

Advisory

Prácticas de seguridad de activos
de información de las empresas
en Venezuela - 2004 *



ESPIÑEIRA, SHELDON y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 

Prácticas de Seguridad de Activos de Información en las empresas en Venezuela - 2004

Introducción

La seguridad de activos de información ha comenzado a tomar un lugar determinante en el mundo de los negocios, en particular en la gestión integral de riesgo, y se ha convertido en un elemento fundamental a ser considerado en toda estrategia organizacional con miras a lograr metas de negocio importantes a corto, mediano y largo plazo.

En consecuencia, las organizaciones experimentan la necesidad de definir estrategias efectivas que faciliten una gestión segura de los procesos del negocio, todo con el fin de darle mayor resguardo a la información, y al mismo tiempo adaptarse a los continuos cambios de la organización como consecuencia de las exigencias del mercado.

Tal necesidad ha impulsado la aparición de nuevos paradigmas en la administración del entorno de la Tecnología de Información (TI) y la gestión de la seguridad de activos de información. Sin embargo, existen interrogantes relacionadas con la manera de aplicar los nuevos paradigmas sin que éstos impacten de manera significativa en las operaciones de una organización y que además perduren en el tiempo.

Para alcanzar la excelencia que muchas de las organizaciones están buscando en materia de seguridad de activos de información, algunos ejecutivos así como profesionales de TI, están haciendo un esfuerzo para organizar de forma adecuada sus recursos, basados en su entendimiento de la seguridad de activos de información. Este entendimiento, permite darle respuesta a una serie de interrogantes que resultan relevantes, a saber:

- Desde una perspectiva tecnológica, ¿qué elementos de TI requiere mi empresa para satisfacer las necesidades de integridad, disponibilidad, confidencialidad y auditabilidad de los activos de información?
- Desde una perspectiva de recursos, ¿cómo identifico la combinación adecuada de personal, procesos y tecnología necesarios para mantener y optimizar la seguridad de activos de información?
- Desde una perspectiva estratégica, ¿está alineada la estrategia de seguridad de activos de información con la estrategia del negocio y el ambiente de riesgo?
- Desde una perspectiva de control, ¿dónde reside la responsabilidad de la seguridad de activos de información en la organización?
- Desde una perspectiva de gestión, ¿cómo administro la seguridad de activos de información, en conjunto con las necesidades del negocio, los constantes cambios de TI y las regulaciones actuales?

Asimismo, existe una creciente necesidad en las organizaciones en cuanto a los servicios de seguridad de activos de información proporcionados internamente o por terceras partes, que garanticen la existencia de controles adecuados.

Para muchas organizaciones, la información y tecnología, representan sus activos más valiosos, debido a:

- La creciente dependencia en la información, en los sistemas y las aplicaciones
- El incremento de las vulnerabilidades y una diversidad de amenazas, tales como “la guerra de información” y las “ciber-amenazas”
- El costo en las inversiones actuales y futuras en TI
- El potencial que tiene la TI para cambiar radicalmente las organizaciones, los procesos de negocio, aprovechar las nuevas oportunidades y reducir los costos
- La existencia de un contexto de mayor sofisticación en la operatividad de las empresas, con un escenario de tendencias de control de riesgo operacional
- Nuevas regulaciones en materia de control, como por ejemplo: la ley estadounidense Sarbanes-Oxley, y las más recientes resoluciones de los organismos reguladores de los diversos sectores en el país

A pesar de algunos esfuerzos, aún es factible encontrar a ejecutivos y tecnólogos que continúan percibiendo la seguridad de activos de información como un asunto meramente técnico, que debe ser resuelto mediante la utilización de un componente tecnológico en particular. En este sentido, existe la creencia de que no es necesario destinar parte del presupuesto del negocio a iniciativas de seguridad de activos de información, sino que por el contrario, esto podría estar incluido en el presupuesto de la Vicepresidencia o Gerencia de TI. Asimismo, encontramos empresas en las cuales las iniciativas de seguridad de activos de información vienen dadas por factores externos y no necesariamente por las evaluaciones formales de riesgo.

La permanencia de este tipo de percepciones, nos lleva a determinar que las organizaciones aún necesitan entender y afianzar la relación estratégica que existe entre sus objetivos de negocio y su estado actual en seguridad de activos de información. Este problema se debe principalmente al hecho de que la mayoría de las empresas no comprenden cómo sacar provecho a los procesos y actividades de seguridad de activos de información con el fin de añadir valor al negocio.

Uno de los factores críticos de éxito es comprender que el asegurar o proteger los activos de información, no es un problema de la TI, sino de conocer cuáles son los objetivos e iniciativas del negocio y de qué forma la seguridad de activos de información va a propiciar el logro de los mismos.

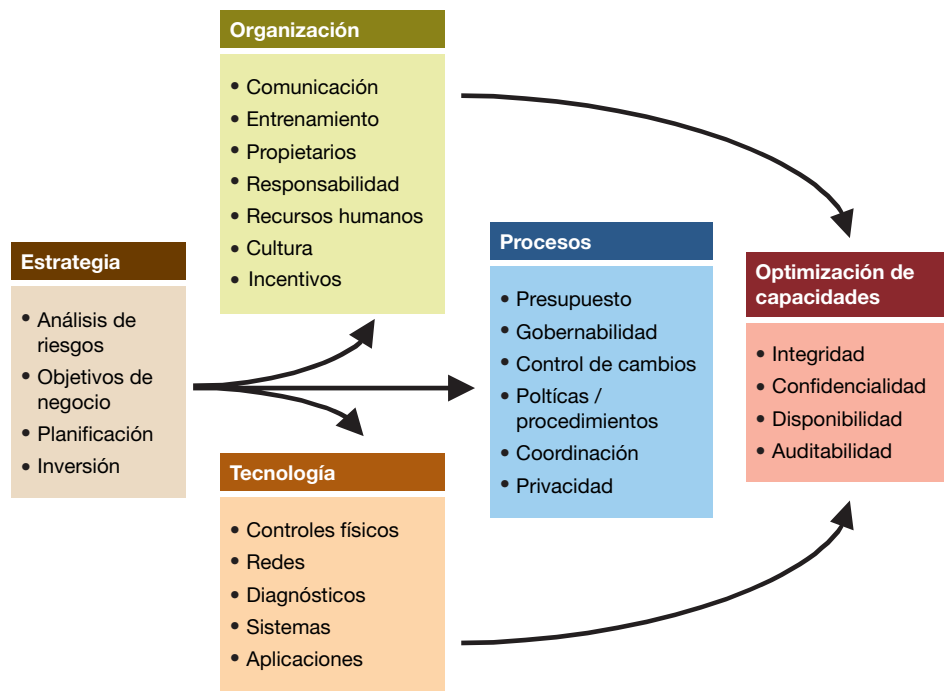


Figura N° 1. Nuevo enfoque de seguridad de activos de información

En este sentido, Espiñeira, Sheldon y Asociados, firma miembro de PricewaterhouseCoopers, por medio de su línea de servicios Advisory (Asesoría), realizó la encuesta anual correspondiente al 2004, orientada a medir las tendencias locales en materia de seguridad de activos de información, con el fin de obtener una visión a futuro en tres (3) grandes áreas en las empresas venezolanas, a saber:

- (a) las estrategias de seguridad que están siendo seguidas actualmente para proteger los activos de información,
- (b) el grado de exposición de las organizaciones a brechas de seguridad de activos de información en los diversos ambientes tecnológicos; y
- (c) los controles de seguridad que han sido implantados con el fin de mantener la confidencialidad, integridad y disponibilidad de los activos de información.

