

Prácticas de Seguridad de Información de las Empresas en Venezuela

*Edición 2011
Resultados de
Encuesta 2010*



Introducción

La Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información. El incumplimiento de cualquiera de estos objetivos expone a la organización a riesgos de diversa índole, que pueden afectar el patrimonio y reputación de la organización.

Por otro lado, la seguridad de información no es un hito, sino más bien un estado que requiere un proceso continuo de renovación y mantenimiento que determina la necesidad de inversión, planificación y medición de los objetivos cumplidos.

Las dos aseveraciones anteriormente mencionadas nos llevan entonces a una conclusión: La seguridad de la información, debe estar inmersa en la estrategia del negocio y en la cultura de la organización.

Atrás quedó la época que la seguridad era una mejor práctica o algo que pudiese diferirse; ante situaciones de crisis como las que afrontamos, las organizaciones son menos tolerantes a fallas o pérdidas financieras y ambas áreas son de interés de la gestión de seguridad de información. En este escenario surge la necesidad de establecer un enfoque estratégico de la seguridad de información, y es por ello que el entendimiento de lo que ocurre en el mercado y sus tendencias, son fundamentales para establecer una gestión de seguridad de información eficiente y en sintonía con los objetivos del negocio.

Hoy tenemos el agrado de presentarles nuestra octava (8^{va}) edición de la Encuesta sobre la práctica de la seguridad de información en las empresas venezolanas.

Como es habitual, hemos incorporado al análisis de los resultados, cifras comparativas de las ediciones anteriores y de la encuesta global de PwC, lo cual permitirá al lector ahondar en la opinión de los encuestados con una retrospectiva en los avances y retrocesos que la seguridad de la información ha sufrido a lo largo de este año, y una comparación con el mercado internacional.

Agradecemos a todas las empresas que dieron respuesta a nuestra encuesta y que nos permitieron establecer una visión de las tendencias y estrategias de las organizaciones en Venezuela en materia de seguridad, así como los principales incidentes, obstáculos y aplicación de las mejores prácticas de seguridad y TI, así como observar el nivel de madurez sobre la forma en el cual se percibe la privacidad de la información en las diferentes organizaciones.

Participación

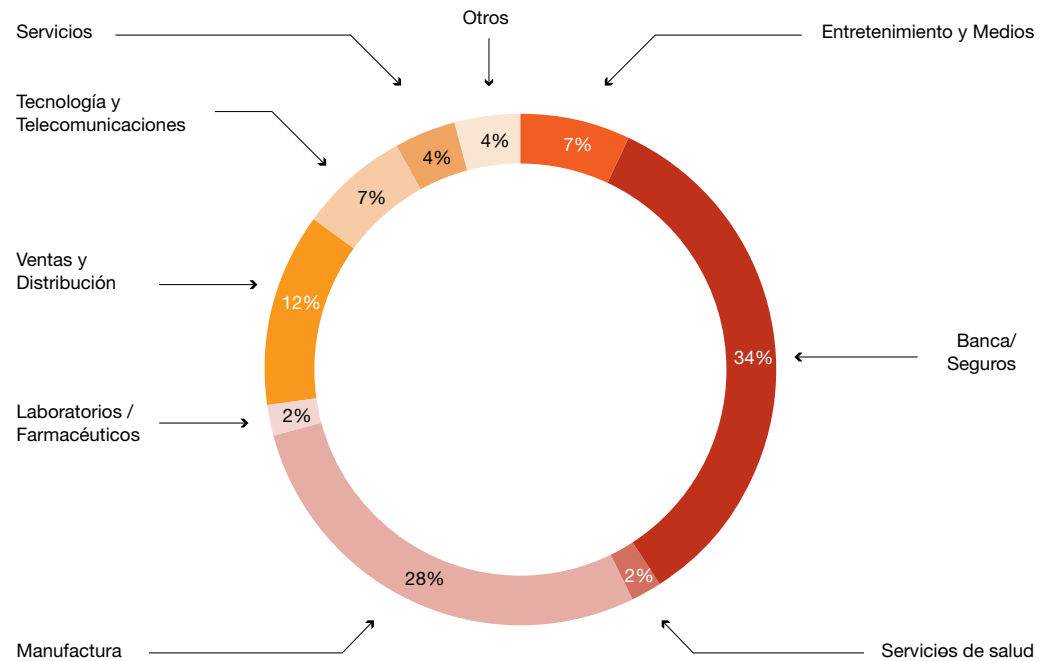
En la octava Encuesta Anual “Prácticas de Seguridad de Información de las Empresas en Venezuela” desarrollada por Espiñeira, Sheldon y Asociados, fueron convocadas empresas de diversos sectores de la actividad económica del país, tanto del sector público como privado, las cuales se encuentran distribuidas porcentualmente de acuerdo a lo que se especifica en la Figura N° 1.

La información recabada corresponde al último trimestre del año 2010 y su procesamiento y análisis se llevó a cabo durante el primer trimestre del 2011.

Del total de empresas venezolanas participantes, se destaca como el sector de mayor participación este año, el de Banca/Seguros/Servicios Financieros con el 34%. El sector Manufactura se encuentra en el segundo lugar (28%) y en tercer lugar se encuentra el sector Ventas y Distribución (12%).

Figura N° 1. Distribución de las empresas venezolanas participantes por sector

P. ¿A cuál de los siguientes sectores pertenece su empresa?



Ficha técnica

Esta edición está orientada a conocer la aplicación efectiva de la seguridad de activos de información en las empresas venezolanas, así como también reflejar las prácticas actuales, tendencias, obstáculos de aplicación y uso de mejores prácticas.

La encuesta fue distribuida en formato electrónico a nuestros clientes y relacionados para su participación; y estuvo conformada por un total de treinta y cinco preguntas agrupadas en diferentes secciones.

Este año se adicionan una nueva sección a la encuesta referente a la Inversión en Seguridad de la Información.

