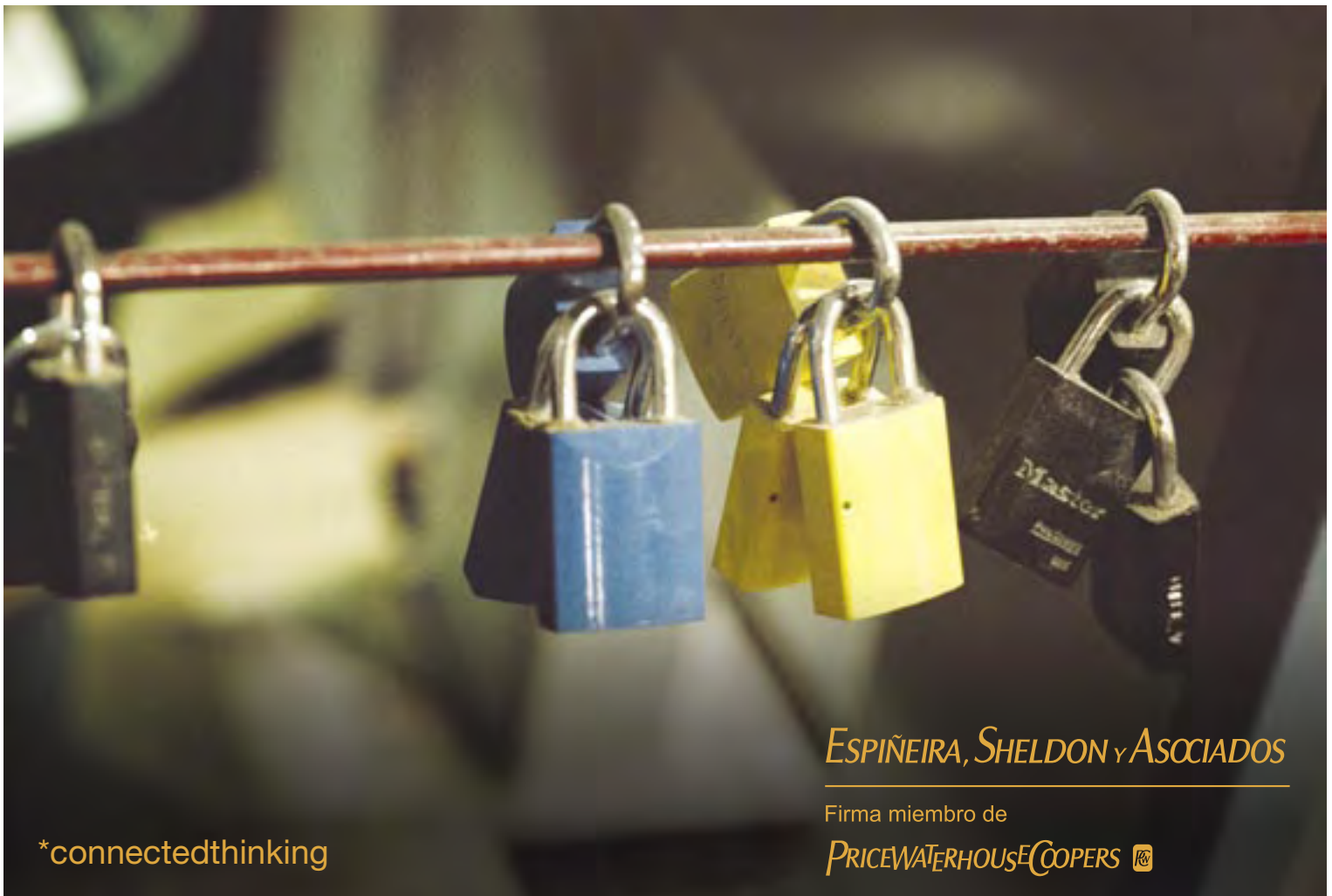


# Prácticas de Seguridad de Información de las empresas en Venezuela\*

Encuesta Nacional 2006 - 2007



*ESPIÑEIRA, SHELDON Y ASOCIADOS*

Firma miembro de

*PRICEWATERHOUSECOOPERS* 

# Introducción

Estamos participando de un cambio paradigmático en la relación de la organización de Tecnología de Información con sus usuarios, que es reflejo de nuevos enfoques sobre cómo la tecnología debe alinearse hacia el servicio.

Esta visión integrada de servicio exige que prevalezca el enfoque gerencial sobre la respuesta técnica cuando el negocio busca el apoyo de la organización de Tecnología de Información. Para que este nuevo enfoque funcione apropiadamente, se hace necesario que la Seguridad de Información alcance tres objetivos fundamentales:

- Avanzar de un enfoque reactivo de gestión, hacia el establecimiento de estrategias y planes de corto, mediano y largo plazo.
- Lograr una reducción efectiva del esfuerzo en Seguridad de Información por la atención y resolución de situaciones cotidianas, en función de enfocarse en el aporte de valor al negocio.
- Incorporar el enfoque de servicio en la gestión de la Seguridad de Información.

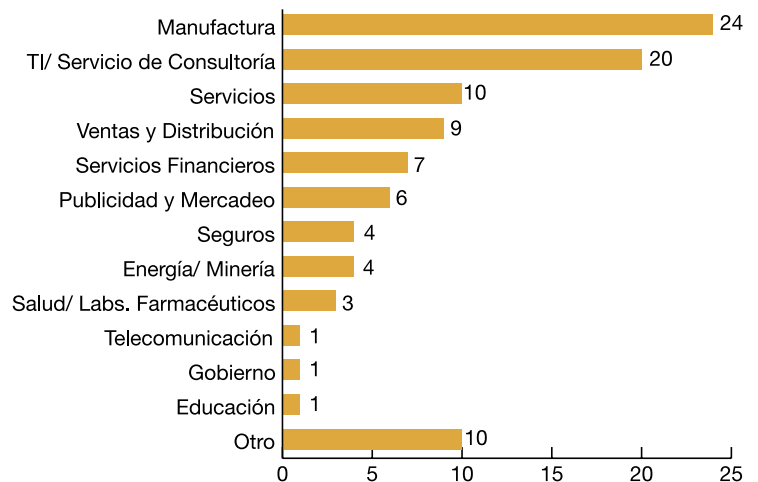
Esta encuesta del año 2007 sobre las “Prácticas de Seguridad de Información de las empresas en Venezuela” elaborada por Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers, se ha desarrollado por tercer año consecutivo, contando en esta edición con el apoyo técnico de la empresa Tendencias Digitales. En esta edición participaron empresas a nivel nacional, abarcando diversos sectores económicos de las grandes, pequeñas y medianas empresas, con un marco muestral que incluye el nivel gerencial de las empresas encuestadas.

## Ficha técnica

En la presente encuesta sobre las “Prácticas de Seguridad de Información de las empresas en Venezuela”, participaron 436 empresas de Venezuela, ubicadas en diversos sectores de la actividad económica, representadas en la Figura N° 1, mediante dos instrumentos con enfoques específicos de penetración: La encuesta Ómnibus Empresarial, desarrollado en conjunto con la empresa Datanalisis y una encuesta ad-hoc a empresas clave de los diferentes sectores del país.

En la muestra de empresas encuestadas predomina el sector de manufactura [24%] y Tecnología de Información / Servicios de Consultoría [20%], destacando igualmente los sectores Servicios y Venta y Distribución.

