

2009 Consumer Business Estudio Global de Seguridad La seguridad no puede ser descartada

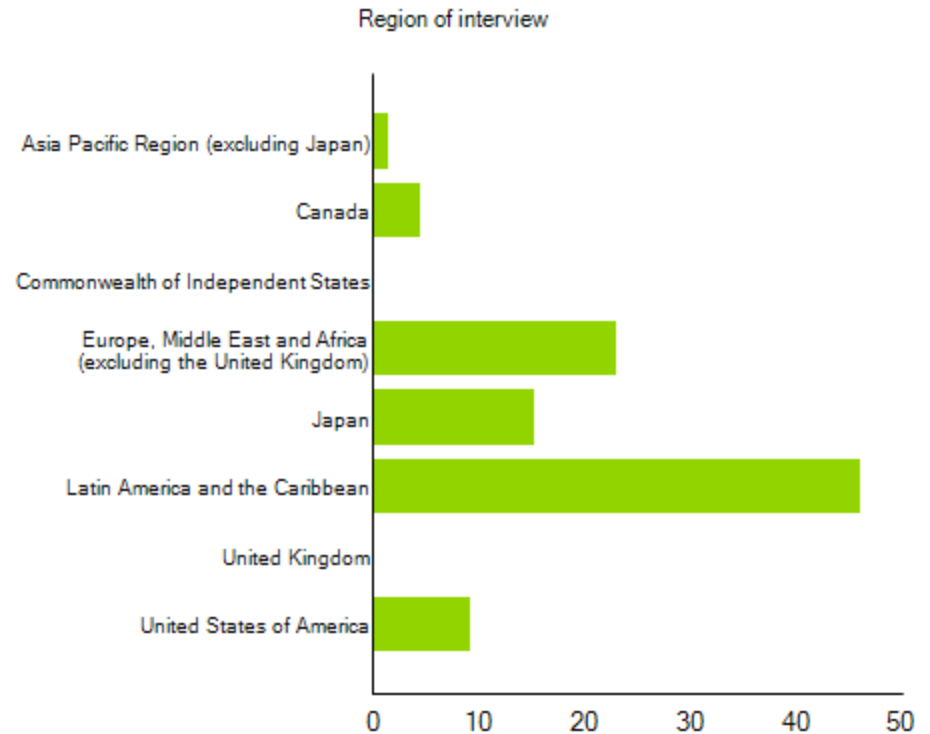


Quién Respondió

Región

La población de encuestados representa a todo el mundo:

- Asia, Pacífico y Japon 16%
- Europa, Medio oeste y Africa 24%
- América Latina y el Caribe 47%
- Norte América 13%

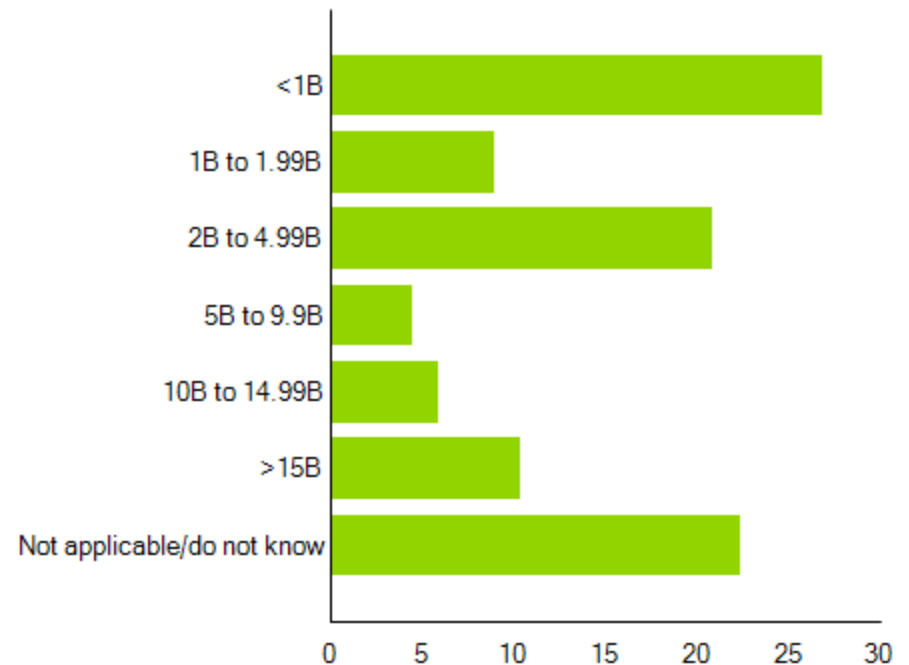


Ingresos anuales

Por los ingresos anuales (\$ USD), las empresas participantes representan un amplio espectro:

- >15B 10%
- 10B to 14.99B 6%
- 5B to 9.9B 4%
- 2B to 4.99B 21%
- 1B to 1.99B 9%
- <1B 27%

Indicate the approximate annual revenue of your organization in 2008 (\$USD):



Número de empleados

Por número de empleados en las organizaciones participantes, la distribución es la siguiente:

- Menos de 500 9%
- 501 a 1,000 1%
- 1,001 a 5,000 41%
- 5,001 a 10,000 15%
- 10,001 a 25,000 12%
- 25,001 a 50,000 7%
- 50,001 a 100,000 3%
- Más de 100,000 12%



Principales Hallazgos

Principales Hallazgos

1. La Seguridad de la información se considera como un problema de infraestructura de tecnología

Los negocios de **Consumer Business** prestan más atención a la **infraestructura** (especialmente en lo que se refiere a la **seguridad de la red**) que al **gobierno** de la seguridad.

La **Gobernabilidad** y la **Estrategia de seguridad de la información** no son claramente la prioridad número uno.

La **Estrategia de seguridad de la información** es una guía de como la organización puede mitigar riesgos cumpliendo con **exigencias legales, estatutarias, contractuales, y requerimientos** internos.

La falta de operatividad de una estrategia es claramente un problema

Las organizaciones de Consumer Business necesitan reconocer que el **Gobierno de Seguridad** ayuda a garantizar que los **controles de seguridad** están adecuadamente implementados.