Los temas considerados en este estudio están divididos en cinco grandes secciones que agrupan las consultas, a saber:

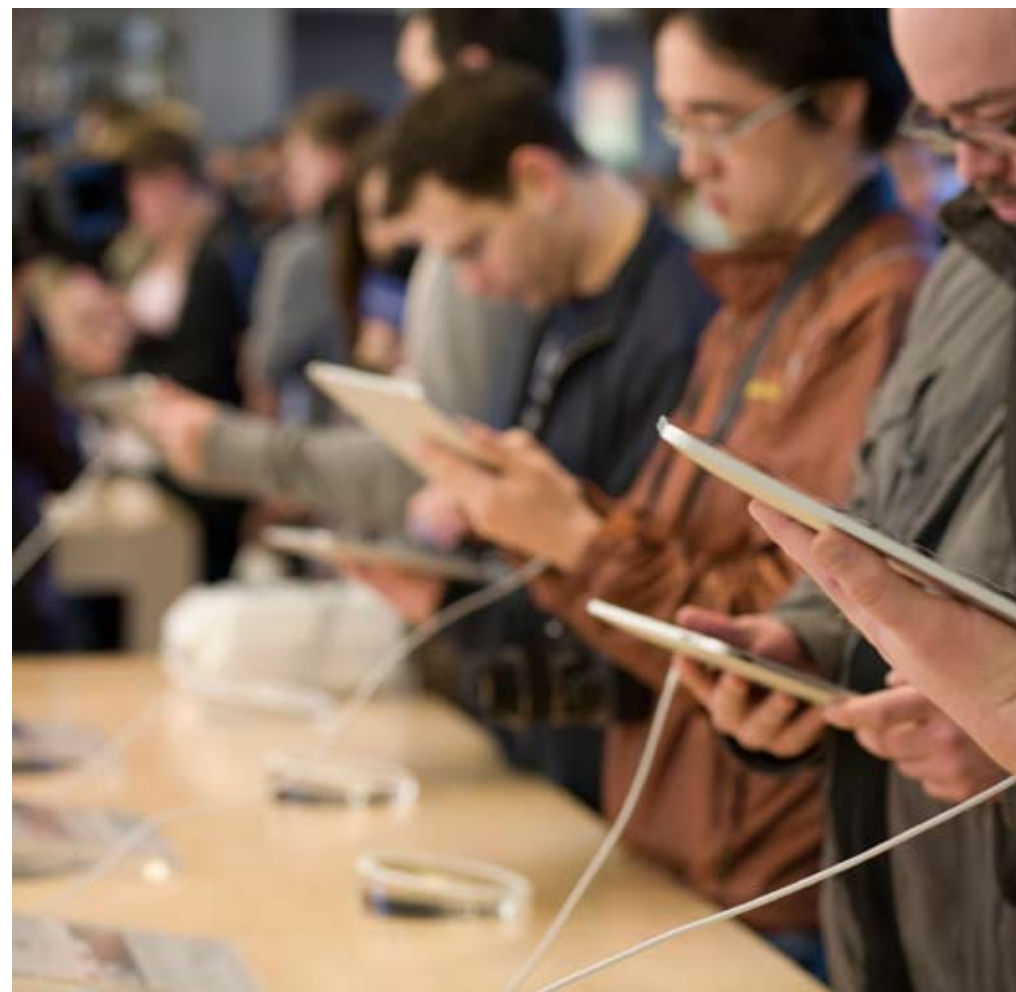
Sección I: Organización y Planificación de la Seguridad de la Información

Sección II: Alineación y Estrategias de Seguridad de la Información

Sección III: Brechas e Incidentes de Seguridad

Sección IV: Inversión en Seguridad de la Información

Sección V: Mejores prácticas y estándares internacionales



Organización y planificación de la Seguridad de la Información (SI)

Sección I

Sección I: Organización y planificación de la Seguridad de la Información (SI)

Estructura Organizativa

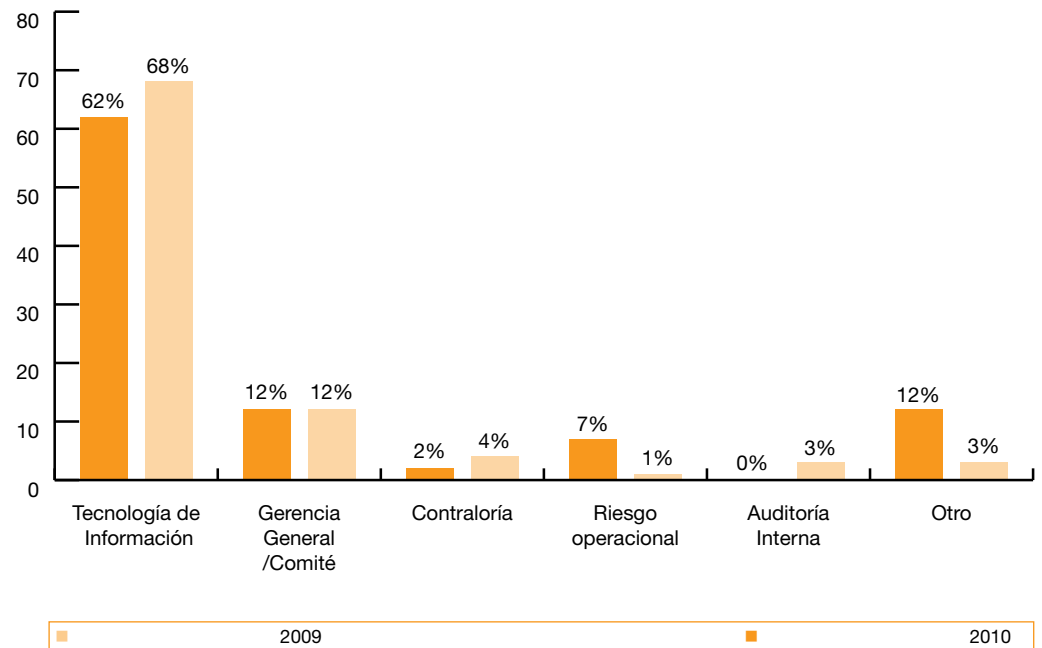
Los resultados obtenidos de la presente encuesta, indican que apenas un 5% de los encuestados no poseen una estructura encargada de dirigir y supervisar los procesos de la FSAI¹, esta es una tendencia esperada si lo comparamos con los años anteriores y se toma en cuenta las regulaciones locales e internacionales, como es el caso de la “Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y el Línea para los Entes Sometidos a Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras”, que indica que para el sector bancario debe existir una función o unidad de seguridad de la información, independiente del área de Tecnología de Información, Auditoría y Riesgo.

En cuanto a la línea de autoridad o reporte, el 62% de las empresas encuestadas manifestaron que las actividades de la FSAI dependen de la unidad de Tecnología de Información, mostrando un decrecimiento de 6 puntos porcentuales en relación al año anterior, lo cual puede explicarse por la tendencia a la adopción de regulaciones locales e internacionales y una eventual maduración de la FSAI.

Asimismo, se observa un incremento de seis puntos porcentuales de las empresas que reportan al área de Riesgo Operacional y se mantiene la proporción de aquellas que se encuentran adscritas a la Gerencia General/Comité. Por otra parte, también se muestra el aumento de otras unidades de reporte, tal como se muestra en la Figura N° 2.