**Figura N° 1: Distribución de las empresas participantes por sector - % de respuestas**

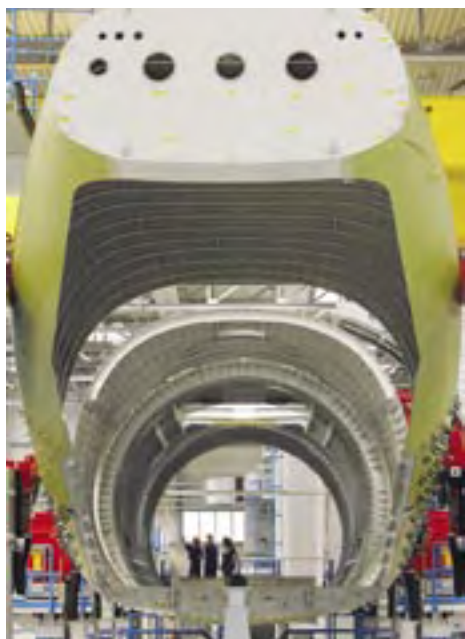
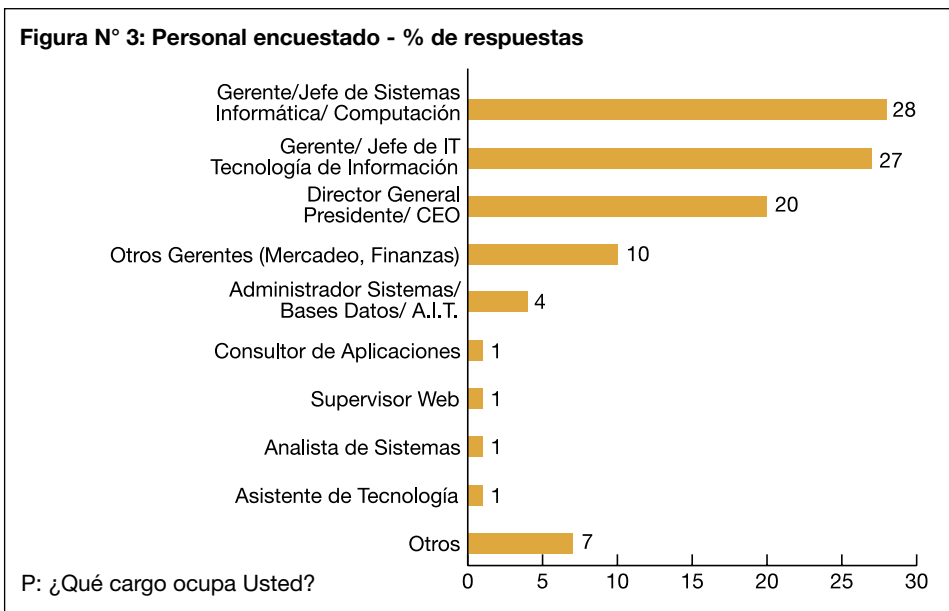
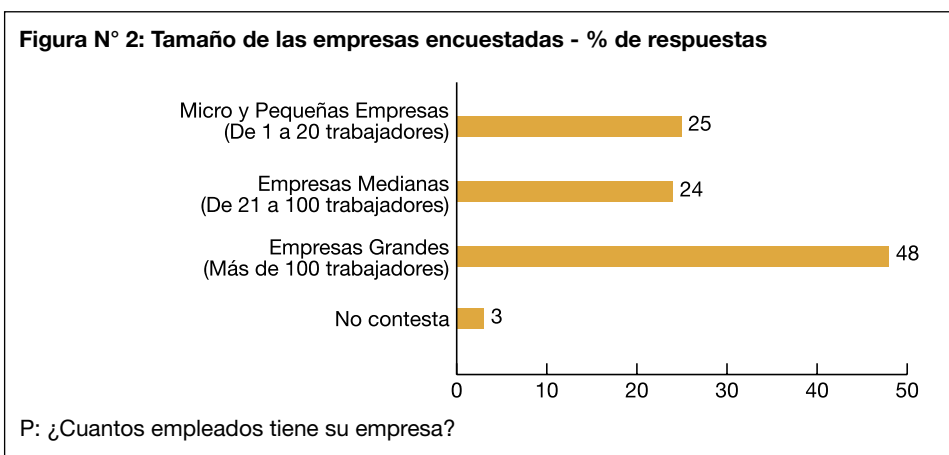


P: ¿En qué sector de negocios se ubica su empresa?

En esta encuesta se incorporó la identificación del tamaño de las empresas encuestadas, en función de analizar las tendencias en seguridad de información por sector. El resultado este año 2007 fue una participación de 48% de empresas con más de 100 trabajadores, consideradas como grandes empresas, y como novedad de esta edición se hizo énfasis en la incorporación de la Pequeña y Mediana Empresa (Pyme), alcanzando una participación de 49% de la base de encuestados, según la distribución que se muestra en la Figura N° 2.

En la mayoría de los casos, las personas entrevistadas ocupan cargos relacionados con Tecnología de Información y altos niveles de las organizaciones participantes, concentrando estos cargos el 75% de los encuestados (ver Figura N° 3).

Este resultado permite confiar que la visión de la práctica de Seguridad de Información en Venezuela que se presenta en esta encuesta, corresponde a la perspectiva de los principales responsables de la toma de decisiones en esta materia.



### Secciones de la encuesta

La presente encuesta se ha dividido en cuatro secciones en correspondencia con la estructura de nuestras encuestas en años anteriores:

- I. Penetración de las Estrategias de Seguridad de Información
- II. Estrategias de Seguridad de Información
- III. Brechas de Seguridad de Información
- IV. Controles de Seguridad de Información

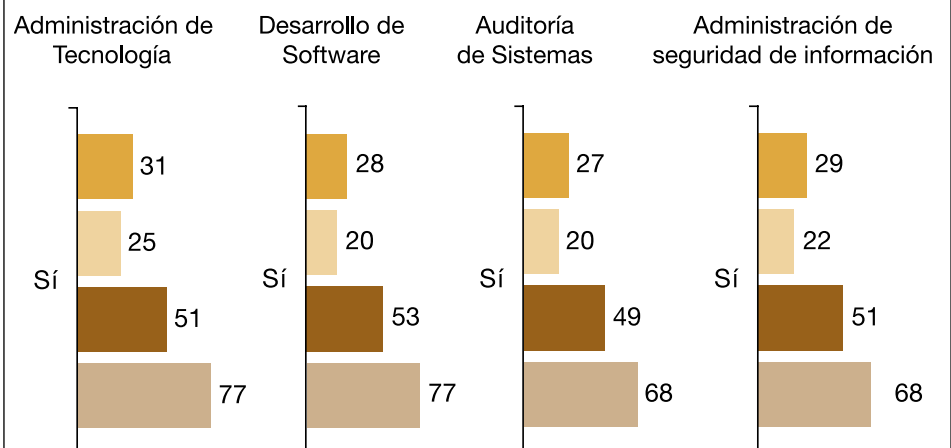
# Sección I: Penetración de las Estrategias de Seguridad de Información

Esta sección de la encuesta busca medir el grado de importancia que las empresas encuestadas otorgan a la Seguridad de Información.

## Existencia de funciones relacionadas con TI y SI dentro de las empresas

La relación entre la presencia de personal para las funciones de Tecnología de Información, Desarrollo de Software, Auditoría y Seguridad de información y el tamaño de la empresa es proporcional. Sin embargo, encontramos que la existencia de funciones de Auditoría y Seguridad de Información se presenta en la mitad de la Mediana y Gran Empresa encuestada. Llama la atención también que la Pequeña Empresa mantiene una proporción similar entre estas cuatro funciones, replicando proporcionalmente el comportamiento de los otros grupos.

