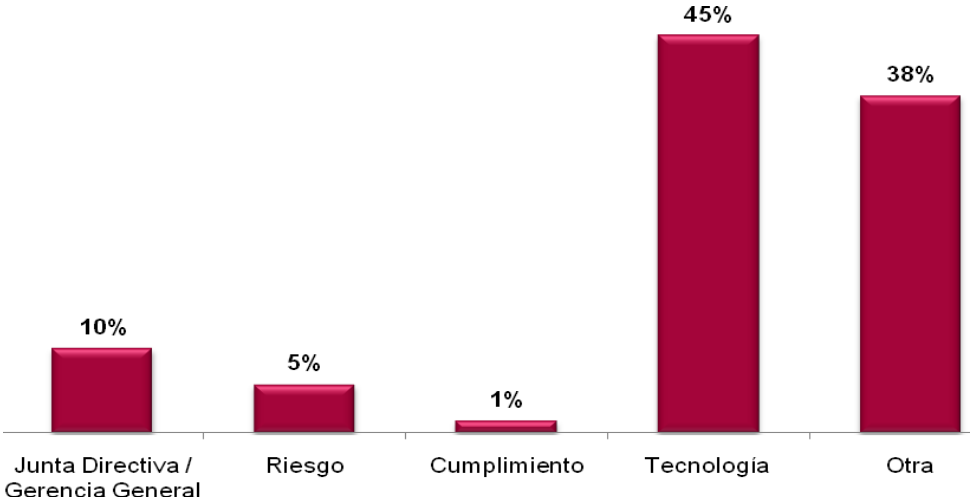


Cuenta la organización con un Auditor Interno de Sistemas



© 2009 -2010 RISCCO. Todos los derechos reservados.

A quién reporta el Oficial de Seguridad de Información



© 2009 -2010 RISCCO. Todos los derechos reservados.

Operaciones y Tecnologías de Seguridad

El estudio refleja claramente, que las organizaciones en Panamá aún prefieren tener el control de la mayoría de las actividades relacionadas con seguridad de información y no seguir la tendencia global al respecto. Muy pocas actividades relacionadas con seguridad de información de los participantes del estudio, han sido dadas en outsourcing:

- ✓ 15% indicó haber dado en outsourcing, pruebas de penetración externas/internas.
- ✓ 3% pruebas a las aplicaciones.
- ✓ 5% manejo de incidentes de seguridad.

El control de las actividades de seguridad de información son, preferentemente, realizadas por personal interno de las organizaciones, revela el estudio. No obstante, sólo un 18% indicó que considera que los controles de seguridad de información son suficientemente fuertes en su organización.

Para tener el control de las actividades de seguridad de información se requieren recursos, incluyendo el económico. Esto parece no ser un problema para los participantes del estudio ya que:

- ✓ 81% indicó que el presupuesto de seguridad de información para 2010 se incrementará o se mantendrá igual con relación al del 2009.
- ✓ 42% indicó que el presupuesto de seguridad de información para 2010, es 3% o mayor con relación al presupuesto total de tecnología.

Sobre el uso de tecnologías de seguridad para proteger los datos, redes y sistemas, el estudio muestra que las organizaciones continúan, preferentemente, utilizando tecnologías tradicionales como antivirus (93%) y firewall (85%) y aún no adoptan otros tipos de herramientas que podrían ayudarlos a proteger la organización de riesgos tecnológicos que tecnologías tradicionales, sencillamente no pueden mitigar.

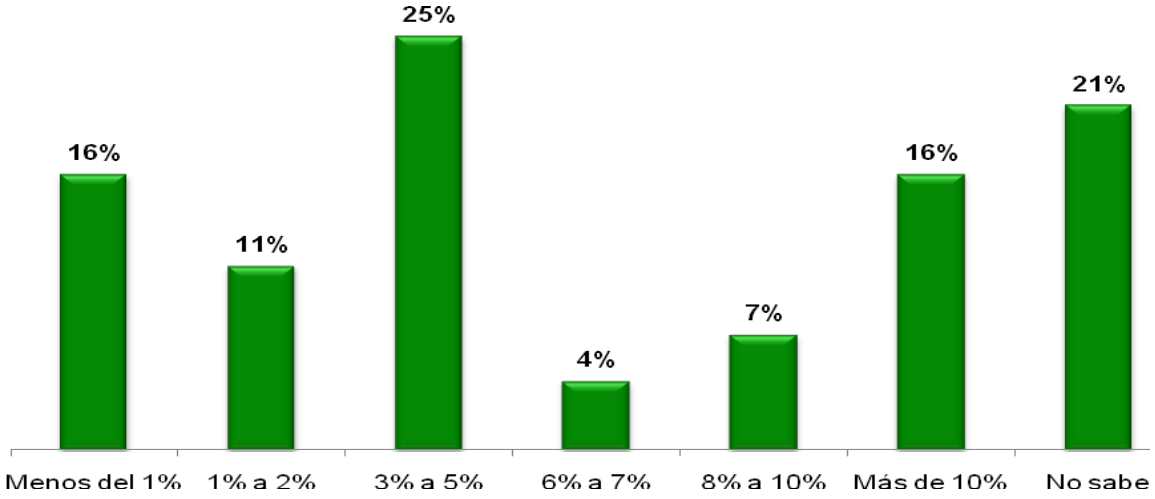
Esto se desprende de lo siguiente:

- ✓ 74% no utiliza encriptación para datos en USB y 64% para datos en tránsito.
- ✓ 66% no encripta los datos de los discos fijos de los computadores.
- ✓ 15% dispone de software para la administración y correlación de bitácoras de auditoría.
- ✓ 90% no utiliza técnicas de autenticación de “one time password”

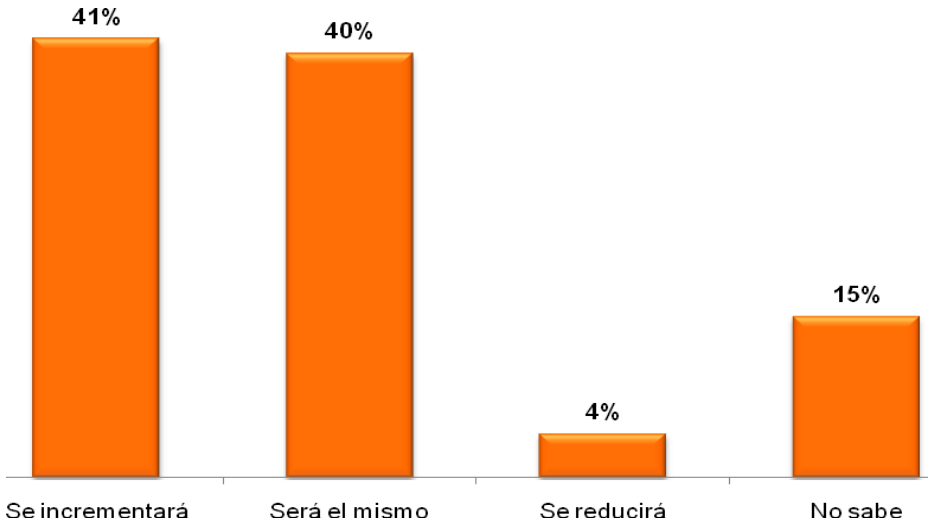
Una estrategia para la recuperación de las facilidades de tecnología ante una interrupción prolongada es un área susceptible a mejora. Sólo el 41% de los participantes indicó tener un plan de recuperación ante desastres.

© 2009 -2010 RISCCO. Todos los derechos reservados.