Figura N° 2. Estructura de Reporte de la FSAI

P. ¿De qué Departamento/Unidad depende la Función de Seguridad de la Información en su empresa?



¹Función de Seguridad de Activos de Información

Sección I: Organización y planificación de la Seguridad de la Información (SI)

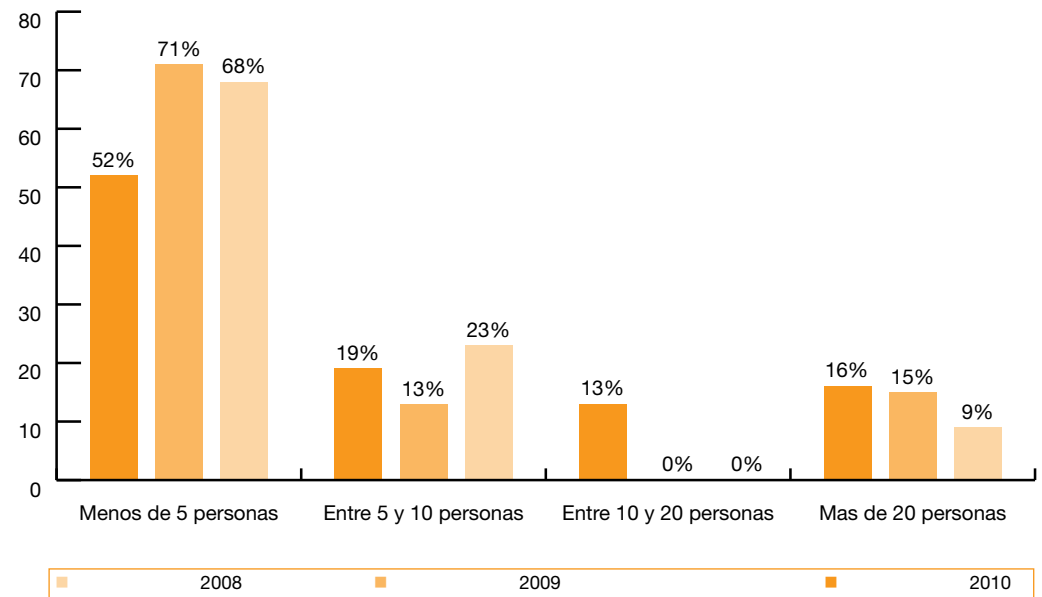
Estructura Organizativa y nivel de reporte

En las organizaciones donde existe una FSAI formalmente constituida, éste estudio indica que al igual que en años anteriores existe un alto porcentaje donde la estructura organizativa está conformada por menos de cinco personas (52%).

Por otro lado, la categoría “Entre 10 y 20 personas” aumentó trece puntos porcentuales en relación al año anterior, mientras que la categoría “Menos de 5 personas” disminuyó diecinueve puntos en relación al año anterior, lo que puede interpretarse como un incremento en la complejidad de las estructuras de la FSAI.

Figura N° 3: Número de personas que conforman la FSAI en las empresas venezolanas

P. Indique el número de personas que conforman la Función de Seguridad de la Información en su empresa.



52%

Más de la mitad de las estructuras FSAI encuestadas está formada por menos de cinco personas

Sección I: Organización y planificación de la Seguridad de la Información (SI)

Políticas y Procedimientos: Gestión de la Función de Seguridad de la Información

Uno de los aspectos que recurrentemente se incluye en la encuesta, está relacionado con la existencia de políticas y procedimientos de Seguridad, su nivel de formalización, divulgación, monitoreo y cumplimiento de los procedimientos.

Es así como este año la interrogante está enfocada en conocer no sólo de la existencia de las políticas y procedimientos sino a conocer el nivel de administración de éstos por parte de la Organización.

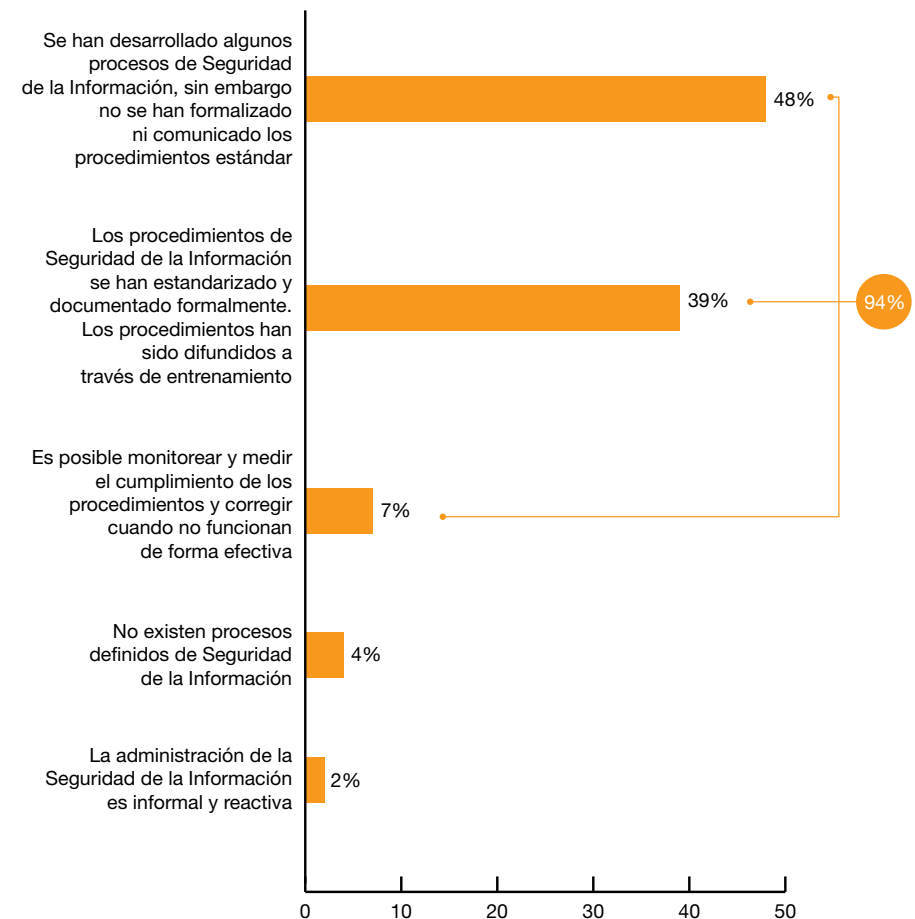
Como se observa en la Figura N° 4, un total de 94% de las empresas ha desarrollado políticas y procedimientos de Seguridad de la Información, sin embargo sólo el 39% de éstas empresas las mantienen formalizadas y difundidas, y tan solo un 7% de éste grupo monitorea y mide su cumplimiento.