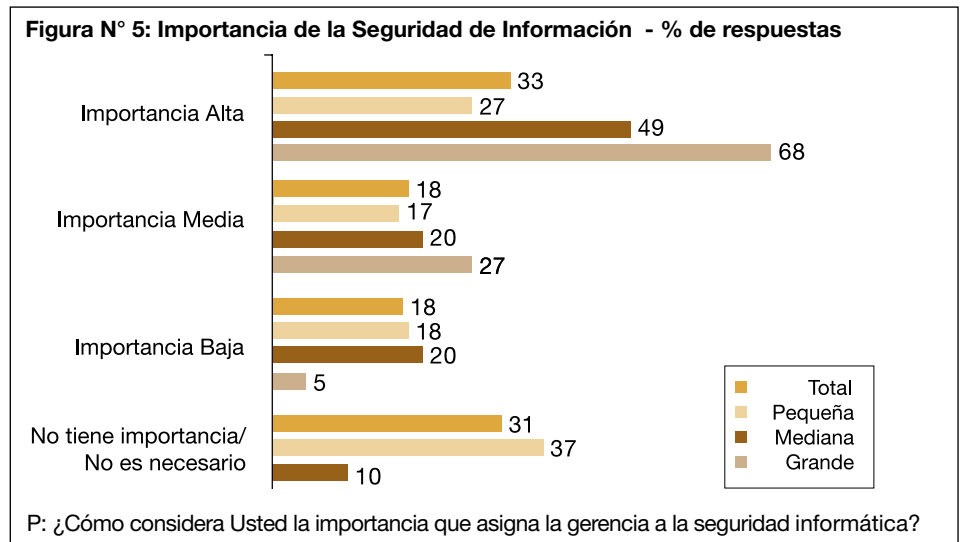
**Figura N° 4: Funciones de Seguridad de Información en las empresas encuestadas (% de respuestas)**



P: Dentro de la empresa. ¿Cuenta con personal que se ocupe de las siguientes funciones?

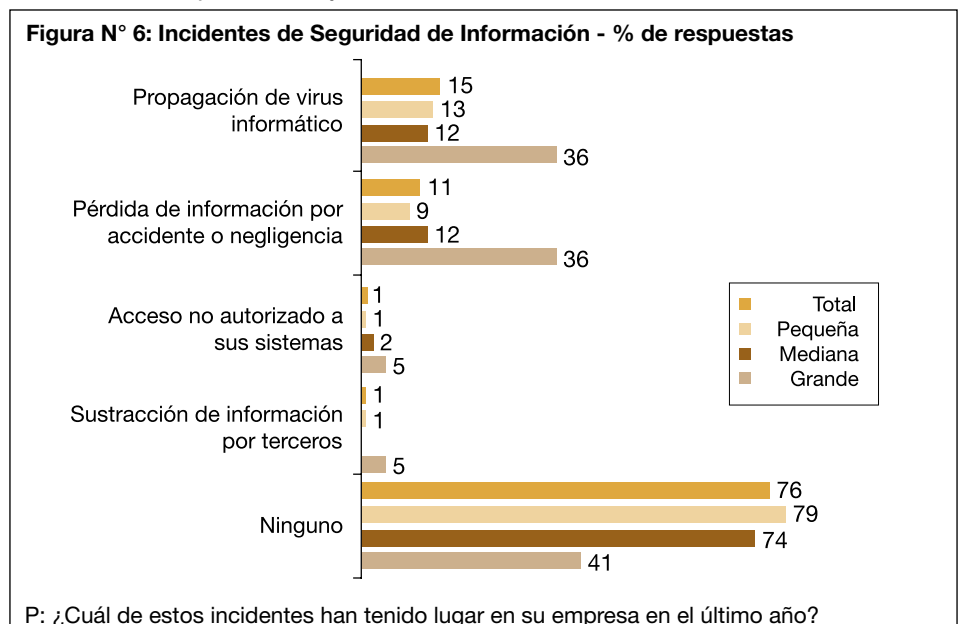
### Importancia de la Seguridad de Información

La Seguridad de Información es altamente importante para el 33% de las empresas encuestadas, existiendo una diferencia notable entre la Pequeña Empresa y el resto, siendo consistente esta postura con la presencia de funciones expresada en la Figura N° 4. También se puede notar en la Figura N° 5 que en la Pequeña Empresa, existe un 37% de los encuestados que descartan absolutamente la importancia de este tema, lo cual evidencia posturas extremas en este sector, si lo contrastamos con el 27% en este grupo que lo consideró como importancia Alta.



### Incidentes de Seguridad de Información que se han presentado en el último año

Manteniendo su nivel de incidencia como principales eventos, la propagación de virus informáticos y la pérdida de información por accidente o negligencia son los principales incidentes de Seguridad de Información que se han presentado en las empresas venezolanas en los últimos 12 meses; siendo esto más significativo para el sector de grandes empresas. En esta pregunta hubo una diferenciación significativa entre la Gran Empresa y el resto de los grupos, lo cual puede ser atribuido a que el impacto de este tipo de evento se incrementa exponencialmente según el número de usuarios de Tecnología de Información. En comparación con años anteriores, este incidente se incrementó en cinco (5) puntos porcentuales, lo que denota que las tendencias en el desarrollo de malware más complejo y sofisticado ha superado los esfuerzos en implantación y actualización de soluciones anti-virus.



# Sección II: Estrategias de Seguridad de Información

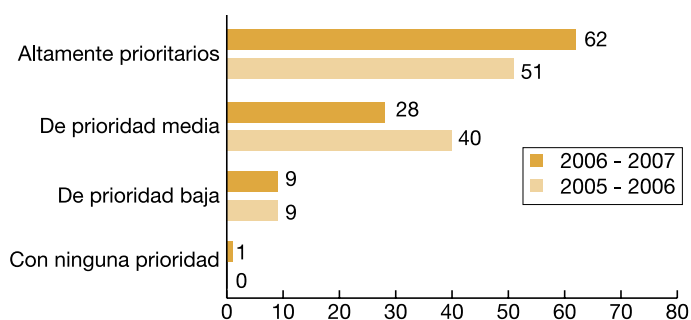
Esta sección de la encuesta trata sobre las acciones que han implementado las empresas, en la búsqueda de garantizar la protección de la información, abarcando temas como:

- Desarrollo del plan estratégico de seguridad
- Conformación de la función de seguridad de la información y su efectividad
- Políticas y procedimientos de seguridad

## Prioridad de la Seguridad de Información

Para el 62% de las empresas encuestadas, la Seguridad de la Información es altamente prioritaria. Esto representa una variación en aumento con respecto al estudio del año pasado, en el cual la Seguridad de Información figuró como un asunto de alta prioridad para el 51% de las empresas encuestadas, y es consistente con el crecimiento que esta posición ha tenido en nuestras encuestas a lo largo de los años, y con la tendencia global.

**Figura N° 7: Prioridad de los tópicos de seguridad para la alta gerencia**  
% de respuestas

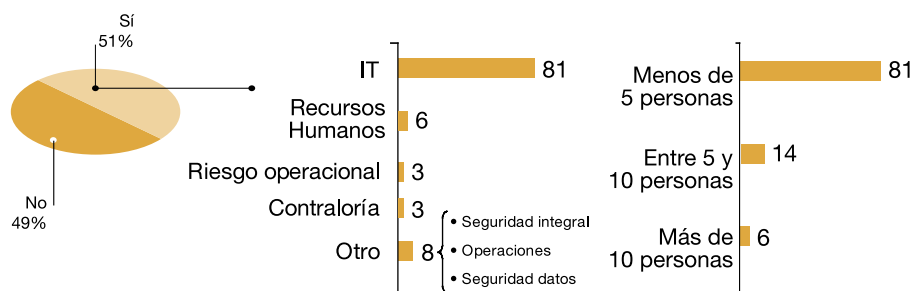


P: ¿Qué prioridad tienen los temas de Seguridad de Información para la Alta Gerencia?

## Función de Seguridad de Información

Dentro del grupo de Mediana y Gran Empresa participante de la encuesta se focalizó la indagación sobre la existencia, nivel de reporta y conformación de la función de Seguridad de Tecnología de Información. Como resultado de esta consulta, se identificó que en la mitad de las empresas encuestadas (51%) existe una estructura organizacional para este fin, concentrando un amplio 81% como unidad bajo la responsabilidad de la función de Tecnología de Información. También en un 81% de los casos, dicha unidad se encuentra conformada por un equipo de menos de 5 personas, manteniéndose esta cifra similar con años anteriores. Ver Figura N° 7.