Porcentaje del presupuesto de tecnología asignado a la seguridad de información

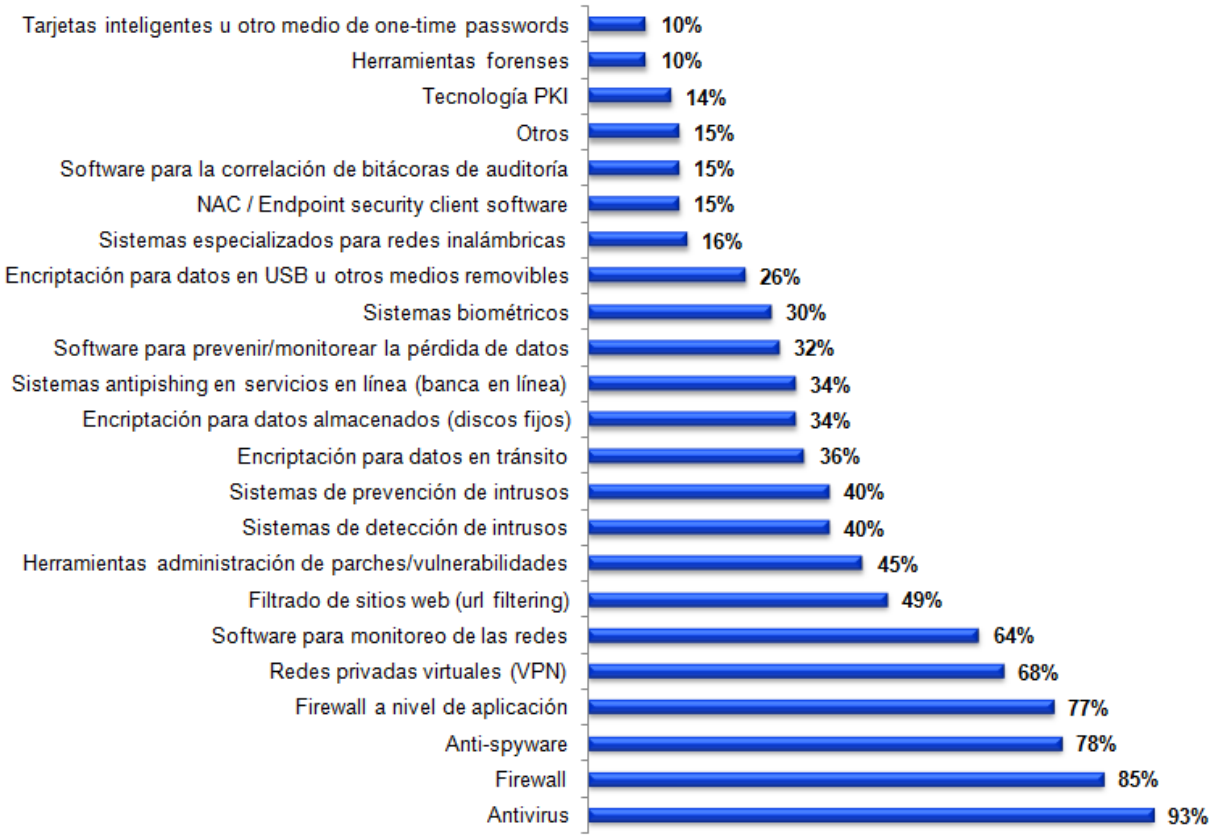


Presupuesto de seguridad de información del 2010 con relación al presupuesto del 2009

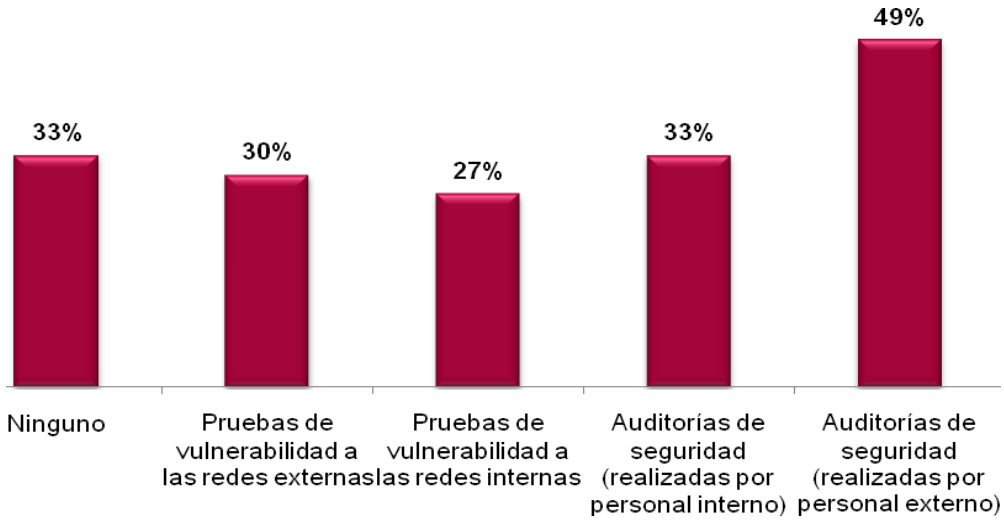


© 2009 -2010 RISCCO. Todos los derechos reservados.