Los resultados de esta encuesta muestran un grado de avance de las empresas de diferentes sectores del mercado venezolano en la gestión de la seguridad de activos de información, con relación al estudio realizado por nuestra Firma en el período 2003-2004.

En este sentido, se percibe que la seguridad de activos de información ha cobrado mayor importancia como un proceso estratégico de negocio.

La Figura N° 1 muestra de forma general cómo la seguridad de activos de información puede ser vista como un proceso estratégico de negocio, el cual está conformado principalmente por tres grandes componentes, los cuales permiten el acceso y la protección de los activos de información de la empresa, a saber: Organización, Tecnología y Procesos. Por último y no menos importante, está el hecho que tanto en el

Distribución de las empresas participantes por sector

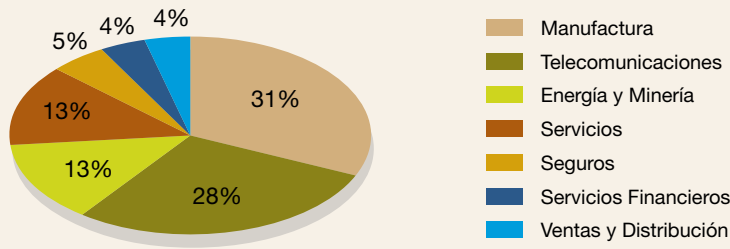


Figura N° 2. Distribución de las empresas participantes por sector

componente de tecnología como en el componente de organización es necesario el desarrollo de un plan de optimización de capacidades, el cual permitirá una evolución de la seguridad de activos de información desde su estado actual hasta el estado deseado o futuro.

Empresas participantes

En el estudio “Prácticas de seguridad de activos de información de las empresas en Venezuela - 2004”, desarrollado por Espiñeira, Sheldon y Asociados, firma miembro de PricewaterhouseCoopers, participó un total de ciento veintiséis (126) empresas del país, las cuales se encuentran distribuidas de acuerdo a los sectores que se especifican en la

Figura N° 2. Cabe destacar que la información recabada en las encuestas aplicadas corresponde al año 2004 y su recolección, procesamiento, y análisis se llevó a cabo durante el primer semestre del año 2005.

Agradecemos a todas las organizaciones que respondieron nuestra encuesta y que permitieron conocer cómo actualmente las empresas venezolanas consideran y ponen en práctica la gestión de la seguridad de activos de información.

Uno de los aspectos resaltantes de la presente encuesta, es el análisis realizado, ya que éste busca identificar las realidades detrás de las creencias o mitos en la práctica de la seguridad de activos de información en las empresas venezolanas.

Asimismo, algunos de los resultados se encuentran contrastados con el estudio “Global Information Security Survey - 2004”¹ en el que participaron sesenta y dos (62) países, lo que significó alrededor de ocho mil (8.000) empresas pertenecientes a diversos sectores del mercado.

En tal sentido, a continuación describiremos las principales conclusiones obtenidas por cada una de las secciones bajo estudio.

Principales conclusiones

La encuesta “Prácticas de seguridad de activos de información de las empresas en Venezuela - 2004”, estuvo dividida en tres (3) grandes secciones, las cuales se observan en la Figura N° 3.

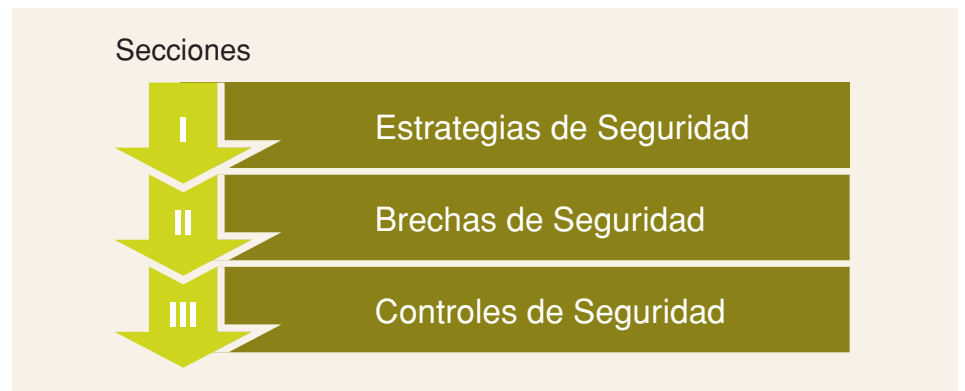


Figura N° 3. Secciones que conformaron la encuesta

¹ “Global Information Security Survey - 2004, marzo-abril 2004. PricewaterhouseCoopers, CIO Magazine y CSO Magazine”

Estrategias de Seguridad

En esta sección de la encuesta se evaluaron las estrategias que, en materia de seguridad de activos de información han sido aplicadas durante el año 2004 por las distintas empresas para proteger sus activos, en términos de:

- Cambios tecnológicos en el negocio
- Visión futura
- Concientización
- Experticia y destrezas
- Inversión
- Organización de la función de seguridad de activos de información o Chief Information Security Officer (CISO)

1. Alineación de la estrategia de seguridad de activos de información con los objetivos del negocio

Una de las primeras inquietudes estuvo orientada a conocer qué tan alineados están los objetivos de seguridad de activos de información, con respecto a los objetivos del negocio. En este sentido, 71% de las empresas encuestadas aseguró que sus objetivos de seguridad de activos de información están totalmente alineados con los objetivos del negocio; sin embargo, este resultado fue catalogado como un mito, ya que sólo un 32% de las empresas encuestadas le da prioridad de inversión al desarrollo y mantenimiento de un plan estratégico de seguridad de activos de información.

Mito	Realidad
<ul style="list-style-type: none"> • 71% de las empresas encuestadas concuerdan en que los objetivos y estrategias de seguridad de activos de información están alineados con los del negocio 	<ul style="list-style-type: none"> • Sólo 32% de las empresas encuestadas plantean como prioridad el desarrollo/mantenimiento de un plan estratégico de seguridad de activos de información

Una alineación con las estrategias del negocio, requiere la formalización de las estrategias de seguridad de activos de información en TI

El plan estratégico de seguridad de activos de información es una herramienta que permite, a las organizaciones desarrollar, ventajas competitivas, distinguirse en el mercado y dar mayor valor a los productos o servicios en relación a la competencia, teniendo como base los objetivos y necesidades del negocio.

2. Chief Information Security Officer (CISO) o Función de Seguridad de Activos de Información

Con respecto a la unidad organizacional encargada de llevar los procesos de seguridad de activos de información en la empresa o CISO, una de las principales interrogantes era conocer **cuál es la tendencia actual en cuanto a la ubicación de la Función de Seguridad de Activos de Información o CISO dentro de la organización**. En este sentido, en la Figura N° 4 se observa que el 70% de las empresas encuestadas coinciden en que de existir el CISO, éste se encuentra dentro de la Función de TI. Caso contrario ocurre a nivel mundial, en donde el CISO está adquiriendo autonomía e independencia, lo cual significa que los procesos de seguridad de activos de información están siendo considerados con mayor atención y menos escepticismo por parte de la alta directiva.