**Figura N° 8: Definición y conformación de la función de Seguridad de Información en la empresa - % de respuestas**



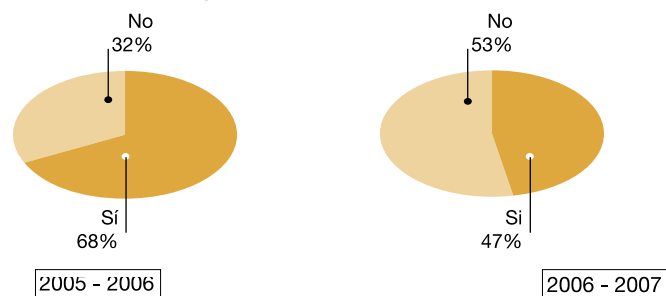
P: ¿Posee estructura que maneje SI?. ¿De quién depende?. ¿Cuántos la integran?

## Función de Seguridad de Información

### Continuación

El 47% de las empresas que poseen una estructura organizacional de Seguridad de Información han definido indicadores de desempeño para medir la efectividad de esta función. La creación y seguimiento de indicadores de gestión permite a las organizaciones establecer objetivos concretos, al exigir que deban ser medibles para efectos de establecer su cumplimiento en el tiempo. En términos generales, los principales indicadores utilizados están relacionados con el número de eventos reportados en materia de seguridad y número de vulnerabilidades identificadas en evaluaciones de seguridad. Es interesante encontrar que la comparación con respecto a nuestra encuesta del año pasado indica una reducción importante, probablemente relacionado con la maduración que ha tenido el mercado de Seguridad de Información, lo cual ha permitido establecer un mayor entendimiento sobre la función y efectividad de los indicadores.

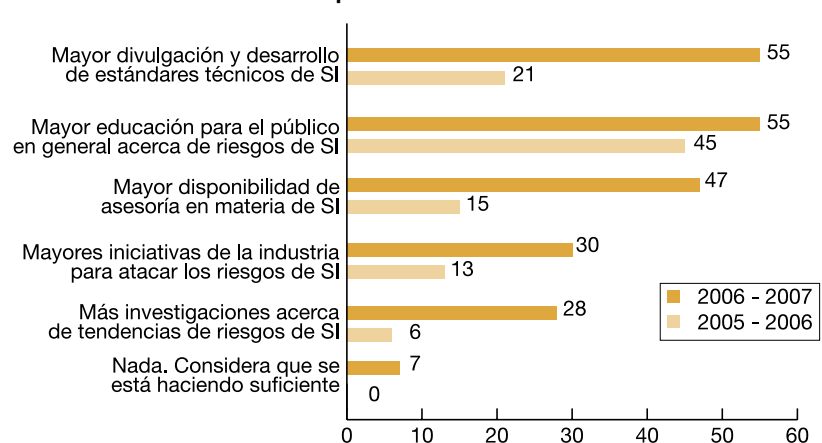
**Figura N° 9: Uso de indicadores de gestión para medir la efectividad de Seguridad de Información - % de respuestas**



P: ¿Posee indicadores de desempeño para medir la efectividad de SI?

Entre las principales consideraciones mencionadas por las empresas encuestadas para manejar con mayor efectividad los riesgos de Seguridad de Información se encuentran mayor divulgación y desarrollo de estándares técnicos de seguridad de información (55%), mayor educación para el público en general acerca de riesgos de seguridad de información (55%), y mayor disponibilidad de asesoría en esta materia (47%). En los tres renglones se registró un incremento en relación con el estudio realizado el año anterior. Este año, la divulgación sobre estándares presentó un notable incremento con relación al año anterior, lo que evidencia el interés de las organizaciones y apoyarse en mejores prácticas y establecer un parámetro de referencia en relación cómo abordar los retos que representa la Seguridad de Información.

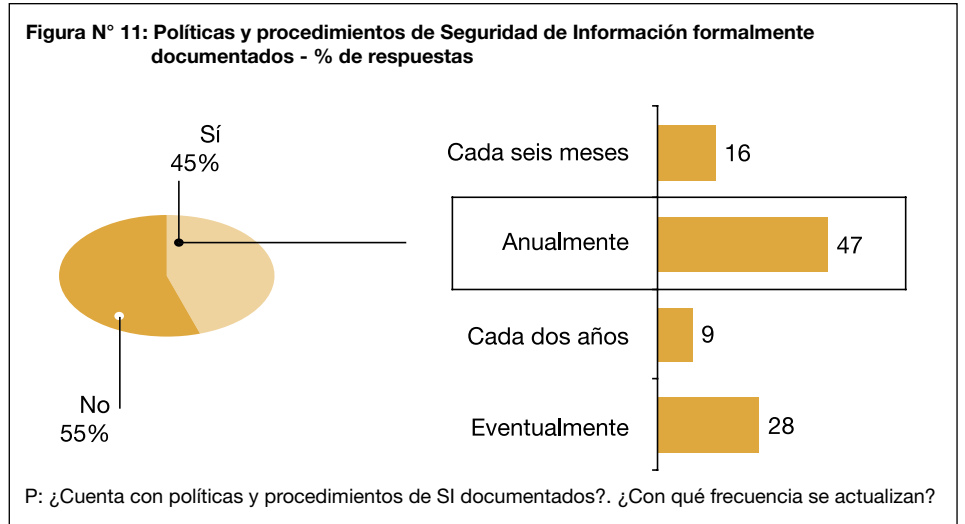
**Figura N° 10: Consideraciones para el manejo de los riesgos de Seguridad de Información - % de respuestas**



P: ¿Que le ayudaría, en el futuro, a manejar más efectivamente sus riesgos en SI?

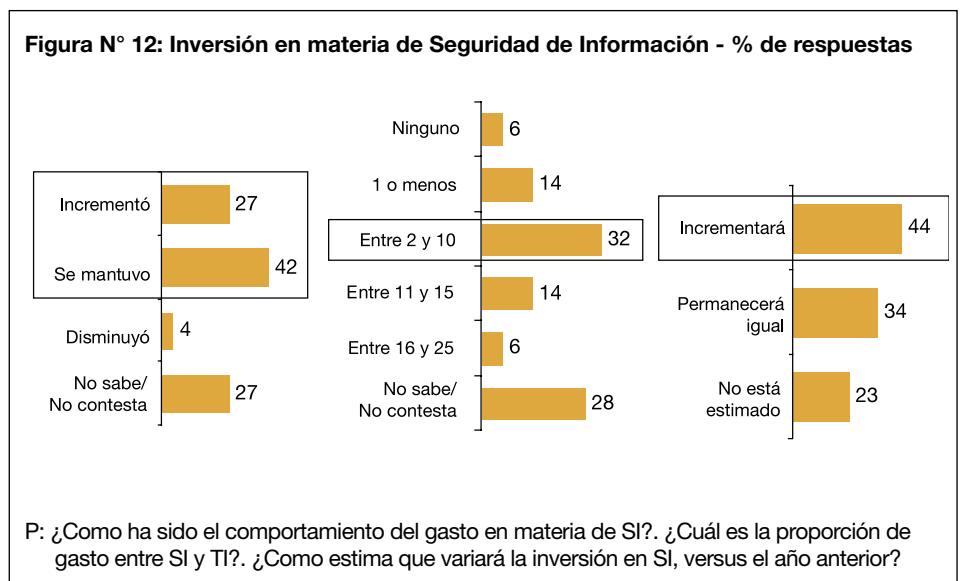
## Políticas y procedimientos de seguridad

El 45% de las empresas encuestadas manifiestan contar con políticas y procedimientos de Seguridad de Información formalmente documentados, que en su mayoría son actualizados anualmente. La documentación, divulgación y mantenimiento de políticas y procedimientos de Seguridad de Información son un elemento fundamental par el establecimiento a largo plazo de un entorno confiable para la gestión de la información del negocio.