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

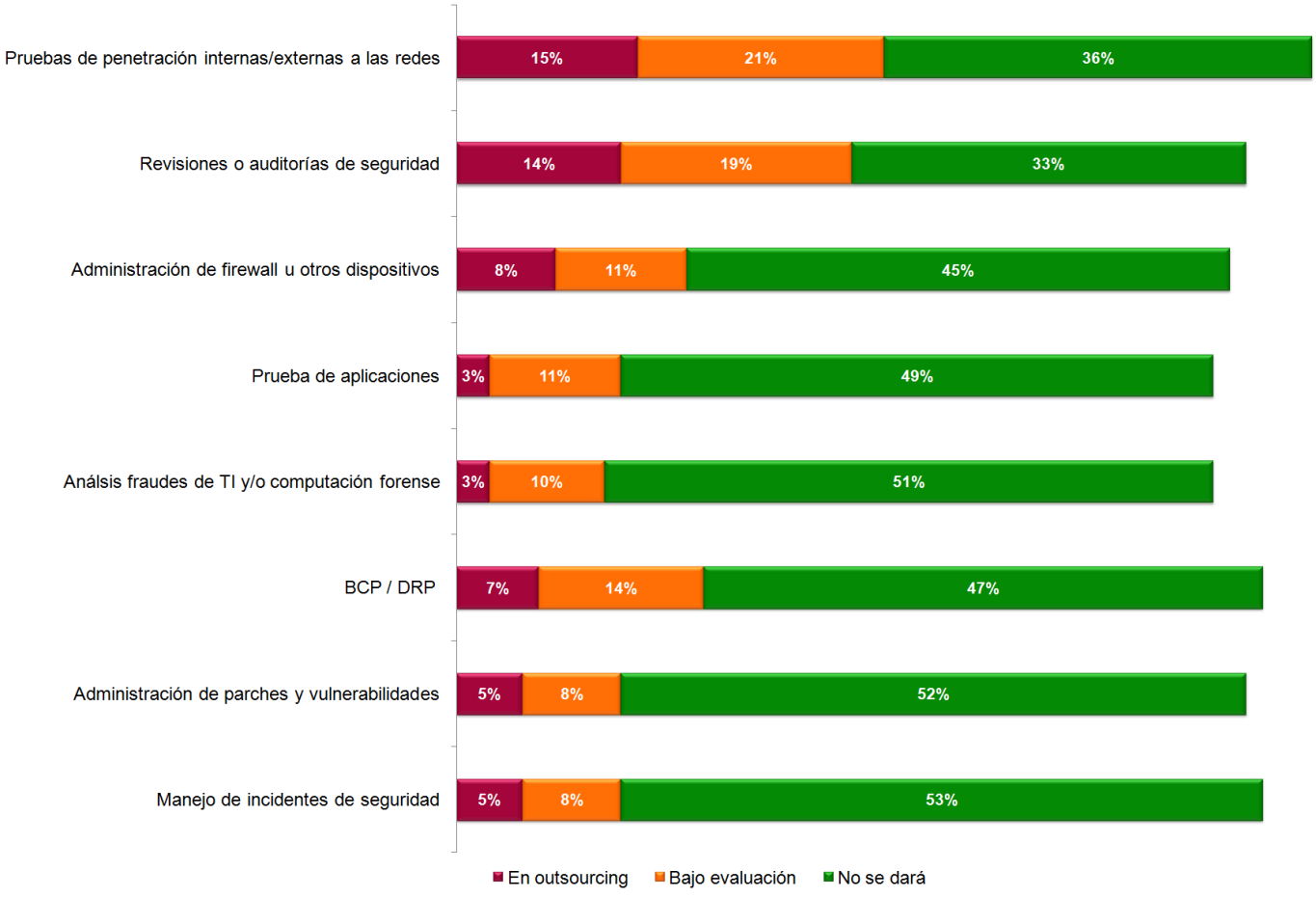


Mecanismo utilizado para evaluar la efectividad de la seguridad de la información



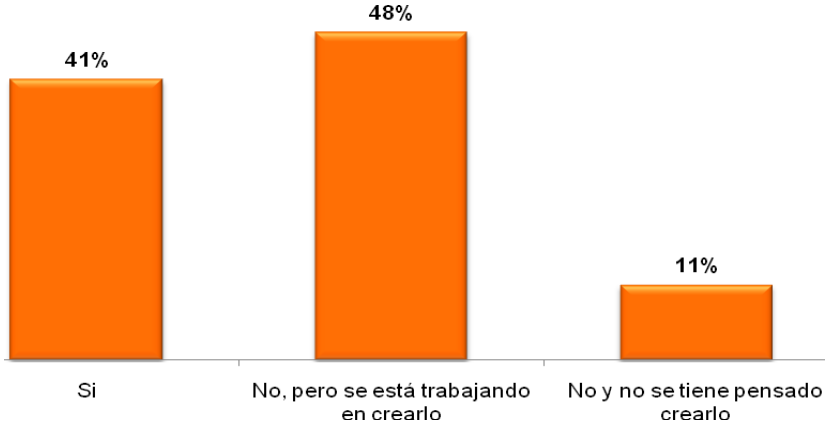
© 2009 -2010 RISCCO. Todos los derechos reservados.

Qué actividades de seguridad de información han sido dadas o se darán en outsourcing



© 2009 -2010 RISCCO. Todos los derechos reservados.

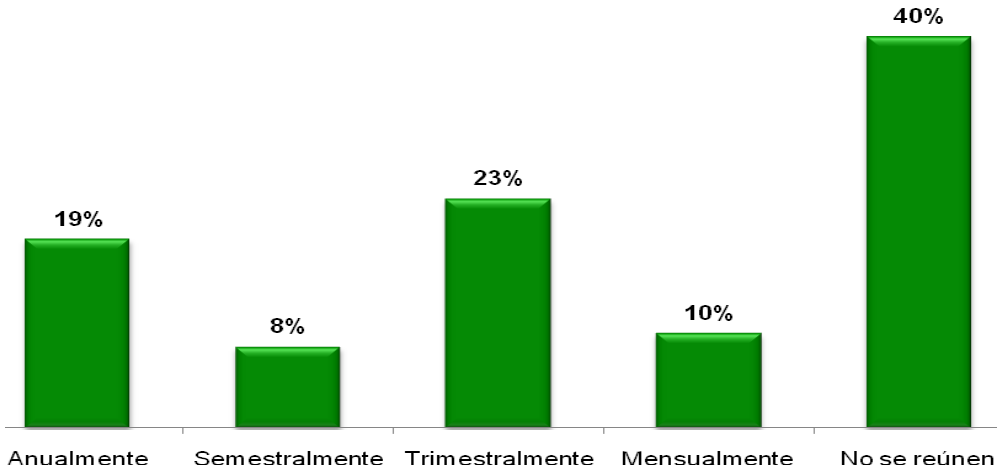
Dispone su organización de un plan de recuperación ante desastres