Esto puede explicarse considerando que el ciclo de vida de la seguridad de información plantea como primeras acciones la definición de las mencionadas políticas, y luego la adopción de medidas de monitoreo y mejora continua. Bajo esta premisa, los resultados de esta pregunta sugieren que para la mayoría de las empresas participantes, la FSAI se encuentra en una etapa temprana de su estructuración.

94% de las empresas encuestadas ha desarrollado políticas y procedimientos de Seguridad de la Información.

Figura N° 4: Nivel de madurez en la adopción de Políticas y Procedimientos en las empresas

P. ¿Cómo considera se encuentra actualmente la Función de Seguridad de la Información en su Organización?



Sección I: Organización y planificación de la Seguridad de la Información (SI)

Definición del Plan Estratégico de Seguridad de la Información (SI)

El Plan Estratégico de Seguridad de la Información permite a las organizaciones orientar las estrategias de seguridad para mitigar los riesgos derivados por el uso de la tecnología, siendo cada vez de mayor relevancia establecer metas de mediano y largo plazo para la seguridad de información.

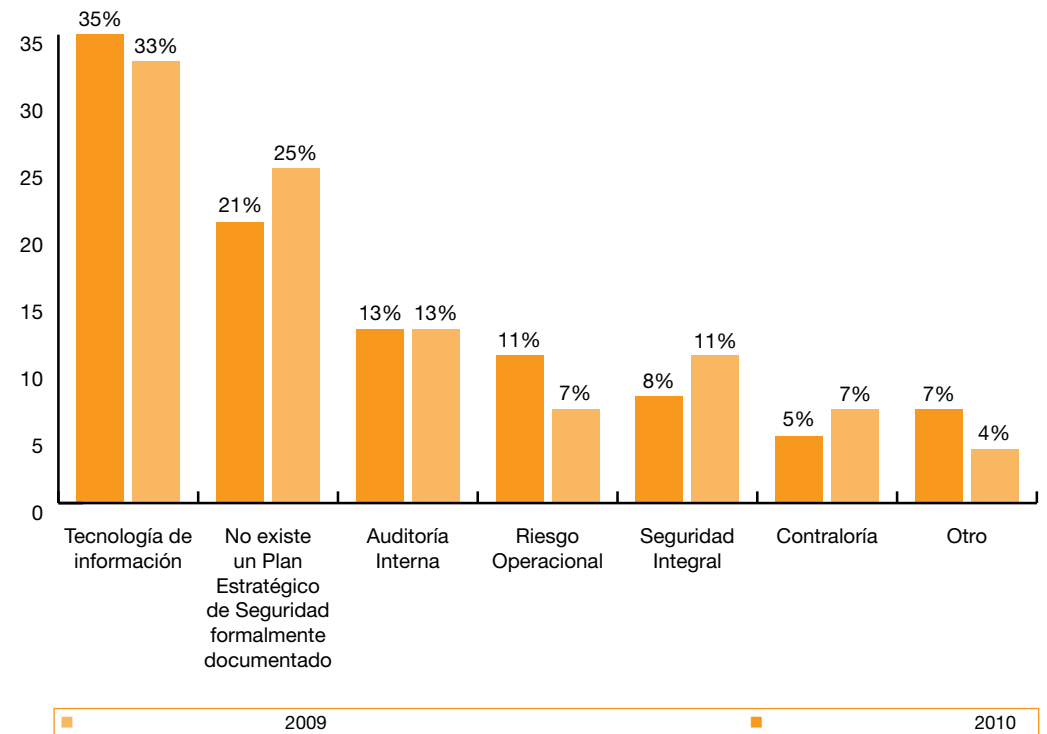
Sin embargo, la existencia de un plan estratégico de SI permanece con una baja prioridad de organizaciones venezolanas. Así lo demuestra, la respuesta de los encuestados al consultarle sobre la existencia de un Plan Estratégico de Seguridad, donde se señala que sólo 21% no posee la definición del Plan, disminuyendo en 4 puntos en relación al año anterior.

Por otra parte, se mantiene con mayor porcentaje en relación al año anterior el área de participación en la definición del Plan Estratégico de Seguridad de la Información, representado por el área de Tecnología de Información con un 35%, dos puntos adicionales versus la encuesta pasada.

Es importante recordar que la ausencia de un Plan Estratégico de Seguridad, dificulta la determinación de las actividades de seguridad que permitan identificar, crear y agregar valor a los procesos de negocio y por ende dificulta el cumplimiento de los objetivos de la FSAI y de la organización.

Fig.N° 5: Distribución de las unidades que participan en la definición del Plan Estratégico de Seguridad

P. ¿Qué áreas de la Organización participan en la Definición del Plan Estratégico de Seguridad de la Información?



Sólo el 21% de las empresas encuestadas indicó no poseer un Plan Estratégico de Seguridad de Información

21%

Sección I: Organización y planificación de la Seguridad de la Información (SI)

Frecuencia de reuniones

La participación de la alta gerencia en temas de SI es clave para alcanzar los objetivos y uno de los principales indicadores de su nivel de involucramiento es la conformación o incorporación de SI en reuniones de alto nivel y la frecuencia de estas reuniones.

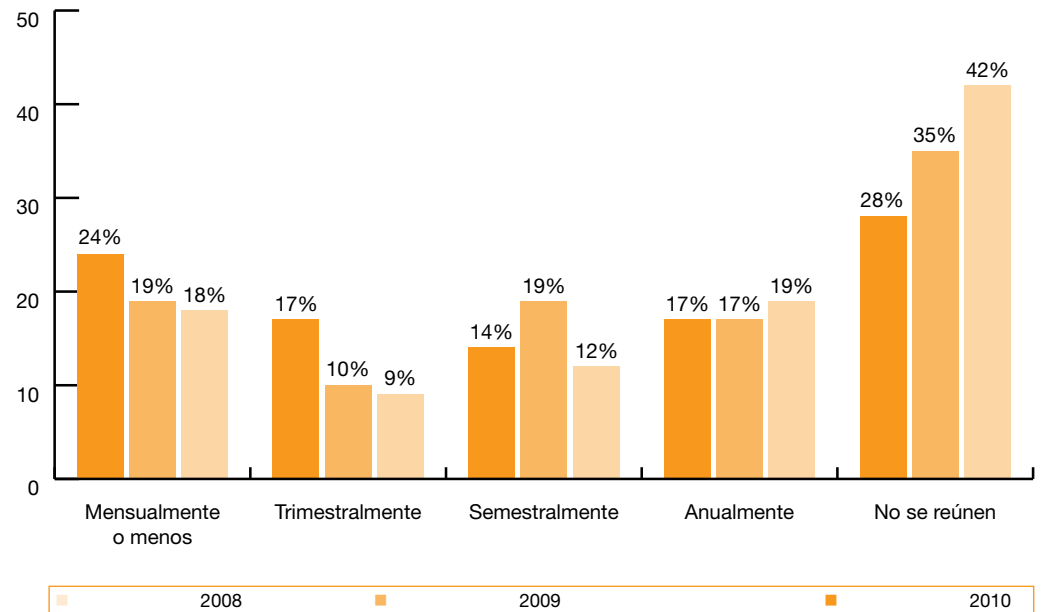
Este año se percibe un incremento en la ejecución y frecuencia de reuniones orientadas a abordar temas de SI. Solo 28% de los encuestados respondió no ejecutar este tipo de reuniones, lo que representa siete puntos porcentuales menos que el año anterior, afirmando la tendencia acumulada de un descenso.