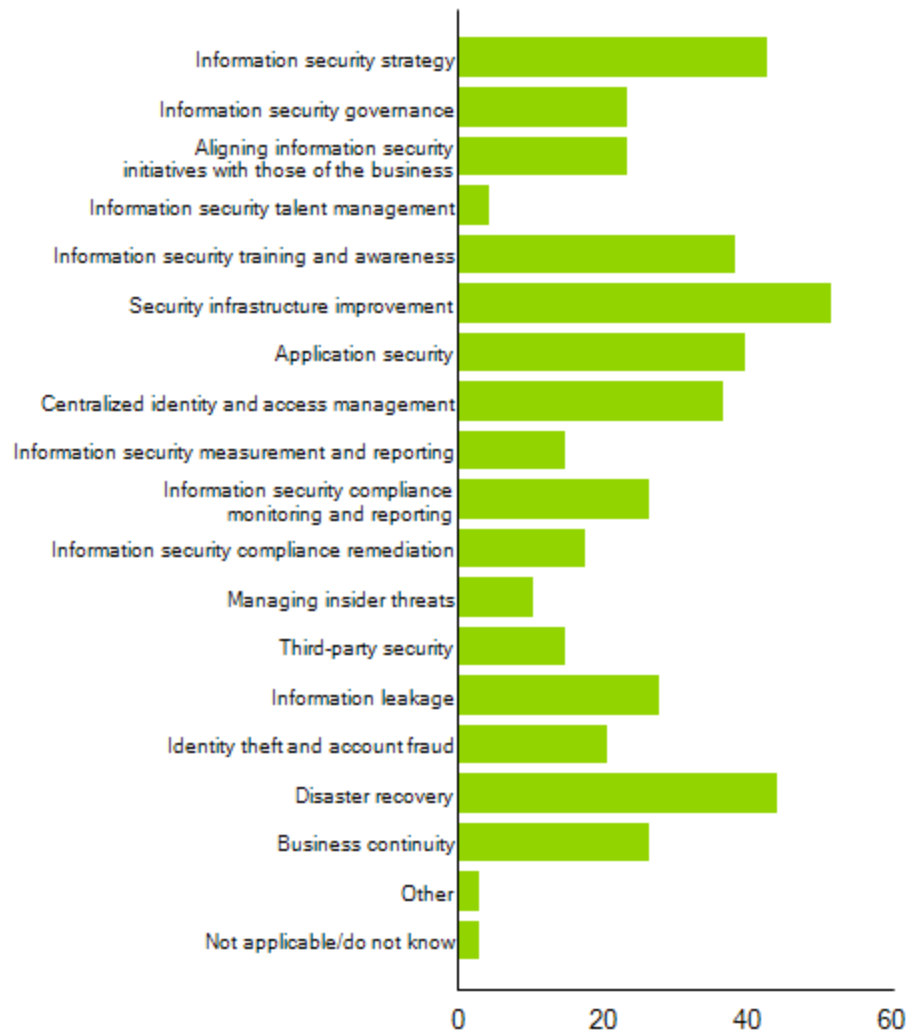
No todos los riesgos de seguridad hoy en día vienen de la infraestructura y es siempre más rentable prevenir un incidente que hacer frente a sus consecuencias.

Principales iniciativas de Seguridad para el 2009

Las mejoras a la infraestructura de Seguridad tomaron el primer lugar en 2009 con el 51% de los encuestados tomando esta elección.

La recuperación de desastres en un cercano segundo lugar (44%), seguido por la estrategia de seguridad de la información (43%), seguridad de aplicaciones (40%), y la capacitación en seguridad de la información y sensibilización (38%).

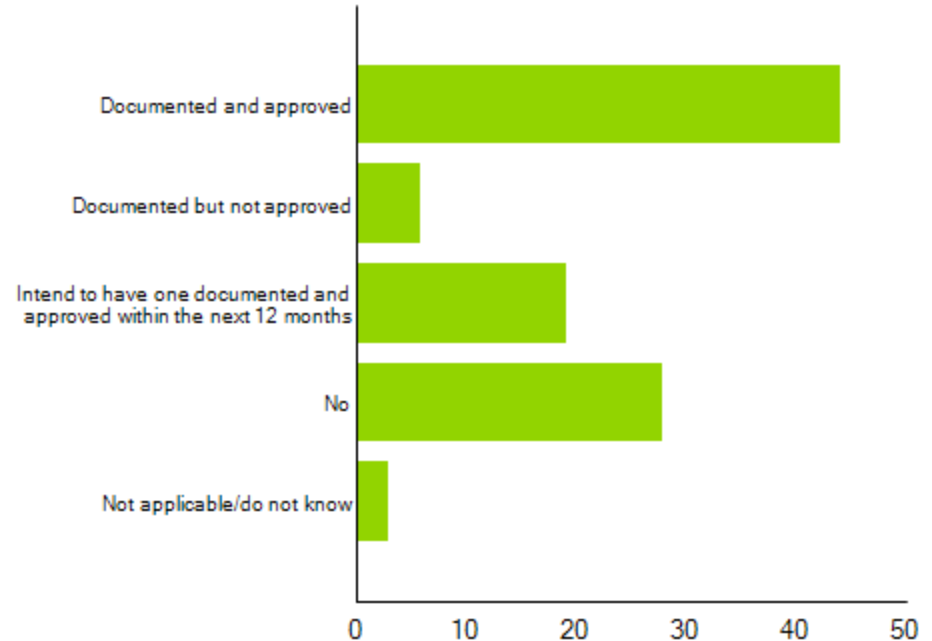
What are your organization's top five security initiatives for 2009?



Estructura del Gobierno de Seguridad.

Un marco de gobernabilidad o estructura define los roles y responsabilidades, políticas y procedimientos, principios guías, y los requisitos de rendición de cuentas de la gestión de seguridad de la información. Mientras que el 44% de las organizaciones tienen una estructura de gobierno documentada y aprobada, el 53% la tienen documentada pero no aprobada, e Intentan tenerla documentada y aprobada en los próximos 12 meses, o no tienen ninguna.