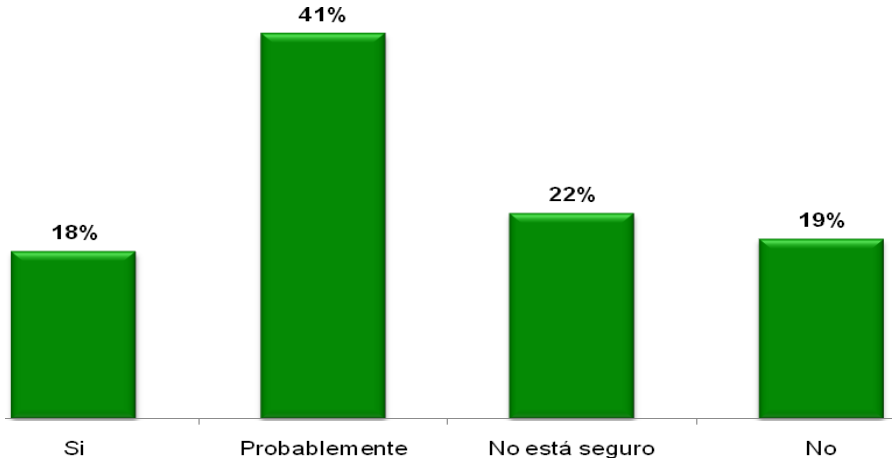
¿Qué solución tiene su organización para la continuidad operativa del negocio?

© 2009 -2010 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

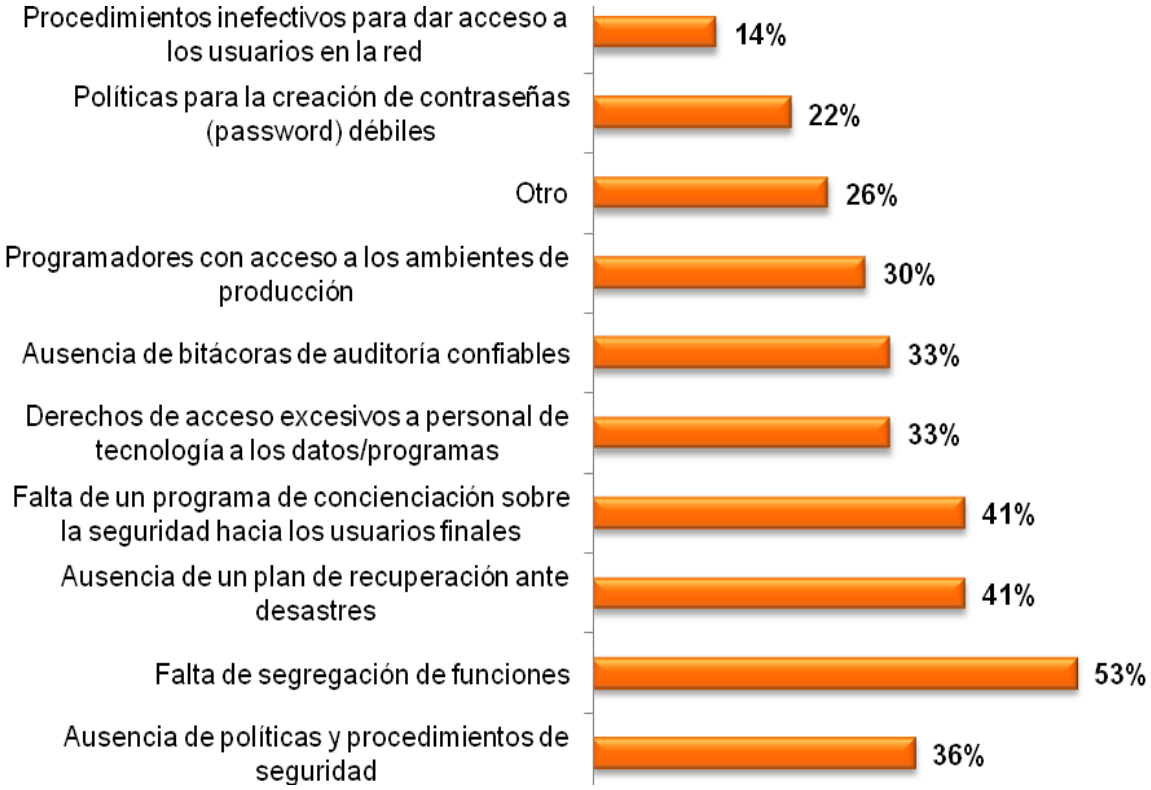


Los controles de seguridad de información son suficientemente fuertes en su organización



© 2009 -2010 RISCCO. Todos los derechos reservados.