El otro aspecto resaltante es que la práctica con mayor aceptación es la reunión mensual, y la reducción sensible en la ejecución de reuniones semestrales.

En la Figura N° 6 se muestra la distribución de las respuestas para ésta pregunta.

Figura N° 6: Frecuencia de reuniones para el análisis de los temas de SI

P. ¿Con qué frecuencia la Alta Gerencia, Comité de Seguridad, Riesgo o Tecnología se reúnen para discutir las necesidades de la Seguridad de la Información y objetivos del negocio?



Sección I: Organización y planificación de la Seguridad de la Información (SI)

Principales retos en la Estrategia de Seguridad de la Información (SI)

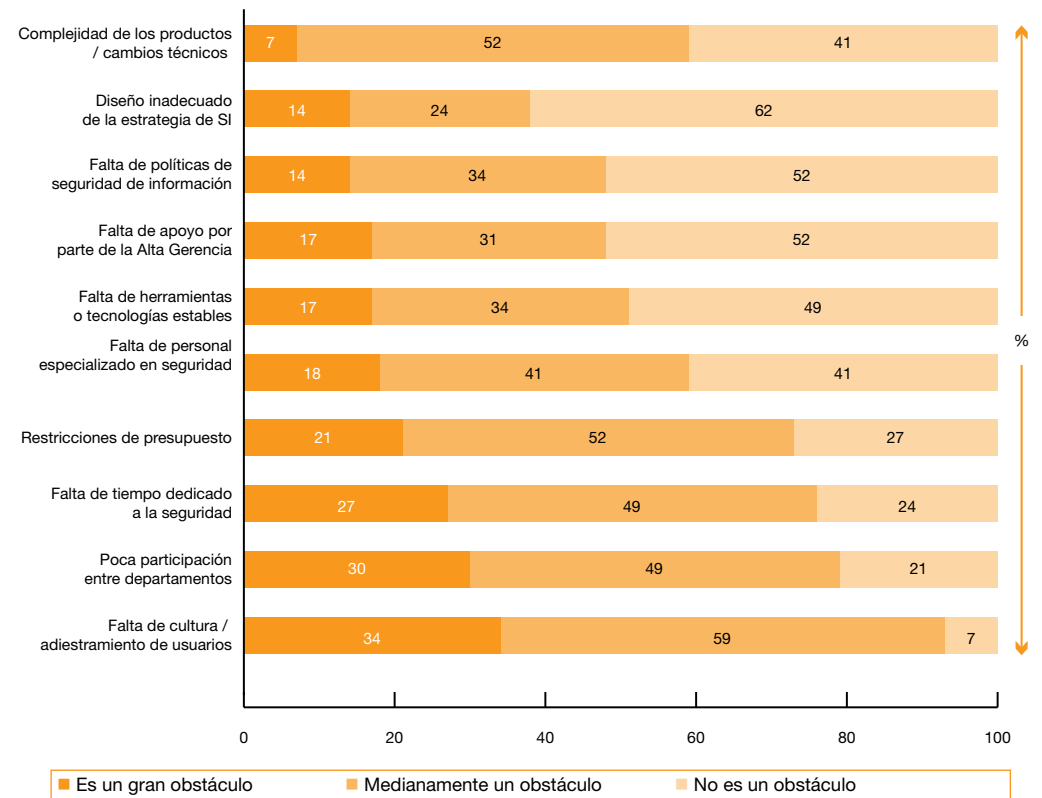
Entre los principales obstáculos que presentan las organizaciones para la práctica de la SI, los resultados indican que el mayor de ellos es la falta de cultura y adiestramiento de los usuarios (34%), seguido de la poca participación entre los departamentos (30%) y la falta de tiempo dedicado a la seguridad (27%).

El cuarto mayor obstáculo está representado por la restricción de presupuesto (21%), sin embargo, el 45% indicó que aumentaría en relación al año anterior y sólo un 7% indicó que disminuirá.

Estas cifras parecieran indicar que el tema presupuestario pierde relevancia como inhibidor de la SI, dando paso a temas relacionados con la organización y las personas. Ver Figura N° 7 con los resultados.

Figura N° 7: Principales obstáculos para la implantación de un Plan Estratégico de SI

P. ¿Cuáles son los principales obstáculos que presenta su negocio para la práctica de seguridad de activos de información e indique en qué medida?



Alineación y estrategias de Seguridad de la Información

Sección II

Sección II: Alineación y Estrategias de Seguridad de la Información

Prioridad en soluciones de SI para la Organización

La adopción de soluciones en SI, implica no sólo la identificación de la mejor herramienta o proveedor que cumpla con los objetivos de negocio sino también el establecimiento de un ambiente de control que haga un uso efectivo de estos recursos.