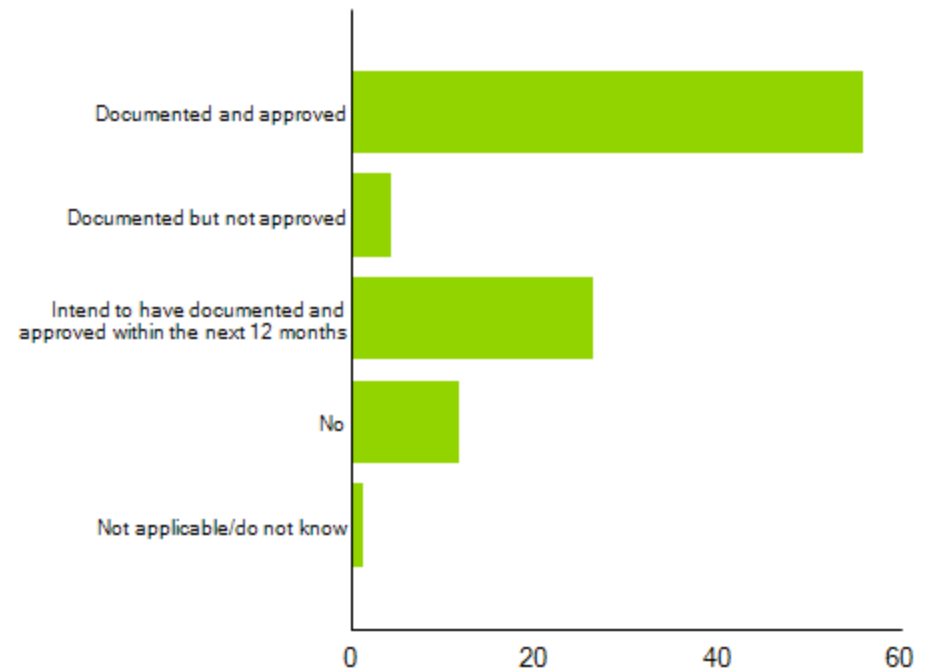
Does your organization have a documented and approved governance structure for information security?



Presencia de una estrategia de Seguridad de la Información definida

Mientras que el 56% de las organizaciones tienen una estrategia de seguridad de la información documentada y aprobada, el 42% la tienen documentada, pero no aprobada, e intentan tenerla documentada y aprobada en los próximos 12 meses o no tienen ninguna.

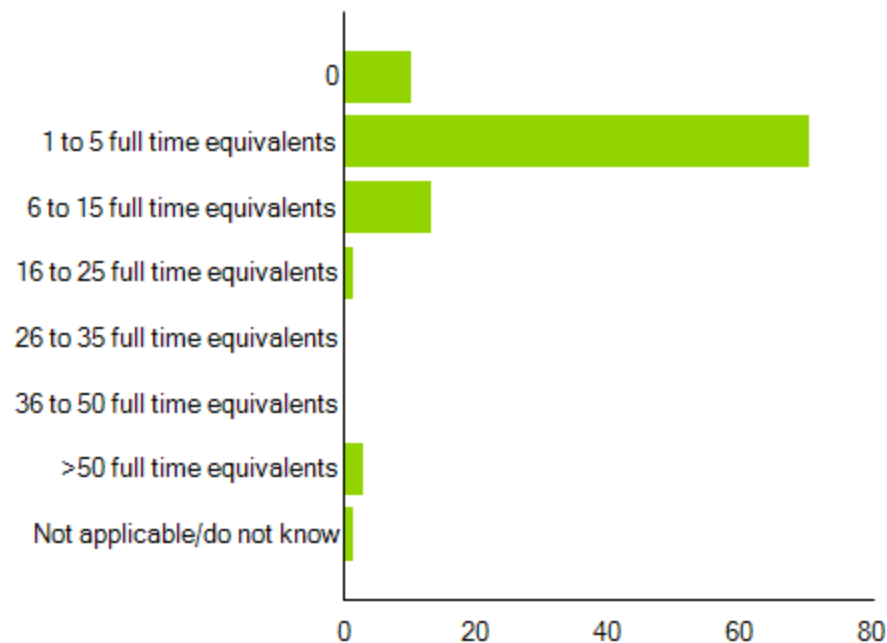
Does your organization have a documented and approved information security strategy?



Número de profesionales dedicados a la Seguridad de la Información.

La mayoría de las organizaciones (71%) reportaron una planta de 1 a 5 profesionales dedicados a seguridad de la información tiempo completo.

How many information security professionals does your organization have who are dedicated to information security?



Principales Hallazgos

2. Los encuestados reconocen que las personas (incluyendo terceras partes) son aún el eslabón más débil, sin embargo todavía es muy pequeño el foco en conciencia de la seguridad y entrenamiento

A pesar del hecho de que más infracciones se originan externamente que internamente, los encuestados siguen teniendo más **confianza en como se están combatiendo las amenazas externas.**