Principales hallazgos plasmados en las auditorías internas/externas de seguridad durante el 2009



© 2009 -2010 RISCCO. Todos los derechos reservados.

Privacidad y Protección de Datos

Los medios de comunicación locales e internacionales, constantemente recuerdan a las organizaciones e Instituciones del Estado, lo frágil que pueden ser sus estrategias de seguridad de información para proteger los datos personales de los clientes. Desde el 2005 a Junio de 2010, 354 millones de registros con información personal sensitiva habían sido comprometidos, solo en los Estados Unidos, según la organización *Privacy Rights Clearinghouse.*

A nivel mundial, el impacto negativo a la imagen de la compañía y los elevados costos de potenciales demandas, ha forzado a que la privacidad y protección de datos personales de los clientes, sean reconocidas como riesgos en la agenda de la Junta Directiva de las organizaciones y no una responsabilidad del área de tecnología de información.

El estudio refleja que la privacidad y protección de los datos de los clientes en Panamá, pareciera no haber alcanzado la prioridad que merece y que sigue siendo un tema en la agenda del área de tecnología de información, contrario a la tendencia mundial al respecto que atribuye esta responsabilidad al área de riesgo o la Alta Gerencia.

Entre los resultados sobre este tema están:

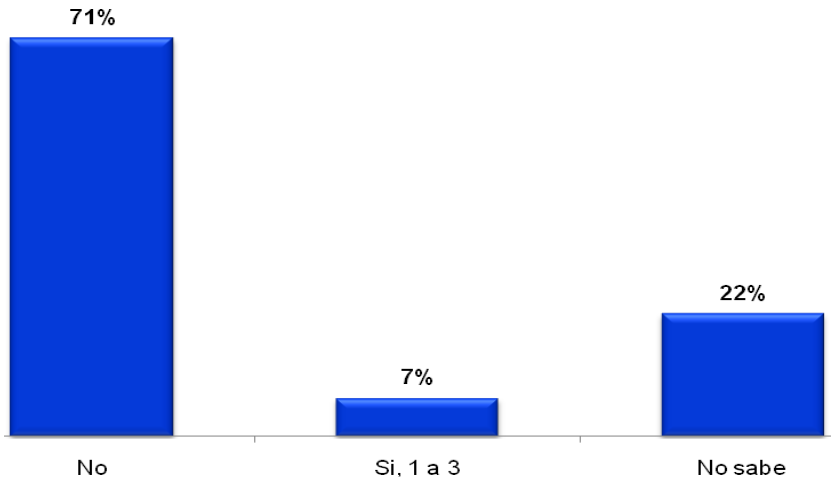
- ✓ 61% indicó que el responsable en definir la estrategia de privacidad y protección de datos es el área de tecnología y seguridad de información.
- ✓ 23% indicó tener controles efectivos para evitar y/o identificar la fuga de datos personales de los clientes.
- ✓ 29% indicó disponer de herramientas de software para prevenir la perdida de datos.
- ✓ 48% afirmó disponer de una estrategia a nivel directivo para proteger los datos personales de los clientes.
- ✓ 44% no tiene un proceso para la clasificación de datos personales de los clientes.

Por otro lado, llama la atención que sólo el 22% de los participantes estén trabajando en cumplir con el estándar internacional PCI DSS (Payment Card Industry Data Security Standard), cuando un número importante de organizaciones en Panamá almacenan, procesan o transmiten datos relacionados con tarjetas de crédito en sus comercios.