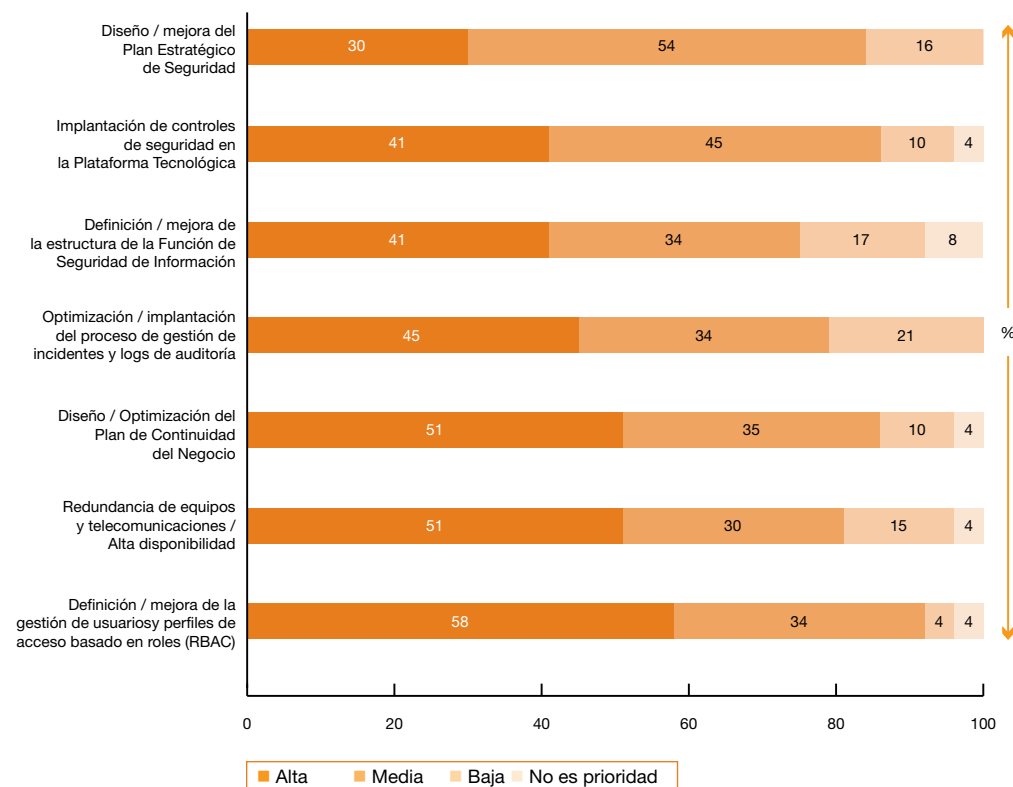
Esta sección recoge información sobre las soluciones estratégicas de seguridad que las empresas venezolanas consideran de importancia. De nuestra pregunta a los encuestados sobre las principales estrategias de seguridad y su prioridad, el primer lugar lo ocupa la definición / mejora de la gestión de usuarios y perfiles de acceso basado en roles (RBAC) (58%), seguido de soluciones para la redundancia de equipos y telecomunicaciones para mejorar la disponibilidad de los servicios (51%) y el diseño u optimización del Plan de Continuidad de Negocio (51%).

Por el contrario, entre las soluciones con menor porcentaje en cuanto a importancia se encuentra el diseño u optimización del Plan Estratégico de Seguridad (30%) y la implantación de de controles de seguridad en la plataforma tecnológica (41%). La distribución de las respuestas pueden observarse en la Figura N° 8.

Comparando estas cifras con las de años anteriores, las tres principales prioridades han permanecido en esta posición. Pareciera entonces que son proyectos que por sus características resultasen difíciles de concretar, pese a la necesidad que SI identifica en su ejecución. En la siguiente pregunta se ahonda sobre la puesta en marcha de dichas iniciativas.

Figura N° 8: Principales soluciones estratégicas de SI e importancia en su adopción

P. Indique la importancia de las siguientes soluciones estratégicas en su organización:



Sección II: Alineación y Estrategias de Seguridad de la Información

Nivel de adopción de soluciones estratégicas

Para complementar el análisis anterior, se consultó sobre el nivel de adopción de las soluciones estratégicas descritas en la Figura N° 9 en las empresas venezolanas.

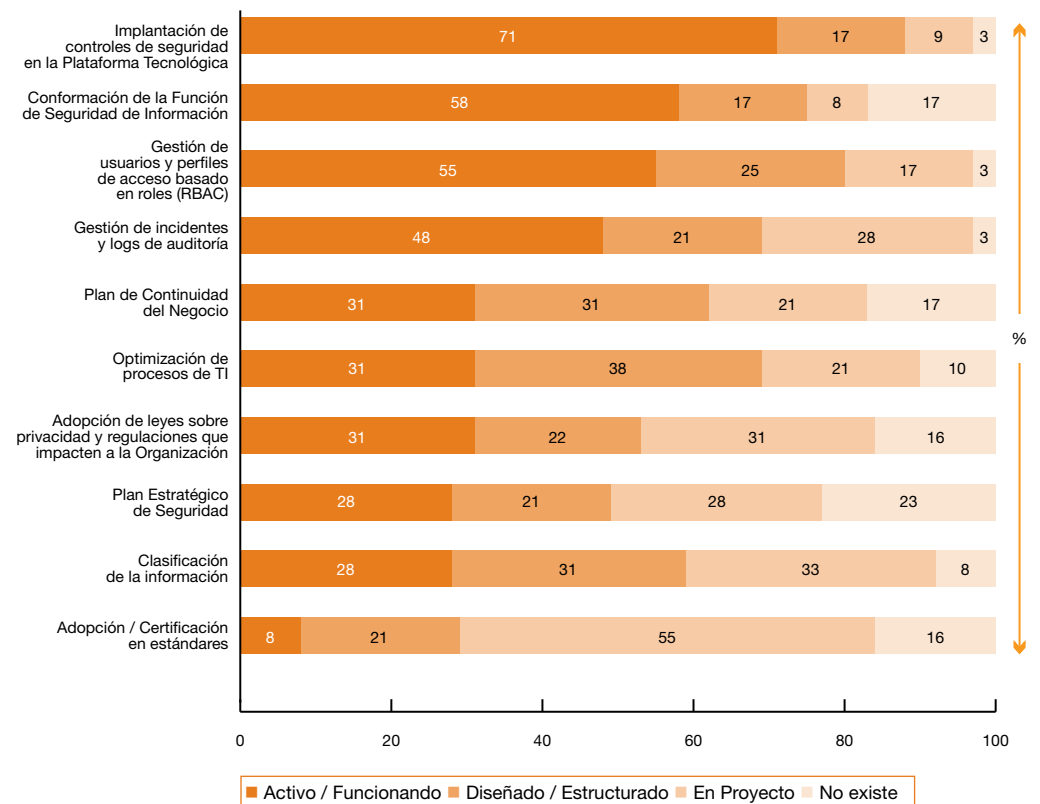
La implantación de controles de seguridad en la plataforma tecnológica se presenta con amplio margen como la primera iniciativa adoptada (71%) y de las que presenta menos índice de inexistencia.

La conformación de la función de seguridad de la información (58%) y gestión de usuarios y perfiles de acceso basado en roles (RBAC) (55%) se presenta muy cerca en los resultados obtenidos, sin embargo es notable que RBAC supere a la conformación del FSAI si consideramos también la respuesta de aquellas empresas que manifestaron tenerlo en proyecto.

Recordemos que esta iniciativa también se presentó como una de las prioridades para las organizaciones durante el año 2010, lo que apunta a sugerir que la gestión de identidades es una tendencia del mercado, pero a su vez un proyecto complejo que se extiende en su ejecución.