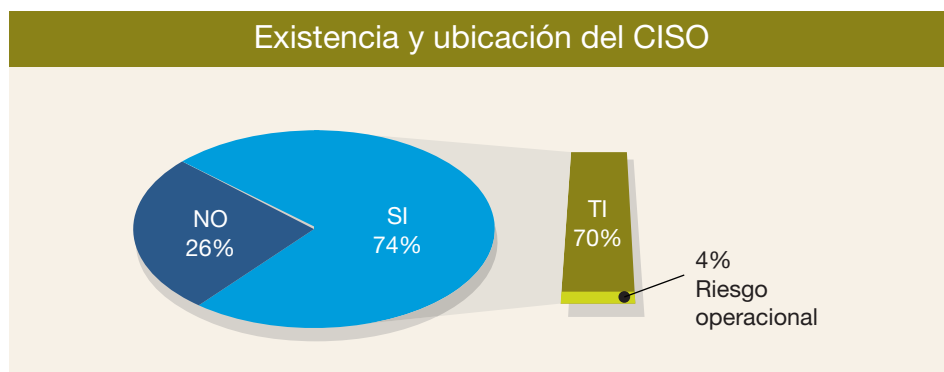
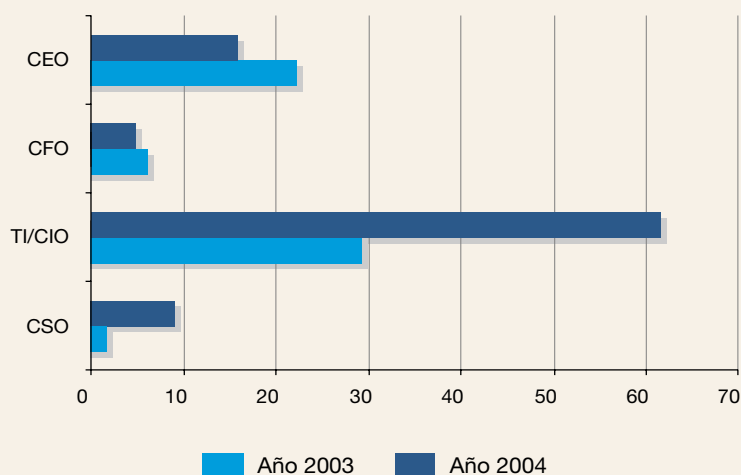


Figura N° 4. Existencia y ubicación del CISO

Línea de reporte del CISO a otras unidades



Fuente: Global Information Security Survey-2004, PricewaterhouseCoopers, CIO Magazine y CSO Magazine

Figura N° 5. Línea de reporte del CISO a otras unidades

Tendencia

La estructura organizacional del CISO reside dentro de TI

Además, para el año 2004, según la “Global Information Security Survey - 2004”, el 31% de las empresas encuestadas aseguró haber creado la posición del CISO o Chief Information Officer (CIO), lo cual representa un incremento sustancial con respecto a la cifra del año 2003, que se ubicaba en un 15%. Asimismo, cuando se le preguntó a las empresas participantes en el estudio global, a quién le reporta el CISO en su organización, se observó

que sólo en un 29% de las empresas encuestadas reportan directamente al Director de TI. Esta cifra representa una disminución de más de la mitad con respecto a la tendencia en el año 2003, tal y como se muestra en la Figura N° 5.

Otra de las inquietudes en el estudio “Prácticas de Seguridad de activos de información de las empresas en Venezuela - 2004”, era dar respuesta a: **cuántos recursos están siendo**

destinados a la Función de Seguridad de Activos de Información o CISO. En este sentido, observamos que más del 60% de las empresas encuestadas indicó que no tiene personal asignado para la Función de Seguridad de Activos de Información o CISO, mientras que sólo el 5% de las empresas encuestadas posee más de 10 personas en el área. Para mayor detalle, ver Figura N° 6.

Cantidad de personas que conforman la Función de Seguridad de Activos de Información



Figura N° 6. Cantidad de personas que conforman la Función de Seguridad de Activos de Información

¿Quiénes del personal del CISO poseen certificaciones formales en esta materia?

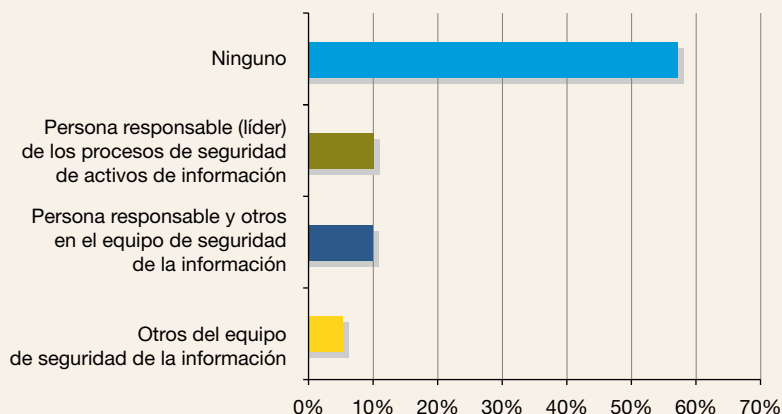


Figura N° 7. Personal del CISO con certificaciones formales en seguridad de activos de información

3. Adiestramiento en seguridad de activos de información

El contar con personal altamente capacitado para gestionar los procesos de seguridad de activos de información resulta determinante para toda organización. En el estudio “Information Security Breaches Survey - 2004”² realizada en el Reino Unido con una base muestral de mil (1000) empresas pertenecientes a distintos sectores del mercado, se determinó que un 75% de las empresas encuestadas aseguró que no contaba con personal certificado formalmente en seguridad de activos de información. Este resultado es similar al obtenido en nuestro estudio “Prácticas de seguridad de activos de información de las empresas en Venezuela - 2004”, el cual puede ser observado en la Figura N° 7, en el que alrededor del 60% de las empresas presenta la misma situación.

Estas cifras nos inducen a pensar que aun cuando las certificaciones formales son usualmente un indicativo importante de conocimiento en la materia, y a pesar que en el mercado en los últimos años, hemos visto la aparición y fortalecimiento de una amplia gama de certificaciones, (CISSP, Certified Information System Security Professional; SSCP, System Security Certified Practitioner; CISM, Certified Information Security Manager), lo que está ocurriendo es que estamos viviendo los primeros años de este proceso, en donde apenas está comenzando la adopción de la práctica de certificación en materia de seguridad de activos de información. En el caso venezolano,

esta situación se ve afectada aún más por la dificultad que existe en términos de accesibilidad a los cursos de adiestramiento, así como a los exámenes de certificación, los cuales en su mayoría deben realizarse fuera del país.

4. Presupuesto, gasto e inversión

En el pasado, la falta de inversión para proteger los activos de información ha sido la principal causa en el incremento de los incidentes de seguridad de activos de información. Afortunadamente, según los resultados obtenidos de nuestro estudio en Venezuela, el 79% de las empresas encuestadas aumentó en el último año el presupuesto destinado a seguridad de activos de información, y más aún, el 59% de las empresas encuestadas asegura que su inversión en el 2005 se incrementará, siendo éste un resultado similar al obtenido por el “Global Information Security Survey - 2004” que lo ubicó en 64%. Es importante destacar, que estas cifras van en aumento no sólo por la

necesidad de las empresas para minimizar las brechas de seguridad de activos de información, sino porque actualmente, uno de los principales aspectos que está marcando la pauta es la inversión en seguridad es la necesidad de cumplir con regulaciones y leyes tanto locales como internacionales. De hecho, se estima que un porcentaje del gasto en seguridad de activos de información provenga de otros departamentos del negocio, tales como la Gerencia de Finanzas, bajo presupuestos de “cumplimiento”.

Por otro lado, muchas de las empresas incluyen el presupuesto de seguridad de activos de información como parte del presupuesto de TI. En este sentido, se observó que el 52% de las empresas venezolanas encuestadas asigna entre un 2% y un 10% del presupuesto de TI a seguridad de activos de información; sin embargo, según los resultados del “Global Information Security Survey - 2004”, la media internacional es de 11.3%, lo cual representó un incremento con respecto al año 2003 de 0.4 puntos porcentuales.