## Inversión realizada en materia de Seguridad de Información

La inversión en materia de Seguridad de Información se mantuvo para el año 2006-2007 con una proporción entre 2% y 10% del presupuesto de tecnología de información para el 32% de las empresas encuestadas. El 44% de la muestra considera que la inversión en Seguridad de Información incrementará para este año. Al igual que el año anterior, las expectativas de incremento en el presupuesto de Seguridad de Información no se correspondieron con el incremento que efectivamente tuvo la función de Seguridad de Información.



## Obstáculos para la práctica de seguridad de activos de información en la empresa

Las empresas encuestadas consideran que los principales obstáculos que presenta la práctica de seguridad de activos de información son falta de cultura/adiestramiento de los usuarios (56%), restricciones de presupuesto (51%), falta de personal especializado en seguridad de información (42%) y falta de tiempo dedicado a seguridad de información (42%). Es importante destacar que la falta de cultura en materia de Seguridad de Información por parte de los usuarios, presenta una concentración muy alta en el grupo de grandes empresas, lo que refuerza el principio que la inversión en tecnología seguridad debe ir acompañada de planes de divulgación y concientización al personal sobre su responsabilidad en este tema.

**Figura N° 13: Obstáculos para la práctica de seguridad de activos de información en la empresa - % de respuestas**



P: ¿Cuáles son los principales obstáculos para la práctica de seguridad de activos de información?

Uno de los principales obstáculos que presenta la práctica de seguridad de activos de información es la falta de cultura/entrenamiento de usuarios (56%)

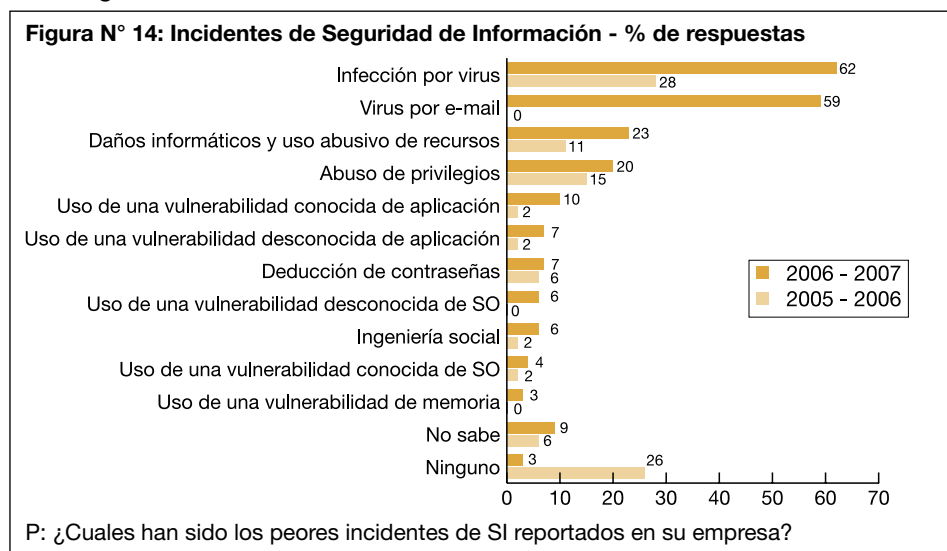
# Sección III: Brechas de Seguridad de Información

En esta sección de la encuesta se midió la ocurrencia y el impacto de las incidencias presentadas en materia de Seguridad de Información, el uso inadecuado de los recursos y sistemas de información, así como también los tipos de incidentes presentados y si estos se originaron dentro o fuera de las organizaciones.

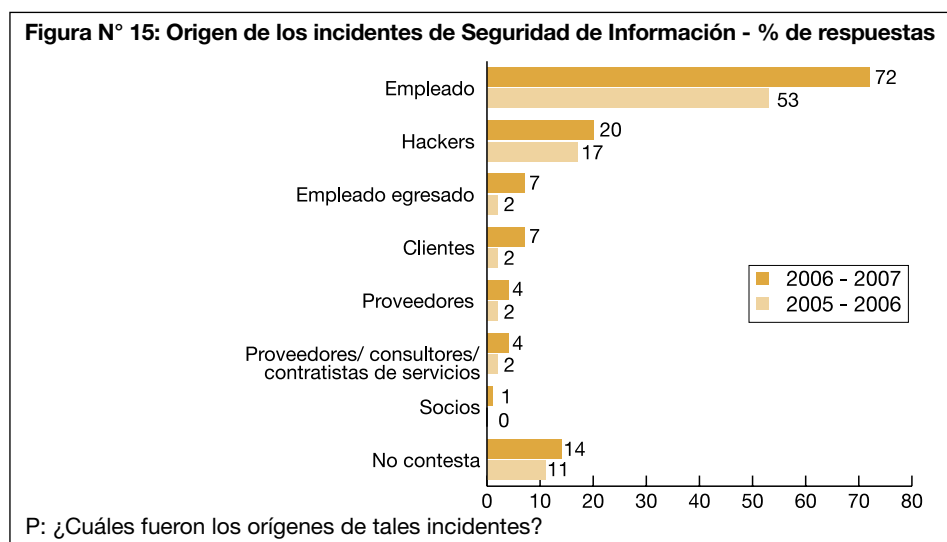
## Incidentes de Seguridad de Información que afectaron a las empresas

Las empresas encuestadas reportaron un incremento general de incidentes, y en particular en lo relacionado con infección por virus en relación con los resultados obtenidos el año pasado, y se corresponde con resultados en mediciones similares a nivel internacional. Otro dato importante en esta pregunta es el incremento de las incidencias relacionadas con el uso abusivo de recursos y el abuso de privilegios.

En esta pregunta hubo una diferenciación significativa entre la gran empresa y el resto de los grupos, lo cual puede ser atribuido a que el impacto de este tipo de evento se incrementa exponencialmente según el número de usuarios de tecnología de información.



Si se analiza el origen de los incidentes de seguridad reportados, se observa que un 72% de los mismos ha sido causado por un empleado de la organización y un 17% por hackers. Comparando resultados con el período anterior, observamos que los empleados han incrementado como principal fuente de ataque, pero que la posibilidad de posibles atacantes también se dispersa hacia clientes, ex-empleados, proveedores y contratistas.

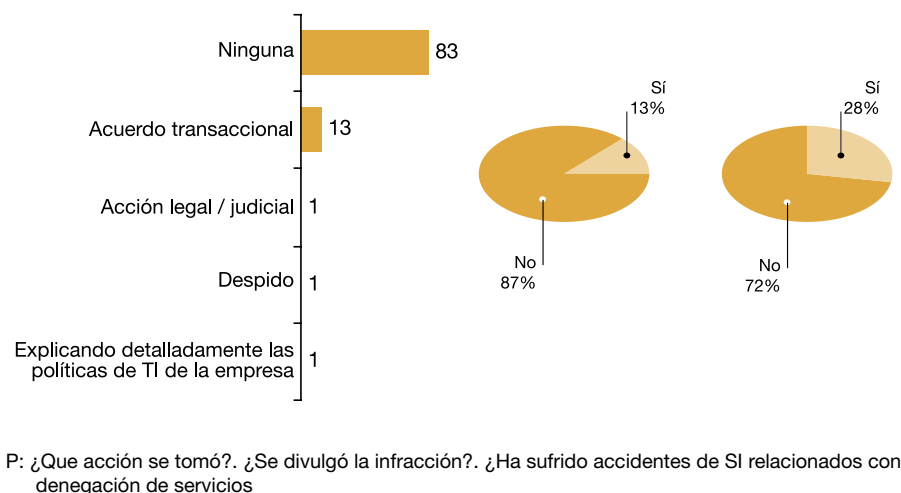


## Incidentes de Seguridad de Información que afectaron a las empresas

Continuación

El 83% de las empresas encuestadas que reportaron incidentes de Seguridad de Información no tomaron ninguna acción para sancionar a los individuos que provocaron dicho incidente. Adicionalmente, un 13% de las empresas que registraron estos incidentes divulgó públicamente la infracción detectada. Este resultado representa una involución con relación al año anterior, ya que se duplicó el número de empresas que manifestó no haber tomado acción al respecto. Este comportamiento está presente particularmente en la pequeña y mediana empresa, y puede estar promovida por los esfuerzos que representa para una organización de esas dimensiones impulsar sanciones o establecer procesos legales. Igualmente, un 28% de las empresas manifestó haber presentado un incidente relación con denegación de servicios.