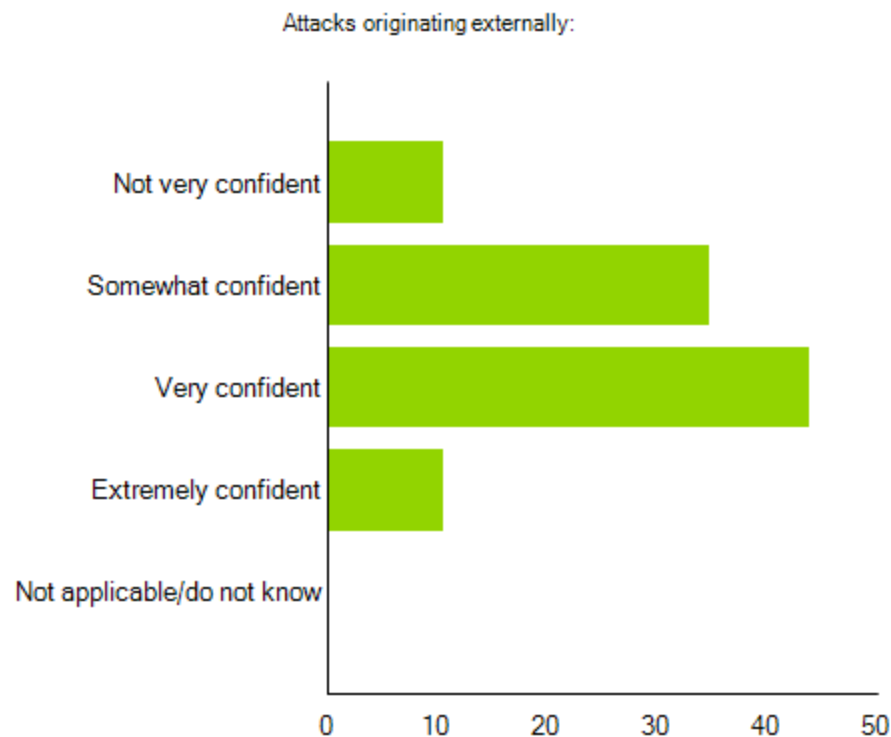
A pesar de este hallazgo, el manejo de las **amenazas internas** recibió una clasificación **baja** dentro de las **primeras iniciativas de seguridad** de su organización para 2009.

Debido a que la mayoría de las violaciones internas se producen como consecuencia de errores involuntarios y no de mala intención, algunas de las iniciativas que se deben considerar son;

Sensibilización y programas de entrenamiento
Iniciativas relativas a la confidencialidad de los datos
Gestión de los accesos privilegiados
Administración de los datos de producción

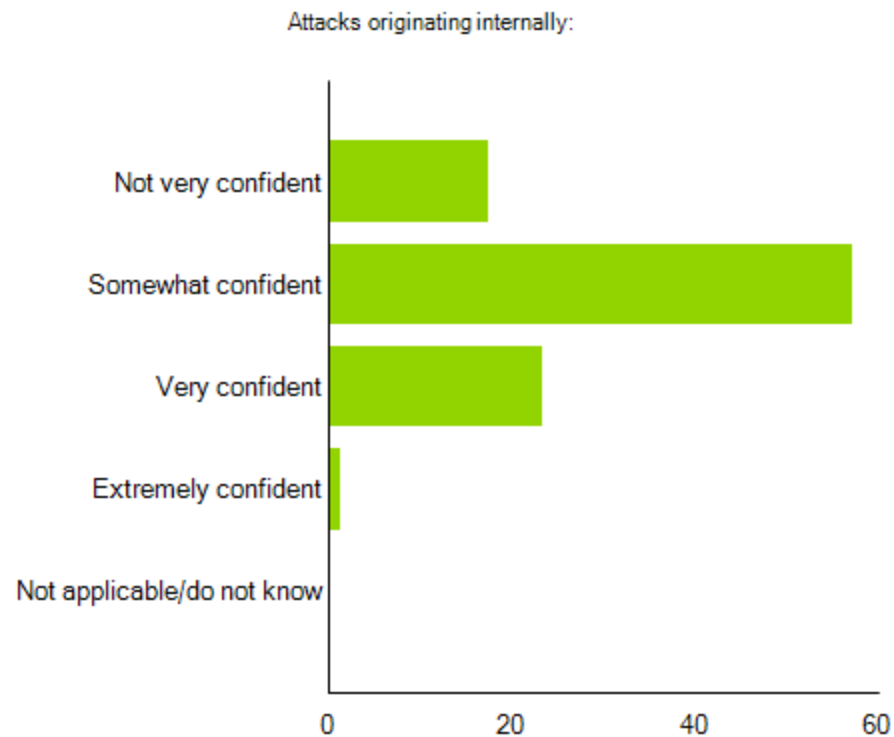
Nivel de confianza en protección de ataques Externos cibernéticos

Según el estudio, la mayoría de los encuestados (44%) creen que sus organizaciones están bien protegidas contra ataques externos relacionados con los sistemas de información. Otro 35% están sólo un poco confiados.



Nivel de confianza en protección de ataques Internos cibernéticos

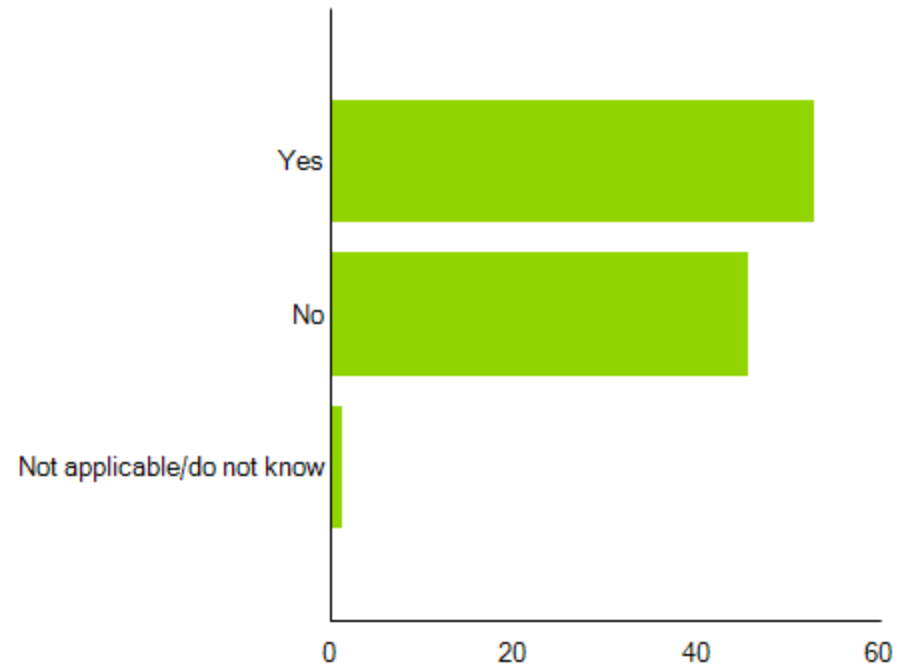
Según el estudio, el 24% de los encuestados está muy seguro de que su organización está protegida contra los ataques internos que envuelven los sistemas de información. Otro 57% está un poco confiada, lo que indica que las organizaciones están preocupadas por los ataques de origen interno.