Figura N° 9: Nivel de adopción de las soluciones estratégicas de SI

P. Indique el nivel de adopción de las siguientes soluciones estratégicas en su Organización



Sección II: Alineación y Estrategias de Seguridad de la Información

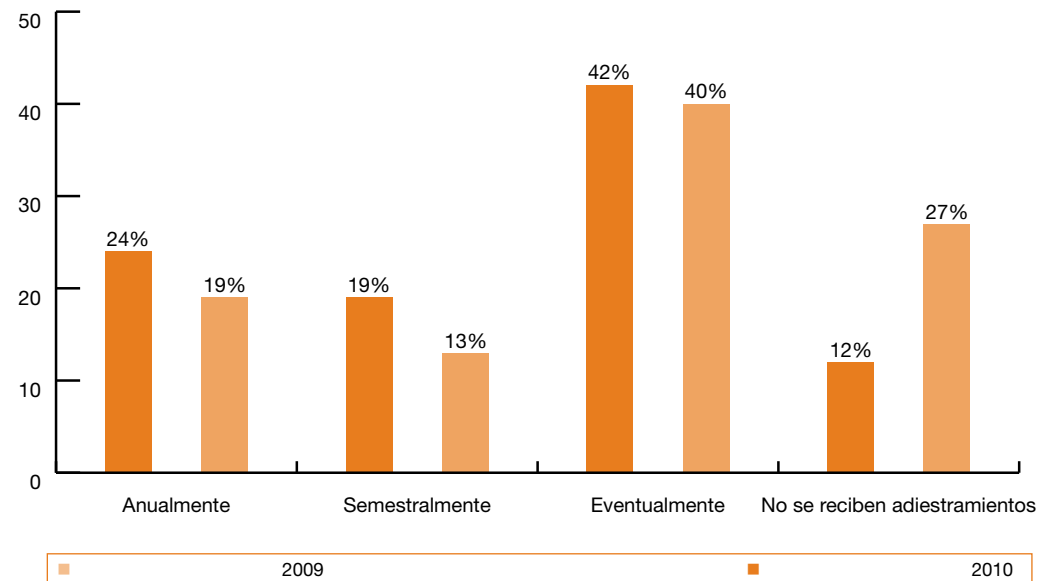
Adiestramiento de Personal

Por segundo año consecutivo se consultó sobre la frecuencia de los adiestramientos impartidos al personal de la FSAI: Sólo el 12% de los entrevistados indicó no recibir adiestramiento, lo cual representa una disminución en quince puntos porcentuales con respecto al año anterior.

Se puede apreciar cómo este resultado es consistente con la frecuencia de los adiestramientos, donde además se identifica un mayor incremento en la planificación anual o semestral de cursos de formación al personal de la FSAI, con respecto al año anterior.

Figura N° 10: Frecuencia en el adiestramiento del personal de la FSAI

P. ¿Cuál es la frecuencia de los adiestramientos del personal encargado de la seguridad de los activos de información?



Sección II: Alineación y Estrategias de Seguridad de la Información

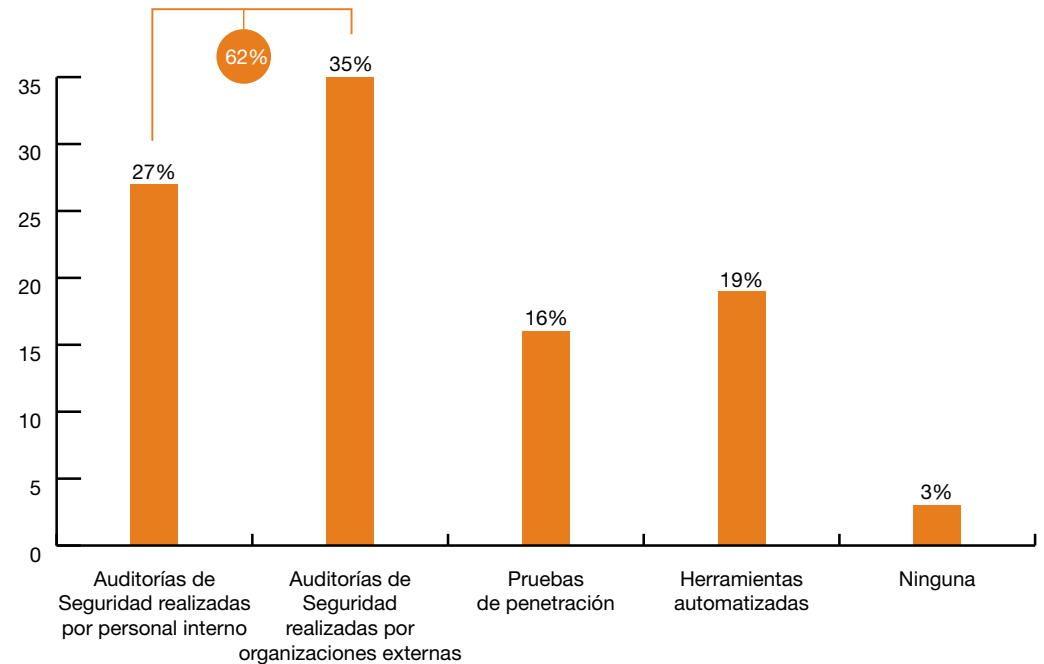
Técnicas usadas

La técnica más utilizada por las empresas venezolanas para evaluar la efectividad del ambiente de control interno y Seguridad de Información, son las Auditorías de Seguridad ejecutadas por organizaciones externas a la Compañía (35%) que, seguida de las Auditorías de Seguridad realizadas por personal interno de la Compañía (27%), agrupan al 62% de los encuestados.

Este resultado guarda relación con los hallazgos de años anteriores, pero observando una disminución de las auditorías internas a favor de tercerizar estas evaluaciones, y un leve repunte de dos puntos porcentuales en el uso de herramientas automatizadas. Ver Figura N° 11.