**Figura N° 16: Acciones relacionadas con los incidentes de Seguridad de Información**  
% de respuestas



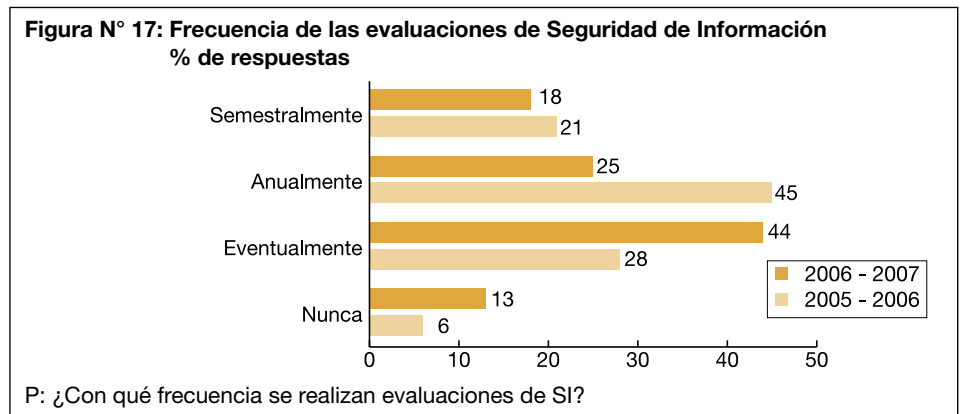
Si se analiza el origen de los incidentes de seguridad reportados, se tiene que un 72% de los mismos ha sido causado por un empleado de la organización

# Sección IV: Controles de Seguridad de Información

En esta sección de la encuesta se evaluaron los controles implementados por las empresas encuestadas, en relación a aspectos como perímetro de red y la definición de planes de Seguridad de Información orientados a la continuidad operativa del negocio.

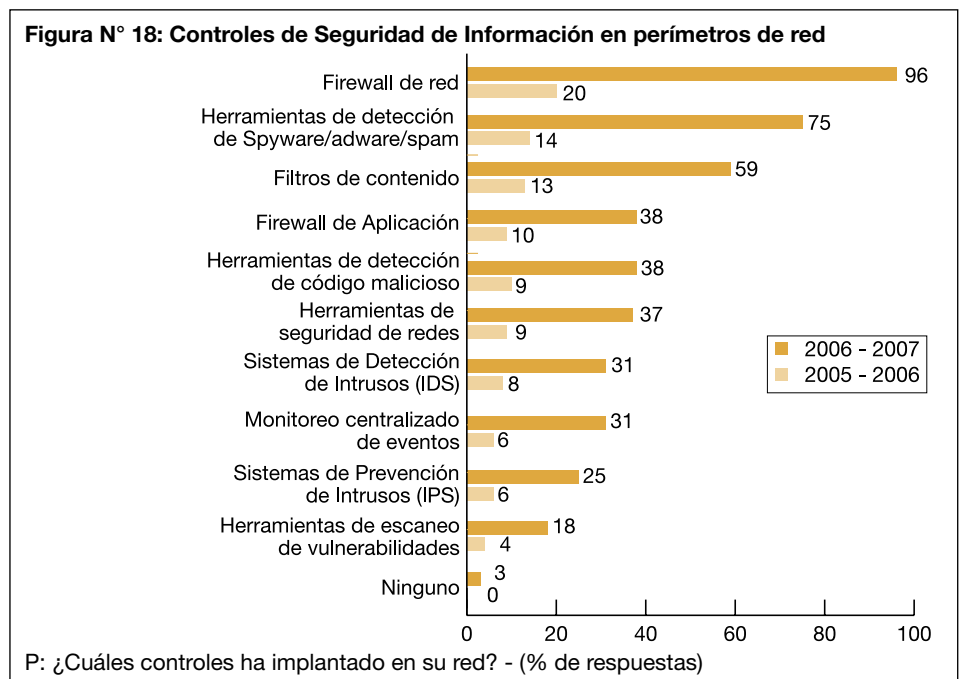
## Frecuencia de las evaluaciones de Seguridad de Información

El 44% de las empresas encuestadas afirma que las evaluaciones de Seguridad de Información en la empresa son realizadas eventualmente, mientras que un 25% ejecuta esta revisión anualmente. Esto representa una movilización de la práctica de evaluaciones anuales y semestrales hacia evaluaciones por demanda, lo que se considera una práctica inapropiada cuando los lapsos de evaluación superan tiempos prudentes de revisión, o no están ajustados a un plan integral de identificación y mitigación de riesgos. En concordancia con otros elementos identificados a lo largo de esta encuesta, son las grandes empresas las que se concentran en la respuesta de la ejecución de pruebas anuales.



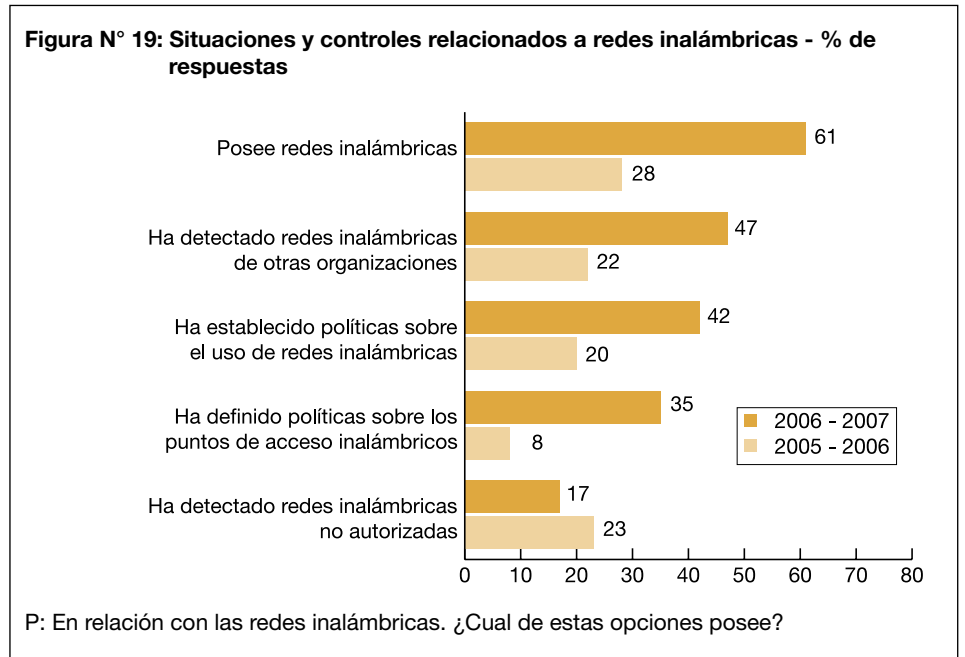
## Controles de Seguridad de Información implantados por las empresas en el perímetro de red

Los principales controles utilizados por las empresas encuestadas para la protección del perímetro de red de la organización son la implementación de firewall de red [96%], la adquisición de herramientas de Spyware, Adware y Spam [75%] y filtros de contenido [59%]. Como puede apreciarse en la Figura N° 18, este comportamiento se mantiene constante con relación al período anterior, y evidencia que los esfuerzos de las organizaciones siguen orientados hacia el atacante externo.