² “Information Security Breaches Survey - 2004 PricewaterhouseCoopers, Computer Associates, Entrust, Microsoft”

A pesar del incremento en estas cifras, una de las principales limitaciones que tienen las empresas venezolanas en estos momentos para incrementar la inversión en seguridad de activos de información, es la dificultad que se tiene para cuantificar los beneficios no financieros. Esto explica, entonces, el por qué sólo el 23% de las empresas encuestadas tiene como práctica el cálculo del retorno de la inversión o ROI (Return of Investment), lo cual pudiera incidir en el hecho que no se estén priorizando de forma adecuada los proyectos de seguridad de activos de información.

Como dato curioso, según los resultados del estudio, "Information Security Breaches Survey -2004", los

sectores del mercado del Reino Unido que han invertido más en seguridad son: telecomunicaciones, servicios financieros, salud y educación. Sin embargo, en los Estados Unidos de América, según los resultados del "CSI/FBI Computer Crime and Security Survey - 2004"³, se tiene que

el sector que ha invertido más en seguridad en el año 2004 ha sido el de transporte, en donde la inversión anual por empleado está alrededor de US\$450 versus un promedio de US\$160 anuales por concepto de gastos operativos por empleado.

Mito	Realidad
<ul style="list-style-type: none"> En general, se habla bastante de la importancia de seguridad de activos de información, sin embargo, no se invierte en ella 	<ul style="list-style-type: none"> El 79% de las empresas venezolanas encuestadas incrementó en el último año su presupuesto destinado a seguridad de activos de información El 59% de las empresas venezolanas encuestadas afirma que la inversión en seguridad de activos de información en el 2005, se incrementará

El presupuesto de seguridad de activos de información seguirá incrementándose, sin embargo, las organizaciones exigirán mayores controles y justificaciones sobre su utilización

Obstáculos para la práctica de seguridad de activos de información

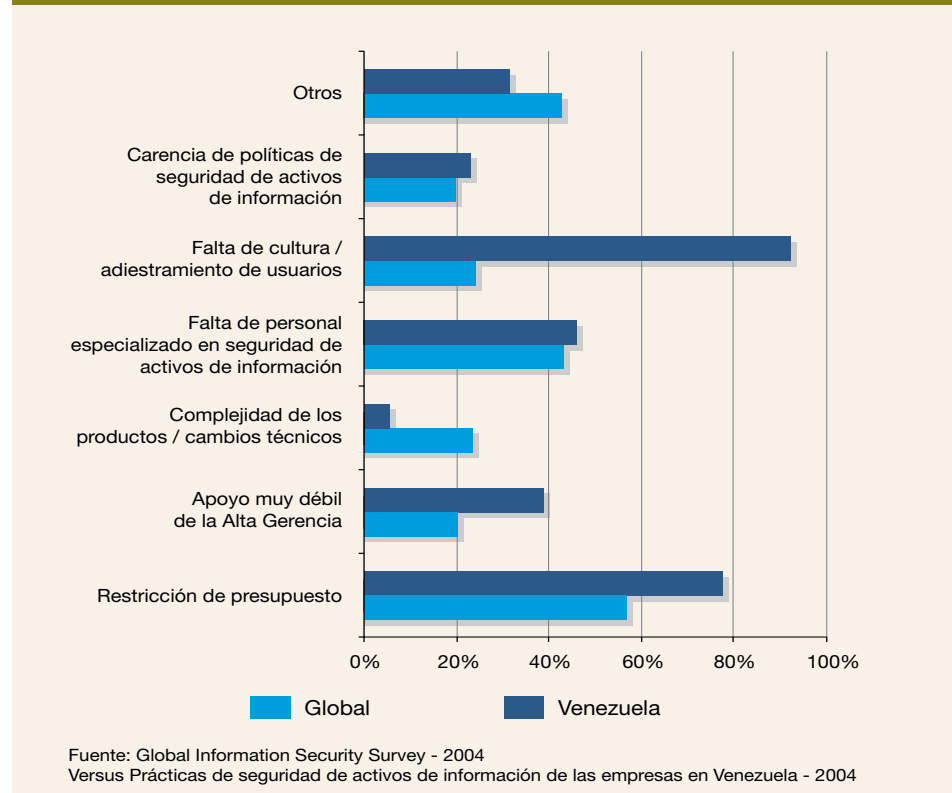


Figura N° 8. Obstáculos para la práctica de seguridad de activos de información

5. Obstáculos para la práctica de seguridad de activos de información

La restricción del presupuesto resultó ser un denominador común tanto en Venezuela como internacionamente para la práctica de seguridad de activos de información. Al contrastar los resultados de nuestro estudio en Venezuela con los datos del "Global Information Security Survey - 2004", los cuales pueden apreciarse en la Figura N° 8, observamos que en el caso venezolano un 76% de las empresas encuestadas coinciden en este aspecto, al igual que un 57% de las empresas a nivel mundial. Sin embargo, aun cuando el presupuesto resultó ser un elemento común en ambos resultados, en el caso venezolano éste no representa la principal barrera para la práctica de seguridad de activos de información. En este sentido, se observó que el 92% de las empresas venezolanas bajo este estudio coincidieron en que la falta de cultura y conciencia en seguridad, así como el poco o inexistente

³ "CSI/FBI Computer Crime and Security Survey - 2004, realizada en conjunto con el San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, la cual fue aplicada a 494 personas pertenecientes a: corporaciones, agencias de gobierno, instituciones financieras, empresas del sector salud y universidades en los Estados Unidos de América".

adiestramiento de usuarios en este particular, representa el principal obstáculo para la práctica de seguridad de activos de información.

Generalizando los resultados para las empresas venezolanas, el mayor desafío será la necesidad de introducir, de forma efectiva, una cultura de seguridad de activos de información en todos los niveles de la organización con el fin de concientizar en la responsabilidad que todos los empleados tienen sobre este tema.

Otro aspecto curioso que resalta de la comparación entre el "Global Information Security Survey - 2004" y los resultados de nuestra encuesta en Venezuela, es el hecho de que la complejidad de los productos, así como los cambios tecnológicos, resultan factores medianamente importantes a considerar como limitantes en la práctica de seguridad de activos de información a nivel internacional, en contraposición con el

caso venezolano, en el cual estos factores son los menos determinantes. Esto sin duda nos hace pensar en una ventaja competitiva que tenemos en Venezuela, el ser más flexibles, logrando adaptarnos rápidamente a los diversos cambios tecnológicos que se suscitan.