Entrenamiento de los empleados en identificación y reporte de actividades sospechosas.

La mayoría de los encuestados (53%) afirman que entrenan a sus empleados para identificar y reportar actividades sospechosas. Sin embargo, muy cerca de ese porcentaje (46%) informan que no lo hacen.

Does your organization train employees to identify and report suspicious activities?



Principales Hallazgos

3 .La continuidad del negocio y la recuperación de desastres se está tornando prioritaria.

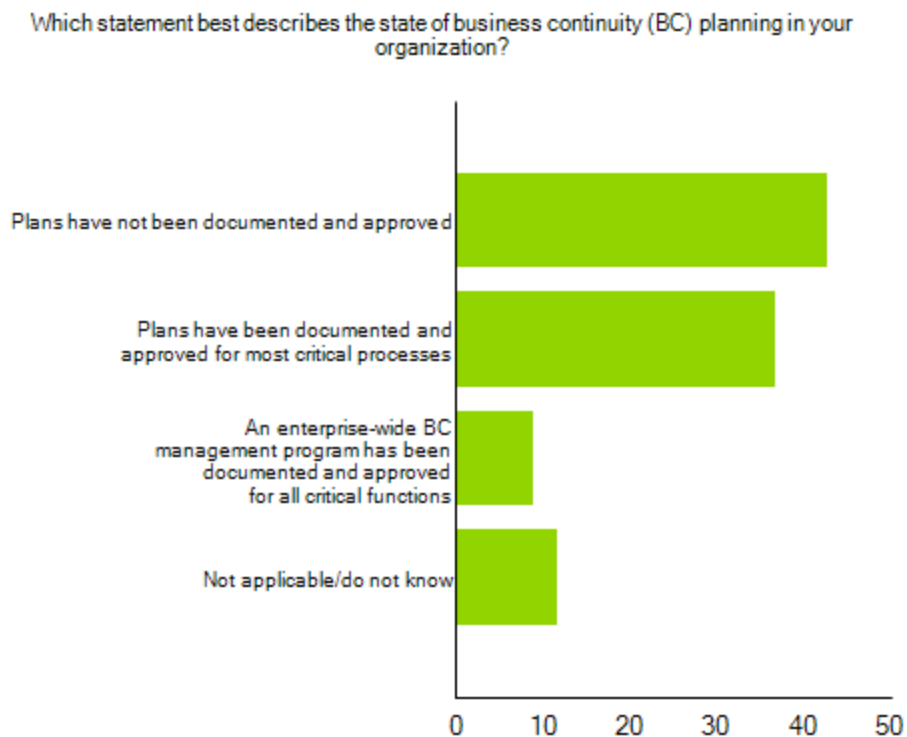
La **continuidad del negocio y recuperación de desastres** desde hace mucho tiempo sólo recibían una atención superficial en las organizaciones de Consumer Business. Sólo el 9% de las organizaciones tienen un **plan de continuad del negocio documentado y aprobado** para todas las funciones críticas.

Sin embargo, no es un punto con el que los encuestados están satisfechos. La recuperación de desastres es la segunda iniciativa de seguridad más mencionada para el 2009.

Las organizaciones de Consumer Business están reconociendo que los desastres pueden ocurrir en cualquier momento y que una adecuada preparación para imprevistos es un factor importante en su continua viabilidad comercial.

Estado del plan de continuidad del negocio

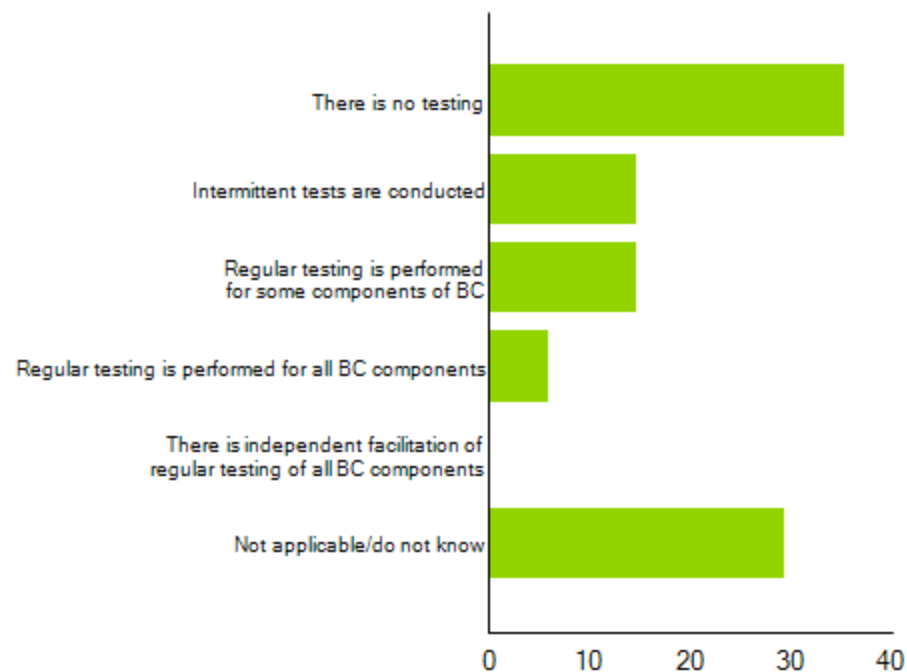
La continuidad del negocio y recuperación de desastres actualmente reciben poca atención. Sólo el 9% de las organizaciones tienen un plan corporativo relacionado con la continuidad de negocio documentado y aprobado para todas las actividades críticas. La gran mayoría de los encuestados (80%) conforman el grupo de los que afirman que los planes no han sido bien documentados y aprobados (43%), o no han sido documentados y aprobados para las funciones más importantes (37%).