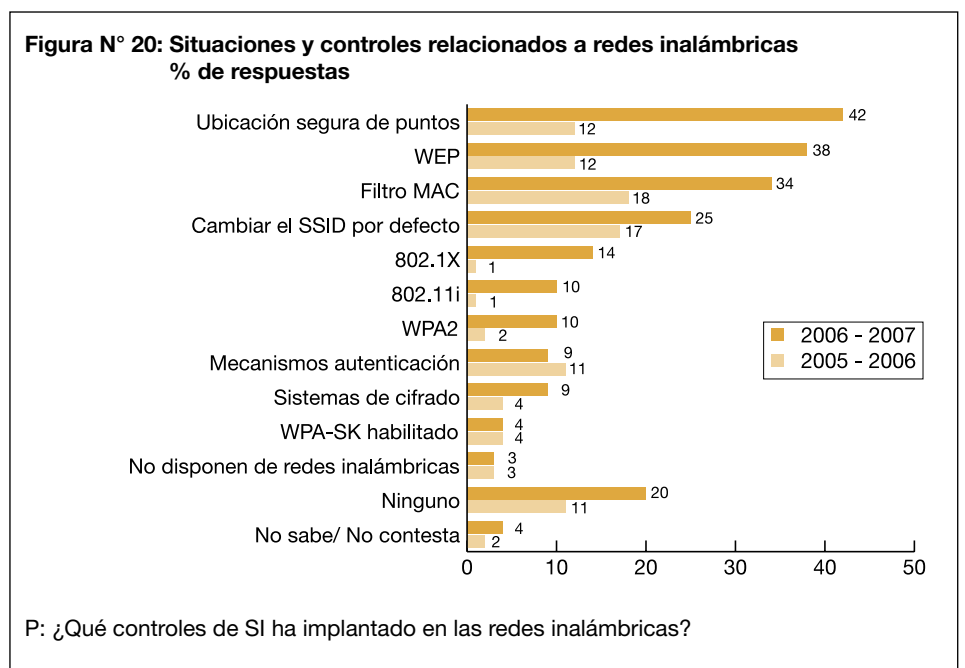


Situaciones relacionadas a las redes inalámbricas

Un 61% de las empresas encuestadas poseen redes inalámbricas en su organización, lo que representa un aumento con relación al período anterior, en tanto que un 47% de las empresas reporta haber detectado, dentro de su perímetro de red, redes inalámbricas pertenecientes a otras organizaciones. A diferencia del período anterior, existe una duplicación en la proporción de empresas que ha establecido políticas para el uso de este recurso (42%), y como consecuencia de esto, se evidencia una reducción significativa en el porcentaje de redes inalámbricas no autorizadas.



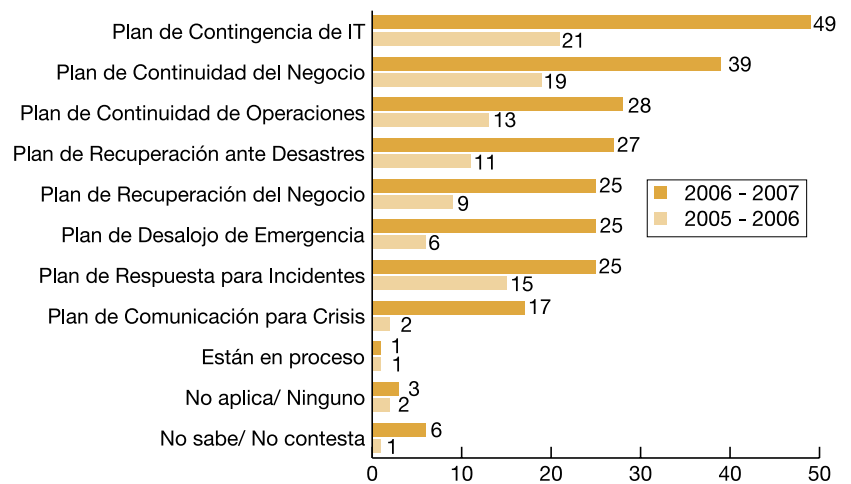
En relación con las medidas de seguridad establecidas, observamos un incremento leve en el establecimiento de controles alternos a la red inalámbrica como el uso de los estándares 802.1x y 802.11i, en tanto que la adopción de WPA2 se incrementa como opciones de protección para esta tecnología.



## Contingencia y continuidad de las operaciones

Un 49% de las empresas encuestadas tiene un plan de contingencia de Tecnología de Información, en tanto que 39% ha implementado un plan de continuidad del negocio. Como puede apreciarse en la Figura N° 21, la presencia de los principales tipos de planes se mantiene, en proporción con el período anterior, lo que evidencia que el interés en esta materia permanece. También en esta pregunta, observamos una concentración importante de la gran empresa entre aquellos que respondieron positivamente a esta pregunta.

**Figura N° 21: Planes de continuidad o contingencia definidos en las empresas**  
% de respuestas



P: ¿Cuales de los siguientes planes ha definido en su empresa?

# Quiénes somos

¿Quiénes somos?

Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers, es líder tanto mundial como nacional, en servicios de auditoría de estados financieros de empresas, asesoría fiscal, finanzas corporativas, así como en la gestión de riesgos de tecnología de información, procesos y sistemas operacionales por medio de nuestra línea de servicios de Asesoría Gerencial (Advisory).

En Asesoría Gerencial contamos con profesionales de variadas habilidades en diversas industrias y tecnologías. Esta diversidad de conocimiento y especialización nos permite asegurar que los recursos apropiados con el nivel requerido de experiencia son asignados a cada proyecto que realizamos.

Con la finalidad de brindar servicios innovadores y de alto valor agregado a nuestros clientes, mantenemos un programa constante de educación y actualización de nuestro personal, el cual incluye formación financiera y especializaciones en las tecnologías emergentes y de vanguardia.

Como Firma, hemos realizado un gran número de proyectos en clientes, entre las cuales podemos mencionar: Auditoría en fraudes de servicios electrónicos (Cajeros automáticos, Sistemas de atención telefónica (IVR), Servicio Maestro y Tarjetas de Crédito), definición del esquema de seguridad global, desarrollo de políticas, procedimientos y estándares de seguridad, revisión del riesgo tecnológico, definición de roles y privilegios en sistemas integrados, evaluación de controles en procesos y revisión de la seguridad en interfaces entre sistemas propietarios y sistemas integrados, elaboración y ejecución de pruebas de auditoría asistida por el computador, revisiones de seguridad de datos, estudios relacionados con seguridad, planes de recuperación y contingencia, auditorías de sistemas en desarrollo, servicios de apoyo para auditoría interna, proyectos de outsourcing de auditoría interna de tecnología de información, así como también asignaciones en las que implantamos soluciones en seguridad de datos y control interno.

Estos trabajos han sido desarrollados, según su aplicabilidad, en sectores de negocio como: Finanzas, Seguros, Petróleo y Petroquímica, Manufactura y Servicios.

## Security and Technology (ST)

En esta área se incluye el desarrollo e implantación de esquemas de seguridad en la plataforma tecnológica que apoyen las operaciones de la organización, así como también la identificación de brechas de seguridad que puedan utilizar intrusos internos o externos para acceder a la información o interrumpir la operatividad del negocio.

Algunos de nuestros servicios en ST son los siguientes:

### - Arquitectura de seguridad global

La tendencia tecnológica apunta a instalaciones cuyas arquitecturas son distribuidas por naturaleza. PricewaterhouseCoopers, reconociendo la necesidad de brindar una solución rentable que permita administrar y controlar la seguridad a nivel general, asiste a las organizaciones en el desarrollo, implantación y revisión de esquemas de seguridad que permitan minimizar en este momento y en el futuro, los riesgos en función a las estrategias del negocio.