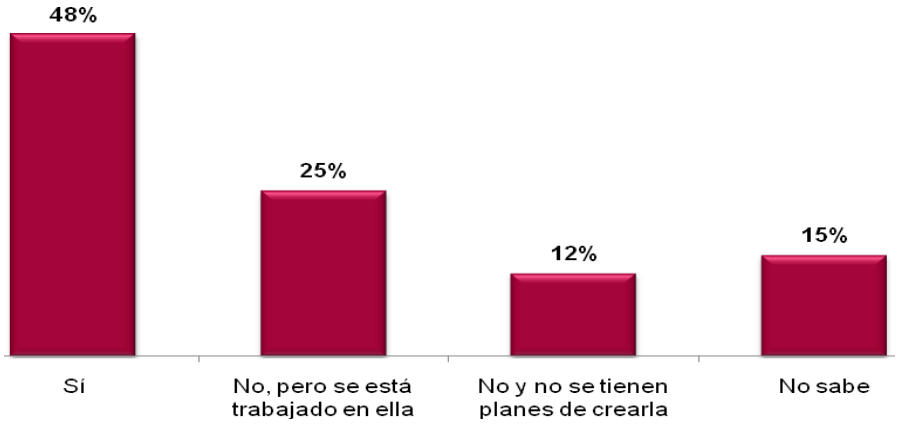
Por último, el 71% de los participantes indicó no haber sufrido incidentes relacionados con la pérdida o robo de datos personales de sus clientes. Este hecho pareciera contradictorio ante la ausencia, en la mayoría de los participantes del estudio, de herramientas de software y una estrategia de privacidad y protección de datos personales de los clientes.

© 2009 -2010 RISCCO. Todos los derechos reservados.

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

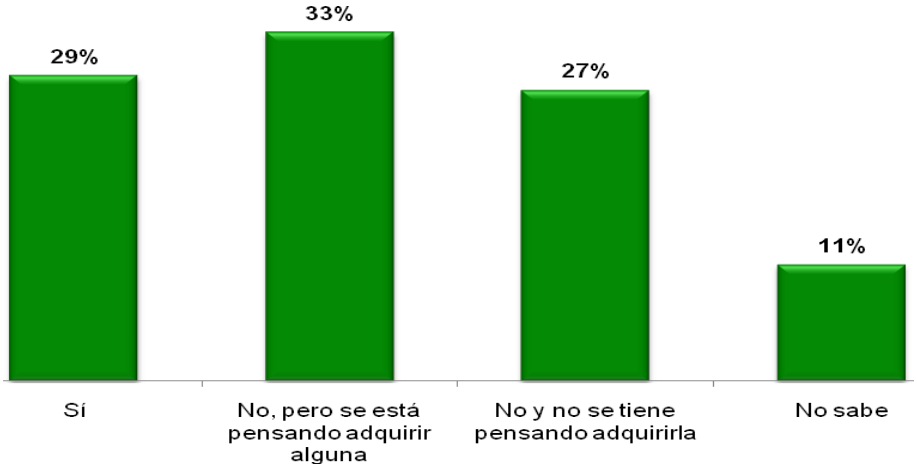


Existe alguna estrategia formal a nivel directivo para establecer controles y procedimientos para proteger los datos personales de los clientes

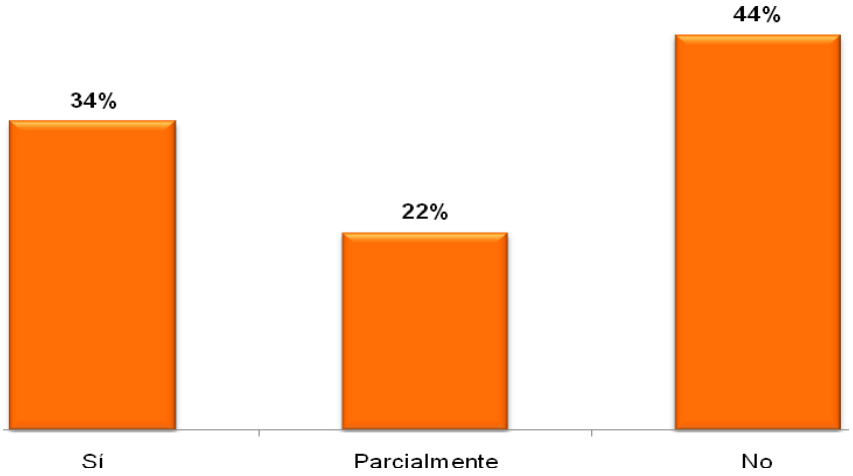


© 2009 -2010 RISCCO. Todos los derechos reservados.