Frecuencia de las pruebas de continuidad de negocio

El mayor porcentaje de los encuestados (35%) admite que no hay pruebas de ningún tipo con respecto a la continuidad del negocio, mientras que el 29% afirma que no tenían conocimiento o la pregunta no es aplicable. Pruebas esporádicas y pruebas regulares sobre algunos de sus componentes sólo representan el 30% de las respuestas. Únicamente el 6% podría afirmar que tienen definidos unos procedimientos de pruebas regulares para todos los componentes de continuidad del negocio.

What is the frequency of testing with regard to business continuity (BC) in your organization?

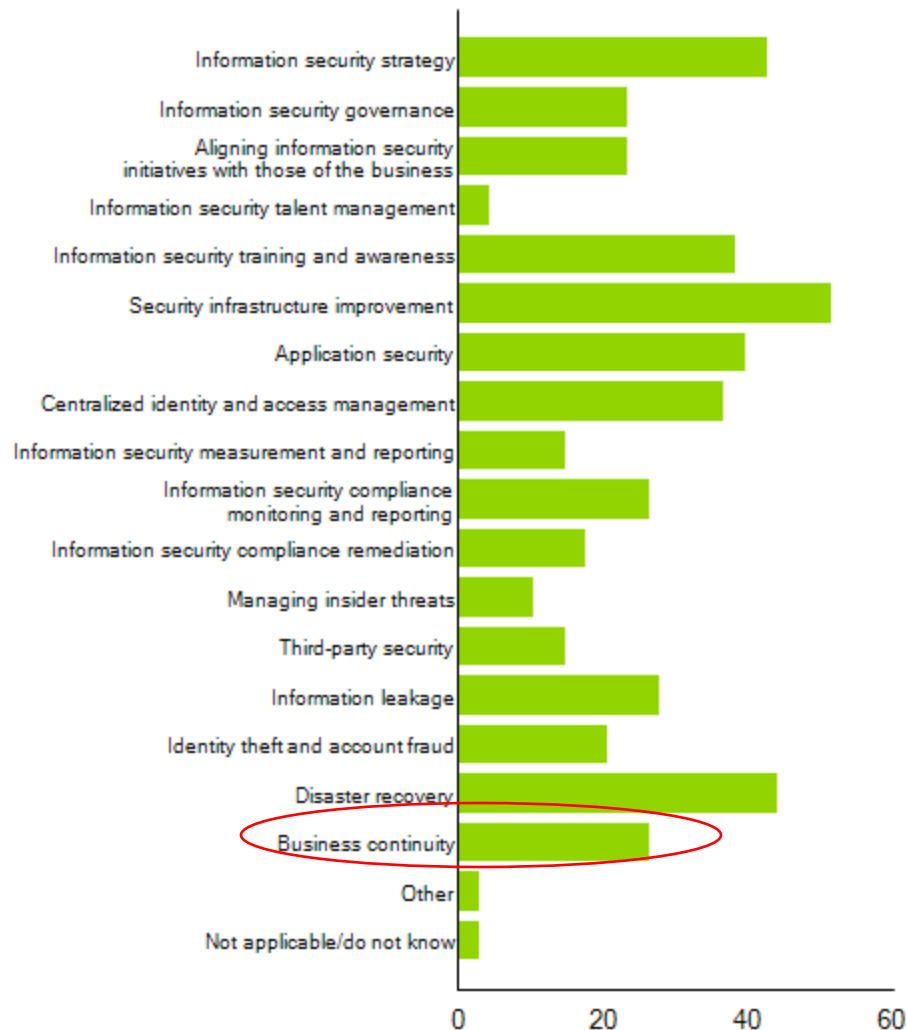


Principales iniciativas de Seguridad para el 2009

Las mejoras a la infraestructura de Seguridad tomaron el primer lugar en 2009 con el 51% de los encuestados tomando esta elección.

La recuperación de desastres en un cercano segundo lugar (44%), seguido por la estrategia de seguridad de la información (43%), seguridad de aplicaciones (40%), y la capacitación en seguridad de la información y sensibilización (38%).

What are your organization's top five security initiatives for 2009?



Principales Hallazgos

4. Los negocios de Consumer Business, tienen una visión “Adopción tardía” cuando hablan de tecnologías de seguridad

La mayoría de los encuestados afirman que aplican una estrategia de **“Adopción tardía”** para las **tecnologías de seguridad**. La tecnología sobre hardware antiguo y tecnología obsoleta pone en riesgo los **datos de los clientes**.

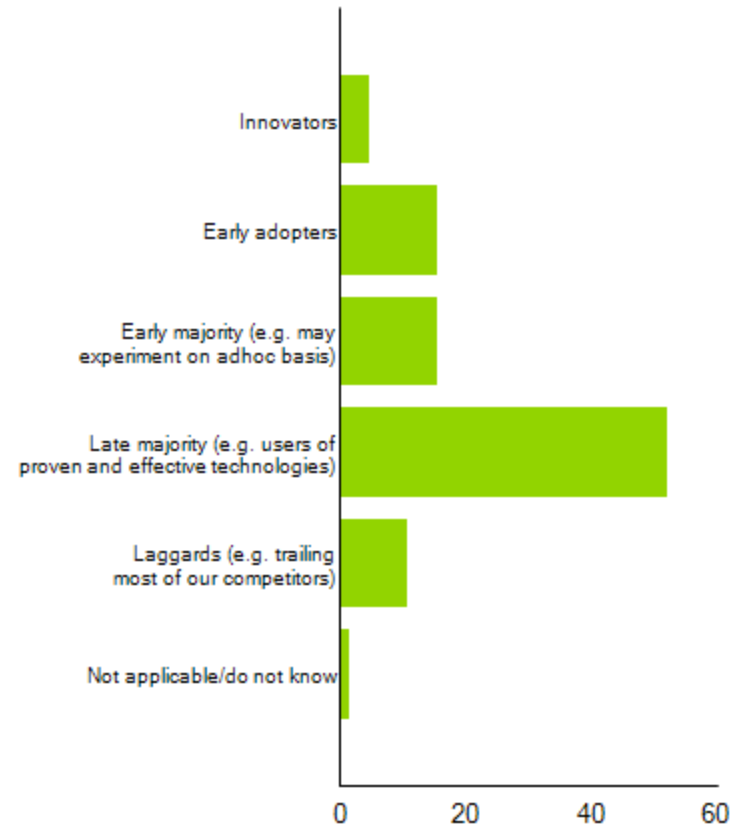
El riesgo de **pérdida de datos de clientes** se está convirtiendo en algo habitual para los negocios de Consumer Business debido al esfuerzo por desarrollar, mantener y aumentar **reconocimiento de marca y lealtad de los clientes**.