## Security and Technology (ST) Continuación

### - Asesoría en el establecimiento de modelos de Gobernabilidad de TI

El negocio exige que la organización de tecnología establezca patrones de gestión adaptados a las exigencias de la organización, y el cumplimiento de normativas como la Ley Sarbanes-Oxley y la adopción de estándares de gestión como CobIT. Las estrategias de TI y las del negocio deben estar alineadas a los objetivos de la Organización, orientadas a la optimización de recursos tomando en cuenta que la calidad de los servicios de TI y sus proyectos deben adecuarse a las necesidades del negocio y culminarse en tiempo y dentro del presupuesto. Es allí donde nuestro apoyo a nuestros clientes en el establecimiento de un marco de gestión, permite avanzar hacia la conformación de una función de TI que represente un apoyo estratégico para el negocio.

### - Asesoría en la adopción de las mejores prácticas de gestión de TI, bajo el enfoque ITIL

ITIL (Information Technology Infrastructure Library) es un modelo para gestionar servicios de IT, que se enmarca en lograr niveles de eficiencia en la provisión, entrega y gestión de servicios a una organización, con sus infraestructuras y actividades correspondientes. ITIL ha sido adoptado como un estándar de facto por muchas empresas líderes, y en este sentido apoyamos a nuestros clientes en el desarrollo humano, implementación y evaluación de esquemas de gestión bajo este modelo.

### - Evaluación de roles y privilegios de acceso a procesos basados en la seguridad del sistema operativo y herramientas especializadas

La complejidad de las aplicaciones hoy en día requiere el establecimiento de privilegios de accesos a distintos niveles dentro de la plataforma tecnológica (Sistemas Operativos, Manejadores de Bases de Datos, Redes, etc). Esta situación puede dificultar el establecimiento de un modelo integral basado en roles para la totalidad de las aplicaciones dentro de la Organización. En este sentido, apoyamos a las organizaciones en la evaluación de los roles y privilegios de acceso definidos dentro de la plataforma tecnológica, con el objetivo de estandarizarlos.

### - Revisión y diagnóstico de seguridad

Los servicios de revisión y diagnóstico integral de seguridad de activos de información están diseñados para evaluar el ambiente de seguridad del cliente y además para ayudarlo a implantar controles que permitan mitigar los riesgos inherentes. Mediante este servicio podemos ayudar a las organizaciones a evaluar qué tan adecuados son los niveles de seguridad implantados en su Organización. Como resultado de esta revisión, se identifican los aspectos que requieren de mejoras potenciales, los cuales son jerarquizados, para luego desarrollar un plan estratégico de seguridad.

### - Desarrollo y evaluación de políticas de seguridad

Como parte de las funciones de administración de seguridad, deben documentarse, aprobarse y comunicarse formalmente las políticas, estándares y lineamientos que establecen las pautas de seguridad en la Organización, de forma tal que éstas apoyen el cumplimiento de las metas estratégicas de la gerencia y sus expectativas. Estas políticas deben ser independientes de la tecnología utilizada en los ambientes operativos. PricewaterhouseCoopers asiste a la Organización en el desarrollo y/o evaluación de las políticas de seguridad.

## Security and Technology (ST)

### Continuación

#### - Desarrollo y evaluación de estándares y procedimientos administrativos de seguridad

El diseño de una administración de seguridad integral en las diversas plataformas tecnológicas de una Organización, requiere desarrollar e implantar procedimientos específicos que permitan el cumplimiento de las políticas de seguridad y, a su vez, establezcan las actividades a ser realizadas por el personal con inherencia en el apoyo de la tecnología y en la administración de seguridad de la información.

#### - Desarrollo y evaluación de arquitecturas integradas de seguridad

Basados en los controles, estándares y los procedimientos anteriormente mencionados, PricewaterhouseCoopers asiste a las organizaciones en el desarrollo y evaluación de soluciones integradas para implantar controles e identificar alternativas de esquemas eficientes de seguridad para las diferentes plataformas tecnológicas. Esta infraestructura provee una metodología que permite identificar soluciones de control para ambientes operativos específicos y adicionalmente, permite evaluar el costo-beneficio de la implantación de controles en las aplicaciones basadas sobre el nivel de riesgos de las mismas.

#### - Estudios de penetración de seguridad

PricewaterhouseCoopers cuenta con una metodología para realizar estudios de penetración de seguridad, la cual es extremadamente efectiva para evaluar la seguridad alrededor de los sistemas de información. Este servicio está basado en pruebas para vulnerar la seguridad que provea un ambiente real, a efectos de disminuir los riesgos de acceso al sistema. Este servicio puede ser efectuado en dos modalidades distintas: El estudio de penetración interno donde se simula un ataque realizado por un usuario interno de la Organización, y el estudio de penetración externo donde se simulan ataques a la Organización por parte de usuarios en Internet.

#### - Revisión de seguridad en Internet

Como parte de nuestro servicio de revisiones de seguridad en Internet, ejecutamos un análisis profundo de las conexiones del cliente a la red Internet y los riesgos asociados a que personas ajenas a la Organización puedan acceder al sistema de su empresa mediante dicha red.

#### - Revisión de seguridad en redes

PricewaterhouseCoopers provee servicios de análisis para ayudar a identificar la conectividad de la red y los riesgos de acceso asociados. Para ello cuenta con metodologías y software especializados que garantizan la excelencia en el producto final.

#### - Desarrollo y evaluación del plan de contingencias de tecnología de información

La metodología de PricewaterhouseCoopers para el desarrollo y evaluación del plan de contingencia consiste en un grupo de servicios diseñados para ayudar a las organizaciones a desarrollar y revisar el conjunto de acciones que aseguren la continuidad de las actividades del negocio en caso de alguna contingencia tecnológica.

## Security and Technology (ST) *Continuación*

### - Revisión de seguridad en comercio electrónico (e-commerce)

Como parte de nuestros servicios a los clientes, realizamos evaluaciones en la infraestructura que apoya las operaciones de comercio electrónico (e-commerce). Este tipo de revisión siempre se orienta a las necesidades del negocio y a los más altos requerimientos de seguridad que este tipo de servicio debe poseer. Para ello, las revisiones de seguridad en Internet, redes, estudios de penetración y revisión y diagnóstico de seguridad complementan las revisiones específicas que este tipo de plataforma debe tener para verificar que exista un entorno seguro para el intercambio de datos involucrado.

### - Investigación de incidentes de seguridad

Como parte de nuestros servicios a los clientes, realizamos la investigación de incidentes de seguridad, haciendo uso de herramientas de auditoría forense, con el objetivo de tratar de determinar el origen y las causas de un determinado incidente.

### - Gestión de actualizaciones en la plataforma tecnológica

El mantener actualizada la plataforma tecnológica es de suma importancia, dada la gran cantidad de vulnerabilidad que son detectadas diariamente, las cuales pueden ser aprovechadas por usuarios no autorizados. PricewaterhouseCoopers presta servicios a sus clientes para la definición de esquemas centralizados de actualización.

### - Gestión de eventos de seguridad

Como parte de nuestros servicios a los clientes, apoyamos en el diseño y definición de esquemas centralizados de gestión de eventos de seguridad, para la estandarización y centralización de los procesos de monitoreo para los distintos elementos de la plataforma tecnológica.

### - Apoyo en el proceso de implantación de paquetes de Software

Como parte de nuestros servicios a los clientes, apoyamos en la identificación de requerimientos para la optimización de los procesos de negocio, diseño de sistemas, planificación de la implantación y negociación de contratos con proveedores de software, así como servicios de integración de sistemas.

### - Gerencia de datos

PricewaterhouseCoopers provee servicios de seguridad sobre las colecciones de datos y listados, así como servicios de control de calidad y procesamiento de sistemas (especificaciones, diseño, desarrollo e implantación).



[pwc.com](http://pwc.com)

© 2008. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. PricewaterhouseCoopers se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. \*connectedthinking es una marca registrada de PricewaterhouseCoopers.  
RIF: J-00029977-3