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

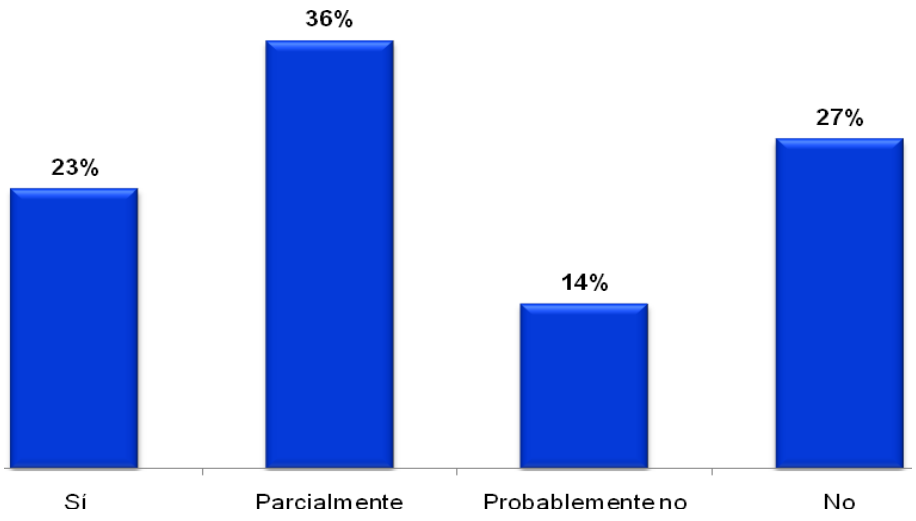


Existe un proceso para la clasificación de datos que defina controles para proteger los datos personales de los clientes

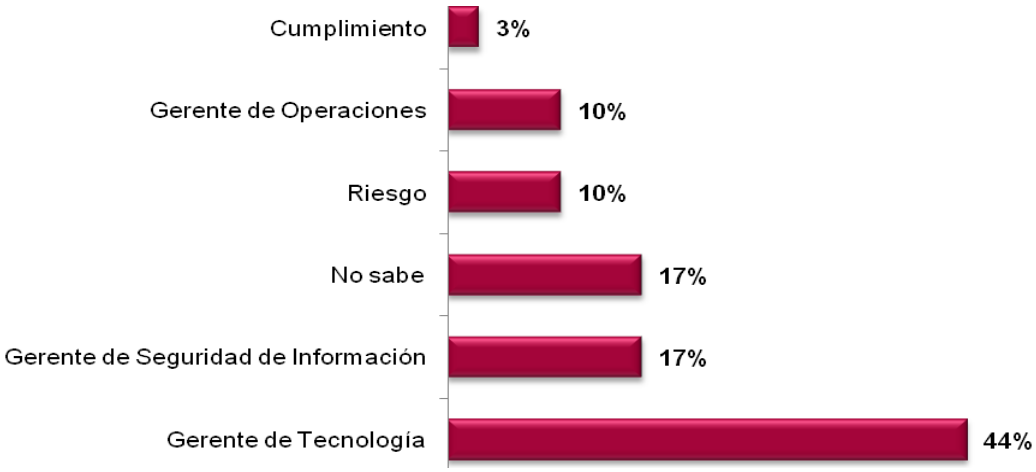


© 2009 -2010 RISCCO. Todos los derechos reservados.

Existen controles efectivos y suficientes para evitar y/o identificar la fuga de datos personales de los clientes

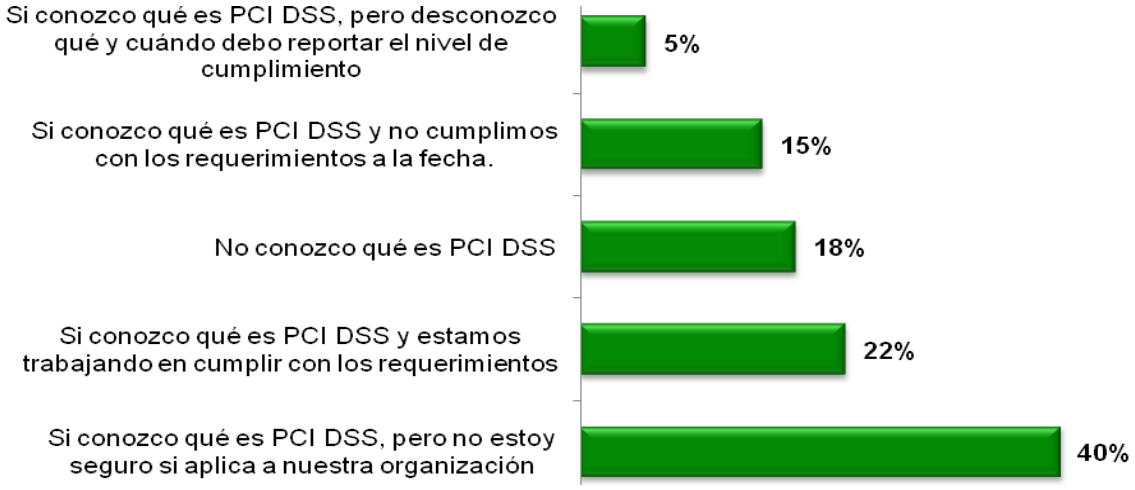


Quién es el responsable de definir la estrategia para la privacidad y protección de los datos de los clientes



© 2009 -2010 RISCCO. Todos los derechos reservados.

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



© 2009 -2010 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

Universidad Tecnológica de Panamá

Facultad de Ingeniería de Sistemas Computacionales

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

© 2009 -2010 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- 2010 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.