Los negocios Consumer Business deben considerar hacer una evaluación de esta estrategia debido a que se relacionan directamente con el consumidor.

Adopción de las tecnologías de seguridad

Para la gran mayoría de los encuestados (52%), caracterizan su adopción de la tecnología como una "Adopción tardía", es decir que son usuarios de tecnologías cuya eficacia está probada.

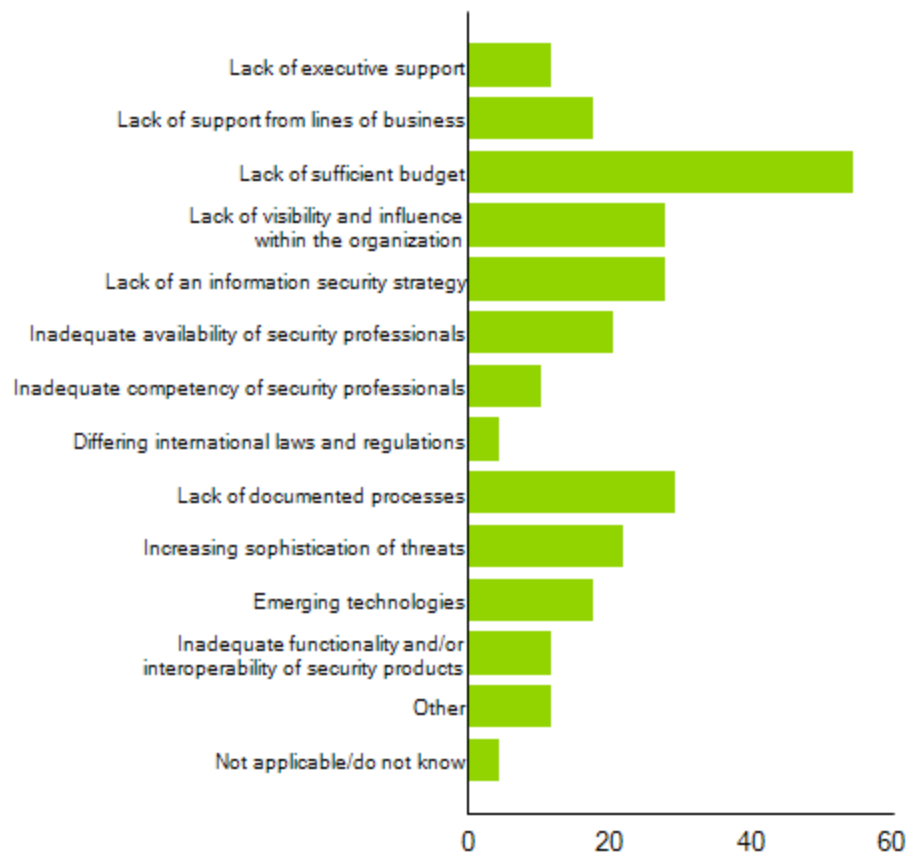
Which of the following categories best describes your organization's adoption of security technology?



Los mayores obstáculos para garantizar la seguridad de la información

Los dos obstáculos mencionados con más frecuencia para garantizar la seguridad de la información son la falta de presupuesto suficiente (54%) y la falta de procesos documentados (29%).

What major barriers does your organization face in ensuring information security?



Principales Hallazgos

5. Los presupuestos en seguridad fueron golpeados en el 2009

Igual a la queja de casi todas las industrias en 2009, "**la falta de presupuesto suficiente**" es el obstáculo más mencionado por la mayoría de los encuestados.

La mayor parte del presupuesto global de TI dedicada a la seguridad de la información es de **1-3%**

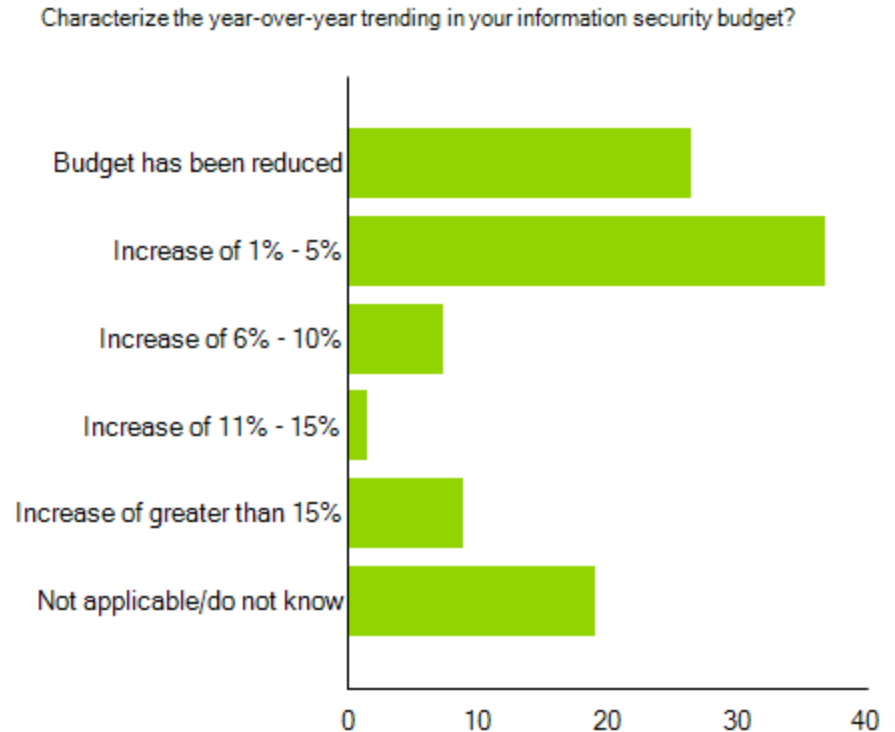
Los encuestados indican que mientras que la **inversión en seguridad** sigue una tendencia **levemente ascendente**, un alto número de encuestados han sufrido **reducciones en sus presupuestos**.