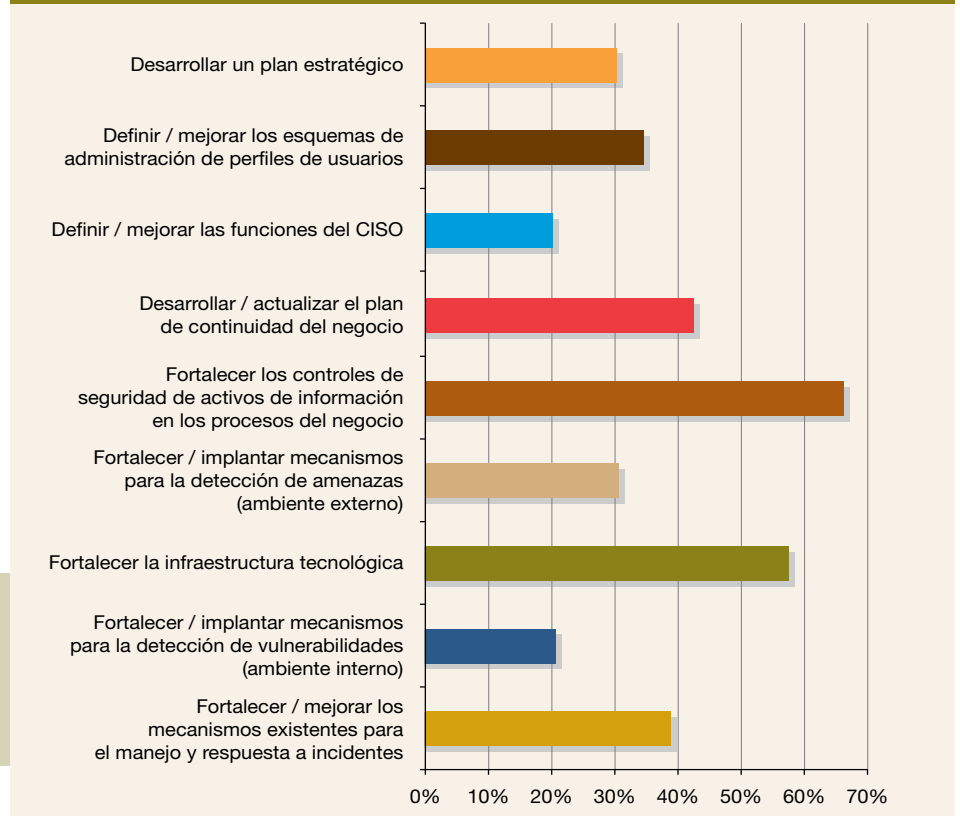
Asimismo, un aspecto que resulta prácticamente de igual importancia tanto en el mercado venezolano como el mercado global, es la falta de personal especializado en seguridad de activos de información (44% de las empresas encuestadas lo consideran un obstáculo en el caso venezolano, versus 42% en el caso global). Esto refuerza el análisis que se realizó anteriormente en el punto 3, en donde se observó que a pesar que en el mercado existen certificaciones en materia de seguridad de activos de información, las empresas en general no cuentan con este tipo de recurso.

6. Prioridades estratégicas en materia de seguridad de activos de información para el año 2005

En la Figura N° 9 se pueden observar las principales prioridades estratégicas de las empresas venezolanas para el año 2005, entre las que destacan:

- Fortalecer los controles de seguridad de activos de información en los procesos de negocio (68%)
- Fortalecer los controles de seguridad de activos de información en la infraestructura tecnológica (59%)
- Desarrollar/actualizar el plan de continuidad del negocio (45%)
- Fortalecer/mejorar los mecanismos existentes para el manejo y respuesta a incidentes (40%)

Las prioridades estratégicas



Las prioridades estratégicas para el próximo año son el fortalecimiento de los controles a nivel de los procesos de negocio y la infraestructura tecnológica

Figura N° 9. Prioridades estratégicas en seguridad de activos de información para el año 2005

Estos resultados coinciden en su mayoría con los datos obtenidos mediante el “Global Information Security Survey - 2004”, en donde las principales prioridades estratégicas están en: mejorar los aspectos de seguridad en la red, desarrollar planes de continuidad de negocio y recuperación ante desastres, gestionar los procesos de incidentes de seguridad y concientizar a los usuarios.

Es resaltante el hecho que para el caso venezolano el “fortalecer los controles de seguridad en los procesos de negocio” sea la prioridad estratégica. Sin embargo, esto pudiese ser visto como un paso importante que están dando las empresas venezolanas en

concientizar que la seguridad de activos de información no es un asunto meramente tecnológico, sino que es un proceso estratégico que abarca: Organización, Tecnología y Procesos. Asimismo, uno de los principales impulsores de esta orientación hacia los controles en los procesos de negocio, es la necesidad que tienen las empresas por cumplir con ciertas regulaciones y leyes nacionales e internacionales.

7. Concientización en seguridad de activos de información (Awareness)

Tal como se muestra en la Figura N° 10, destaca el hecho que alrededor del 78% de las empresas venezolanas

coinciden en que una de sus principales necesidades para el manejo adecuado de sus riesgos, es definitivamente una mayor educación en la materia. Sin embargo, encontramos que alrededor del 40% de la población encuestada coincide en una mala práctica: **el esquema o proceso de concientización de seguridad de activos de información utilizado no es aplicado de forma periódica y continua, por el contrario se limita a una aplicación puntual del control en un período específico (generalmente en el proceso de ingreso de personal).**

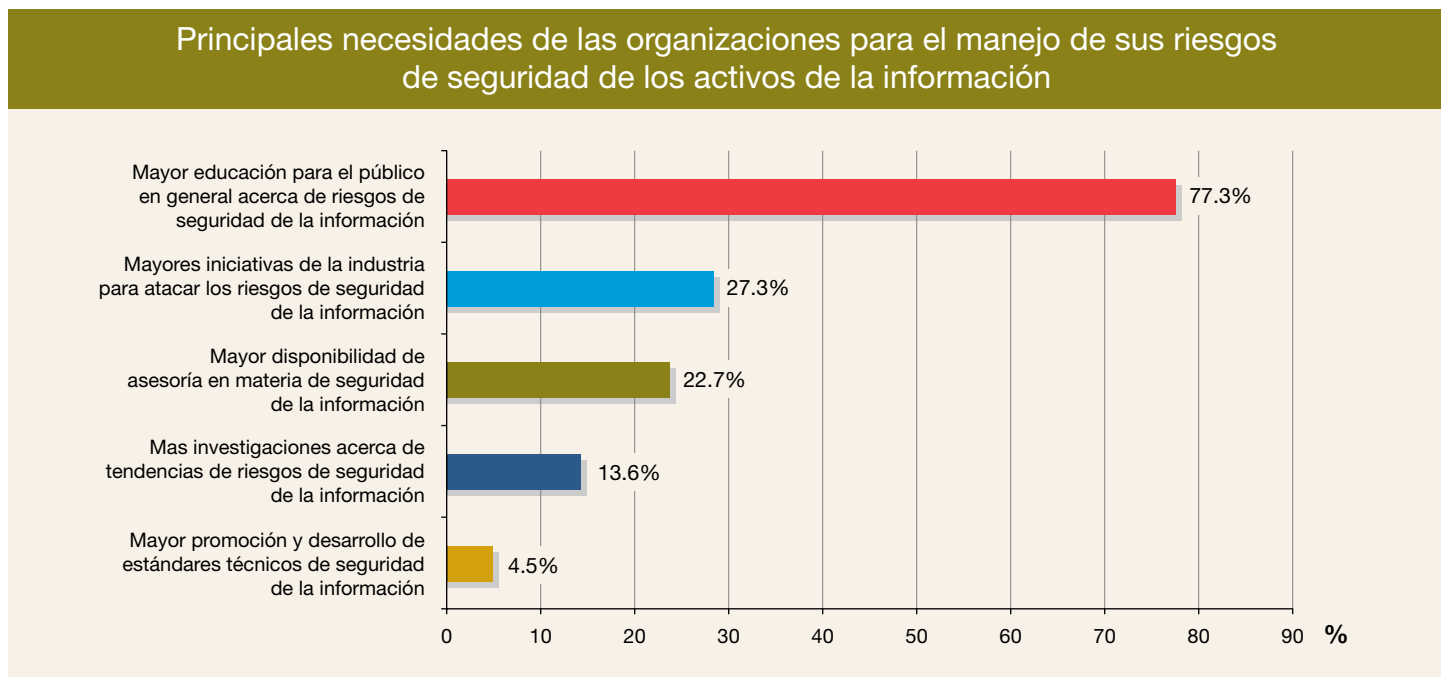


Figura N° 10. Principales necesidades de las empresas para el manejo de sus riesgos de seguridad de activos de información

En este sentido, en la Figura N° 11, se observa que las dos (2) herramientas que son utilizadas con mayor frecuencia para concientizar al personal en materia de seguridad son:

- La inducción como parte de un nuevo ingreso de personal
- Firma de documentos o acuerdos de responsabilidad y confidencialidad de la información que se maneje

Sin duda, estas herramientas no constituyen la mejor práctica, ya que suelen aplicarse una sola vez en el tiempo, dejando a un lado el

reforzamiento continuo y periódico que debe existir como parte de un proceso adecuado de concientización de usuarios en una organización.