Tiempos de recesión resultan en desafíos excepcionales. Para consumidores: excelente época de rebajas. Para el negocio: se debe reforzar la seguridad pero con presión de reducir costos.

Impulsar la seguridad es crucial en tiempos de recesión debido a la reducción del personal y la exigencia de hacer más con menos.

Tendencias en el presupuesto de seguridad año tras año

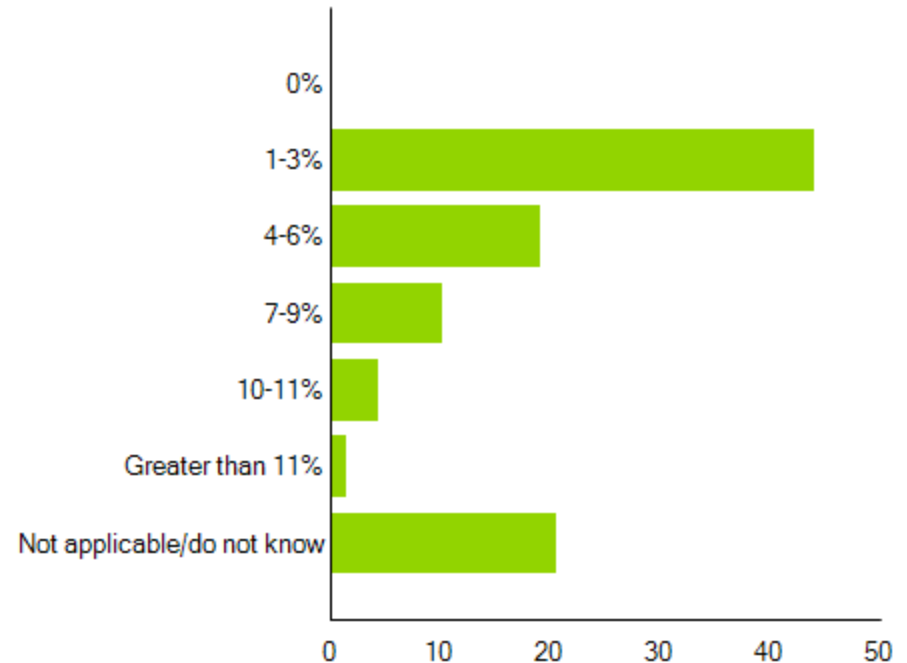
Mientras que la inversión en seguridad continúa con una tendencia levemente ascendente, (37% indicó un incremento entre 1% y 5%), un número alto de encuestados ha sufrido una reducción en su presupuesto (26%)



Gastos relacionados con seguridad de la información como un porcentaje del presupuesto total de TI

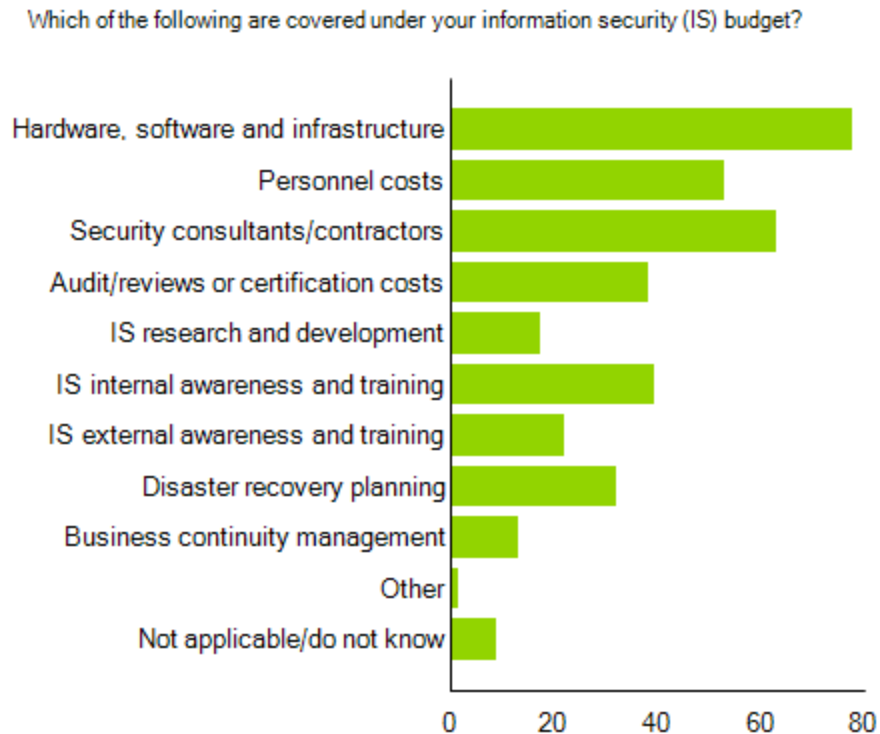
El mayor porcentaje de los encuestados (44%) indican que el menor porcentaje del presupuesto de TI (1-3%) es dedicado a la seguridad de la información. Esto es coherente con la conclusión de que los presupuestos de seguridad no están a la par, porque la seguridad no está recibiendo un porcentaje lo suficientemente alto del presupuesto general de TI.

What percentage of your organization's overall IT budget is dedicated to information security?



Segmentación del presupuesto de seguridad de la información

78% de los encuestados indican que el hardware, software e infraestructura son cubiertos por el presupuesto de seguridad de la información, con los consultores de seguridad y contratistas (63%) y costos de personal (53%) como los siguientes grandes gastos.



Deloitte.

© Deloitte & Touche LLP and affiliated entities.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.