Mito	Realidad
<ul style="list-style-type: none"> • Las empresas venezolanas aseguran que sus empleados están conscientes de los riesgos y su responsabilidad en el uso de la tecnología de información 	<p>Local e internacionalmente, los principales esfuerzos de concientización se limitan a:</p> <ul style="list-style-type: none"> • Como parte de la inducción de nuevo ingreso • Firma de documentos / acuerdos de responsabilidad y confidencialidad de la información que manejan
<p>La concientización de los empleados debe ser un proceso continuo</p>	

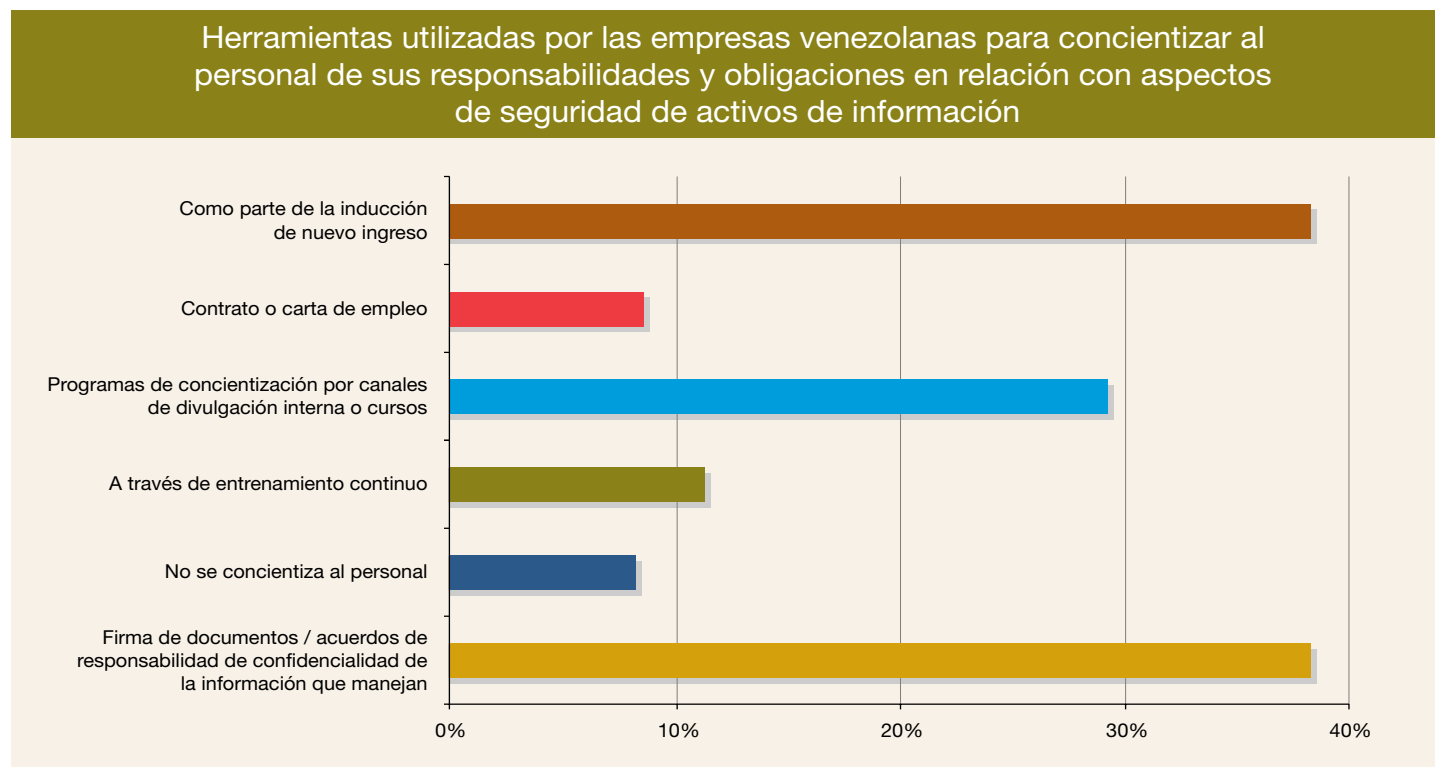


Figura N° 11. Principales herramientas utilizadas por las empresas venezolanas para concientizar al personal en relación con la seguridad de activos de información

Brechas de Seguridad

En esta sección de la encuesta se evaluó el grado de exposición de las organizaciones a las brechas de seguridad en los diversos ambientes tecnológicos, en términos de:

- Incidencias de seguridad
- Ataques internos y externos
- Infección por virus
- Uso inadecuado de sistemas de información y recursos
- Accesos no autorizados

8. Incidentes de seguridad de activos de información

Al preguntarle a las empresas venezolanas sobre los aspectos relacionados con los principales incidentes de seguridad, los mecanismos utilizados para

solventarlos, así como los niveles de interrupción ocasionados, encontramos los siguientes resultados:

- La infección por virus fue el incidente más frecuente (30%), y en general éste originó un nivel de interrupción de menos de un día

(interrupción menor). Para mayor detalle ver Figura N° 12

- El 65% de las empresas utilizó planes de respaldo y contingencia para solventar su peor incidente de seguridad de activos de información

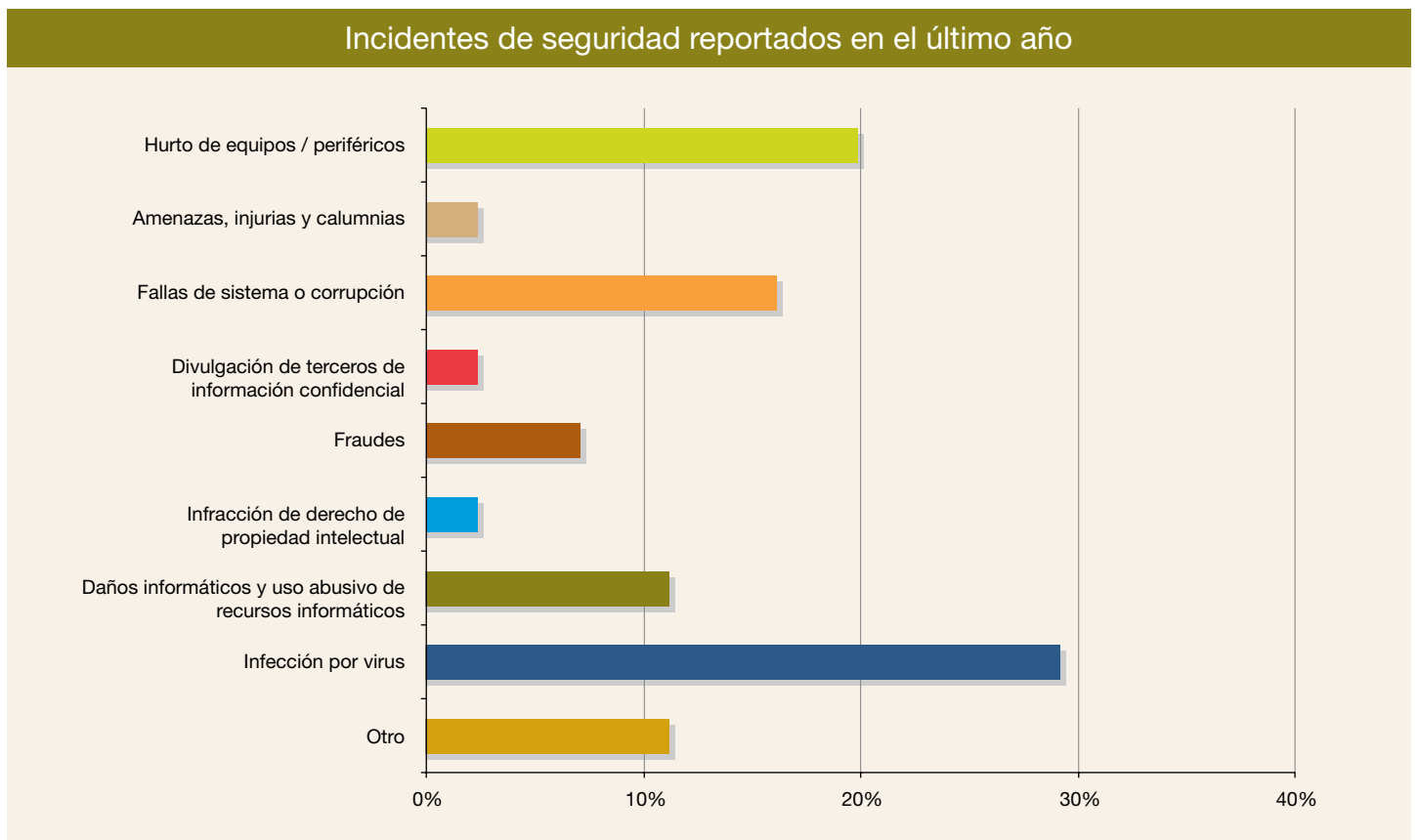


Figura N° 12.: Incidentes de seguridad de activos de información reportados en el último año

- La investigación del peor incidente fue realizada por un grupo interno, y sólo un 10% de las empresas encuestadas lo informaron públicamente
- 60 % de las empresas encuestadas coincidieron en que el origen del peor incidente de seguridad de activos de información fue interno, tal como se muestra en la Figura N° 13

Mito	Realidad
<ul style="list-style-type: none"> • Los incidentes de infección por virus son un asunto meramente técnico que se resuelve reduciendo los tiempos de actualizaciones del software 	<ul style="list-style-type: none"> • Todo marco integral de seguridad de activos de información posee un alto componente relacionado con la educación del personal
<p>El usuario debe ser formado en el riesgo individual y colectivo sobre el uso de la tecnología de la información</p>	

9. Vulnerabilidades más importantes para el negocio

En la Figura N° 14, se observa que para las empresas encuestadas en Venezuela existen aspectos de negocio que resultan muy importantes al considerar las posibles vulnerabilidades a las que están expuestas, a saber:

- Confiabilidad, ética y motivación del personal
- Perfiles inadecuados en los sistemas e infraestructura tecnológica
- Conocimiento del personal sobre sus procesos de negocio
- Componentes y periféricos electrónicos
- Oportunidad de desarrollo profesional

Uno de los aspectos que destaca de este resultado, es que sólo alrededor del 25% de las empresas encuestadas considera el aspecto de “Confiabilidad, ética y motivación del personal” como “muy importante”, y la realidad es que para lograr una adecuada gestión integral de riesgos, la ética, la moral, el comportamiento, los valores y creencias del personal que labora o mantiene relación de negocio con la empresa, resultan fundamentales para la adecuada gestión de sus procesos de seguridad.

En este sentido, es imperativo que las empresas venezolanas tomen conciencia de la importancia y necesidad de que aspectos como la confiabilidad, ética, comportamiento y motivación del personal, deban ser los principales impulsores para la conformación de un marco de seguridad para el negocio.

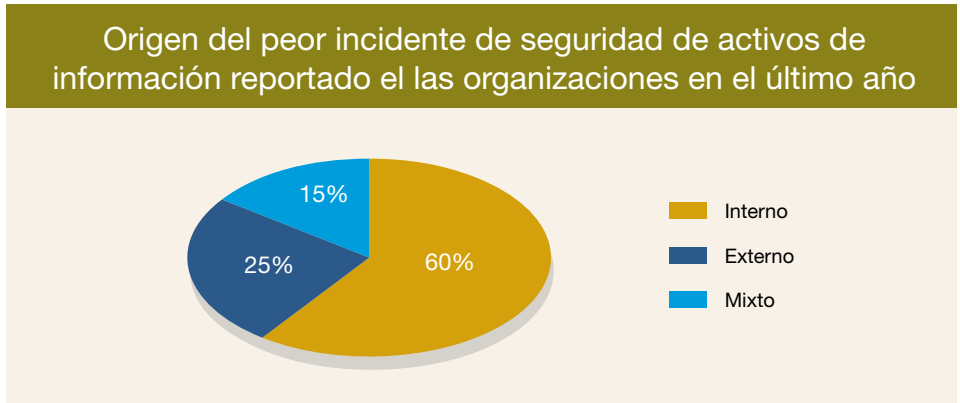


Figura N° 13. Origen del peor incidente de seguridad de activos de información reportado en las organizaciones en el último año



Figura N° 14. Importancia de las vulnerabilidades en los aspectos de negocio

Controles de Seguridad

En esta sección de la encuesta se evaluaron los controles de seguridad que han sido implantados a fin de mantener la confidencialidad, integridad y disponibilidad de los activos de información en los siguientes ambientes:

- Internet y correo electrónico
- Accesos remotos
- Red interna
- Proceso de gestión del cambio
- Outsourcing / proveedores de servicio

10. Evaluaciones de seguridad de activos de información

El panorama general de las empresas venezolanas encuestadas, indica que entre las actividades consideradas de mayor importancia, se incluye la realización de evaluaciones de seguridad de activos de información, al menos una vez al año (Ver Figuras N° 15 y N° 16), seguidas de las actividades de administración de seguridad de activos de información. En este sentido, estos resultados permiten conocer que en el caso venezolano, las empresas encuestadas están conscientes de la importancia que tienen estos aspectos en la protección y establecimiento de los controles adecuados para otorgar los privilegios de acceso a los activos de información a las personas autorizadas, en el momento indicado.



Figura N° 15. Actividades más importantes de seguridad de activos de información

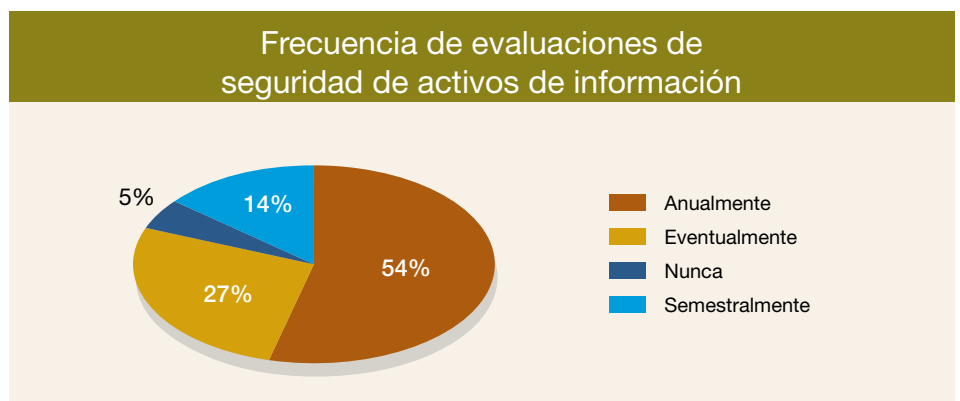


Figura N° 16. Frecuencia de evaluaciones de seguridad de activos de información

11. Accesos remotos

Al preguntarle a las empresas encuestadas, en el caso venezolano, acerca de aspectos relacionados con los mecanismos utilizados para conexiones remotas, así como el uso de dispositivos portátiles de almacenamiento de información, observamos los siguientes resultados:

- El 48% de las empresas encuestadas tienen su red o Intranet accesible desde el exterior
- El 78% no restringe la salida de información confidencial por medio de dispositivos informáticos miniaturizados tipo USB o tarjetas de memoria
- El 87% de las empresas encuestadas cuenta con personal que utiliza equipos portátiles, PDA's o dispositivos similares

Mito

- Los privilegios de acceso remoto están controlados y se restringen a personal de confianza

Las fronteras de nuestros esquemas de seguridad de activos de información y control deben extenderse en igualdad de exigencia a todo elemento asociado con nuestra información y procesos

Realidad

- Los controles sobre acceso remoto son insuficientes y la información puede salir de manera autorizada o no
- Los esquemas de protección de dispositivos móviles son básicos

12. Proveedores de servicio

Las principales conclusiones relacionadas con los controles implantados para una adecuada interacción con los socios de negocio, proveedores de servicio o terceras partes, son:

- El 46% de las empresas venezolanas encuestadas no poseen acuerdos de niveles de servicios formalmente documentados
- El 47% de las empresas venezolanas encuestadas no verifica el cumplimiento de sus estándares y políticas de seguridad por parte de sus proveedores de servicio

Mito

- Los proveedores de servicio igualan o superan las normas de seguridad de activos de información establecidas por las empresas encuestadas

Las evaluaciones de seguridad de activos de información y control sobre mis proveedores de servicio deben formar parte de mis actividades regulares

Realidad

- Los proveedores de servicio son fuente de vulnerabilidades e incumplimientos de las normativas de seguridad de activos de información de la empresa

Comentarios

La seguridad de activos de información es otro proceso estratégico del negocio, ya que al lograr el equilibrio adecuado entre la protección y la habilitación de acceso a los activos de información, así como el hecho de estar alineado con los objetivos de negocio, se estarán optimando substancialmente las operaciones. La noción de seguridad de activos de información como un habilitador de negocios es hoy en día un concepto esencial para las organizaciones de cualquier sector industrial.

Como un proceso estratégico, la seguridad de activos de información pudiera estar enfocada en proteger los activos de información de una organización contra pérdidas y uso indebido, o enfocada en brindar acceso a los activos de información apoyando los objetivos de negocio. Uniendo estos dos conceptos - seguridad como "Protección"

(Exclusión) y seguridad como "Habilitador de Accesos" (Inclusión) - se define de manera integral un nuevo enfoque de seguridad de activos de información en las organizaciones, ver Figura N° 17.

La seguridad de activos de información no es sólo un aspecto tecnológico, por el contrario, es una solución integrada de negocio que combina recursos organizacionales, procesos y tecnología. Si no se cuenta con reglas, lineamientos, responsabilidades y procedimientos predefinidos y ante la ausencia de personal que esté capacitado para la gestión del proceso, la inversión sólo en tecnología no es más que una pérdida de dinero. Este concepto de seguridad de activos de información, como una solución integral, es esencial para la transformación de este nuevo enfoque en una plataforma tangible, pragmática y operativa de seguridad, que brinde resultados cuantificables para el negocio.

Finalmente, con el objeto de dar los primeros pasos en la incorporación de la seguridad de activos de información como un proceso estratégico del negocio, presentamos a continuación los siete (7) principales secretos de las empresas internacionales que pertenecen al grupo de las mejores prácticas (Best Practice Group):

1. Definir un plan estratégico de seguridad de activos de información
2. Incrementar la inversión en seguridad de activos de información
3. Separar el CISO de la Función de TI
4. Realizar estudios de penetración y auditorías periódicas al ambiente de TI
5. Ejecutar un proceso continuo y periódico de evaluación de riesgo y control, con el fin de identificar y priorizar amenazas y vulnerabilidades
6. Definir un modelo y una arquitectura integral de seguridad
7. Establecer un proceso de revisión periódico con el fin de medir la efectividad del CISO

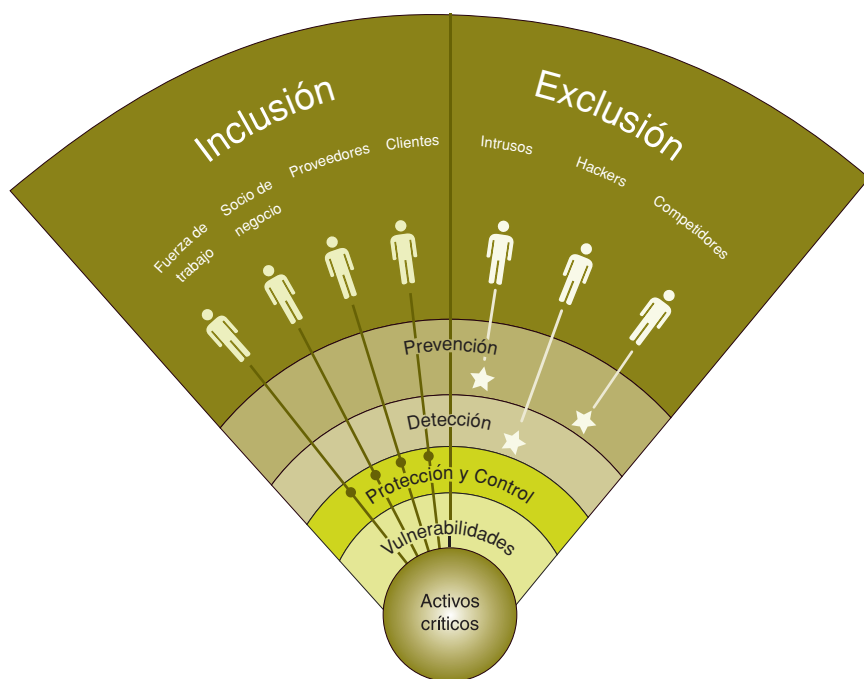


Figura N°17. Enfoques de seguridad de inclusión y exclusión

¿Quiénes somos?

Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers, es líder tanto mundial como nacional, en servicios de auditoría de estados financieros, 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 Advisory (Asesoría). En Advisory

contamos con más de noventa y cinco (95) profesionales de variadas habilidades en diferentes 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.
- **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 las organizaciones en el desarrollo y/o evaluación de las políticas de seguridad.
- **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 activos de 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 la tecnología. 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 / Plan de continuidad del negocio**
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.

- **Revisión de seguridad en e-commerce / e-banking**
Como parte de nuestros servicios a los clientes, realizamos evaluaciones en la infraestructura que apoya las operaciones de comercio y banca electrónica. 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 de estas plataformas 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 vulnerabilidades 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).



Espiñeira, Sheldon y Asociados
firma miembro de
PricewaterhouseCoopers

Avenida Principal de Chuao
Edificio Del Río
Caracas
Teléfonos: 0212 700-6666

Encuesta

Prácticas de seguridad de
activos de información de las
empresas en Venezuela - 2004

Espiñeira Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers ha realizado las comprobaciones necesarias para asegurar que toda la información utilizada para la elaboración de este informe, procede de fuentes fiables y reúne un grado de precisión adecuado. Aun aceptando la premisa anterior, Espiñeira Sheldon y Asociados, no garantiza en ningún modo la plena veracidad y exactitud de la información que contiene este informe. Por ello, aunque el trabajo y las conclusiones que se derivan del mismo cumplan con los máximos estándares de calidad, esta publicación no pretende ofrecer, en ningún caso, las cifras definitivas de los tópicos aquí tratados.

Sus mundos  nuestra gente*