Figura N° 11: Técnicas utilizadas para evaluar la efectividad del ambiente de control y la gestión de SI

P. ¿Cuáles técnicas son usadas en la Organización para evaluar la efectividad del ambiente de control interno y Seguridad de Información? (Puede seleccionar más de una respuesta)



Sección II: Alineación y Estrategias de Seguridad de la Información

Servicios tercerizados

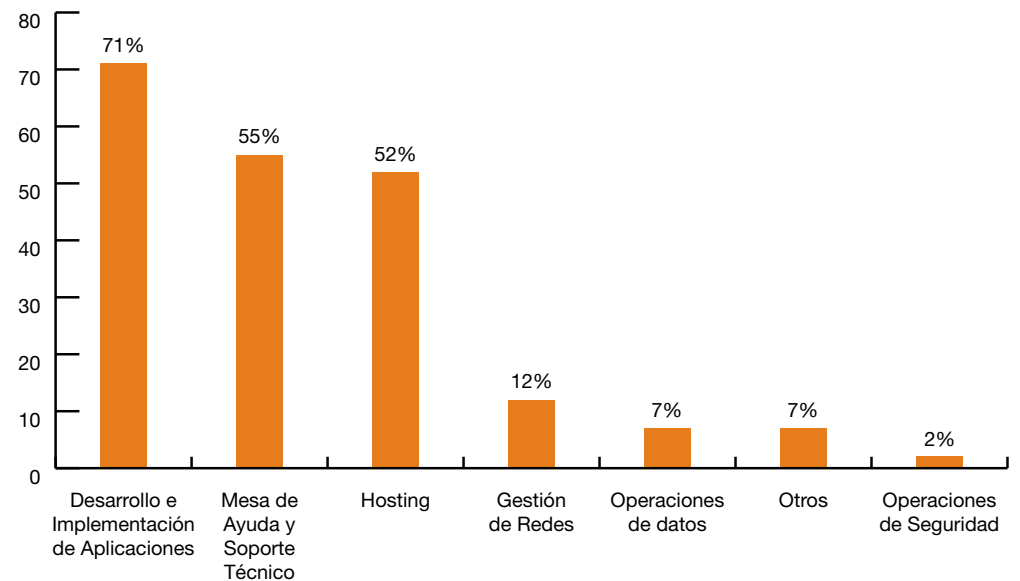
Se consultó a las empresas venezolanas sobre el uso de servicios de terceros (outsourcing) en procesos o actividades relacionadas con servicios de SI.

De acuerdo con los resultados se obtiene que los más servicios más utilizados son: Desarrollo e implementación de aplicaciones (71%), Mesa de Ayuda y Soporte Técnico (55%) y Hosting (52%), tal y como se muestra en la Figura N° 12.

En general, en la totalidad de las áreas consultadas se observó crecimiento, particularmente en la Mesa de Ayuda y Soporte Técnico, ocupando el segundo lugar de las opciones de tercerización más utilizadas.

Figura N° 12: Servicios de TI que usualmente son tercerizados en las empresas venezolanas

P. ¿Cuál es el alcance de los servicios prestados por terceros en procesos o actividades de tecnología y/o seguridad?
(Puede marcar más de una respuesta)



Sección II: Alineación y Estrategias de Seguridad de la Información

Riesgos derivados de la tercerización

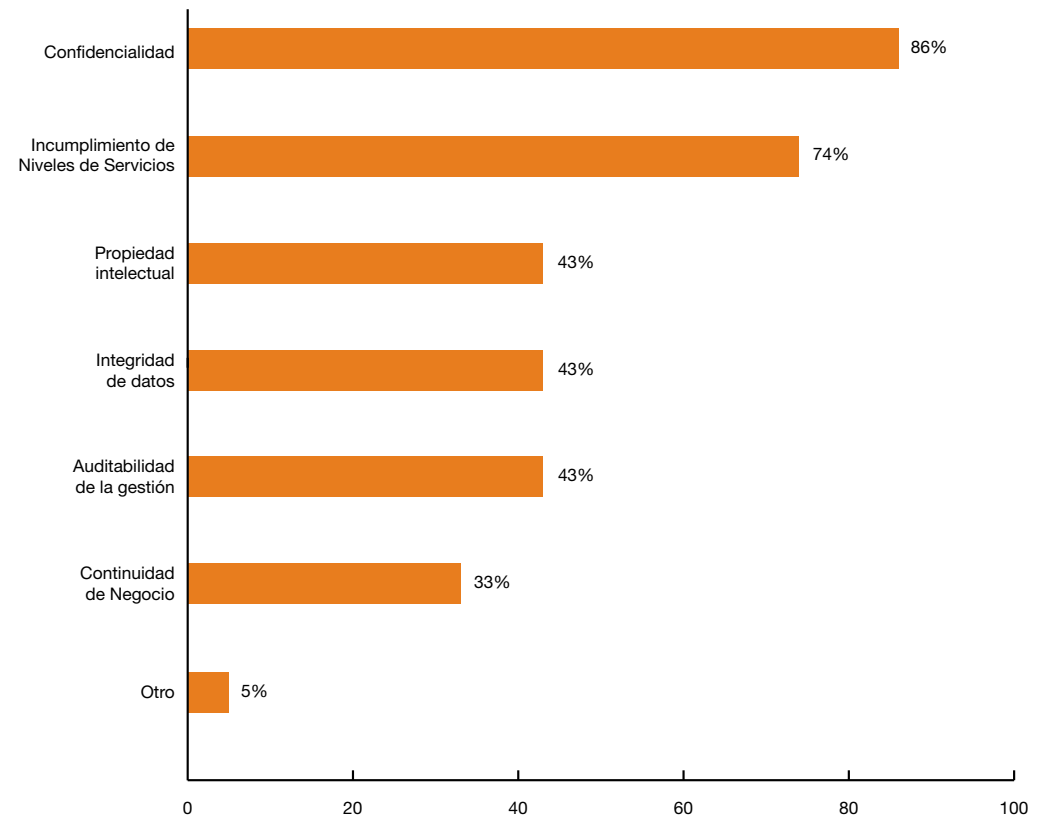
Es importante recordar que en los procesos o actividades que son tercerizados, se está transfiriendo no sólo un servicio sino que también se transfieren los riesgos que se derivan de este, sin obviar que los riesgos impactarían no sólo a la contratista sino también a la contratante.

Así lo considera, por ejemplo, la normativa emitida por la SUDEBAN denominada “Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y el Línea para los Entes Sometidos a Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras”, que indica que para el sector bancario las obligaciones que impone esta norma deben ser igualmente transferidas a sus proveedores.

Ahora bien, los principales riesgos que las empresas han identificado al transferir procesos o actividades a un tercero, son la Confidencialidad (86%), seguido de Incumplimiento de Niveles de Servicios (74%) y la Propiedad Intelectual, Integridad de Datos y la Auditabilidad de la Gestión.

Figura N° 13: Riesgos derivados de la delegación de funciones y servicios a terceros

P. ¿Cuáles son los riesgos que usted considera existen con la delegación de funciones a terceros?
(Puede marcar más de una respuesta)



Brechas e incidentes de seguridad
Sección III

Sección III: Brechas e incidentes de seguridad

Tecnologías bajo la atención de la FSAI

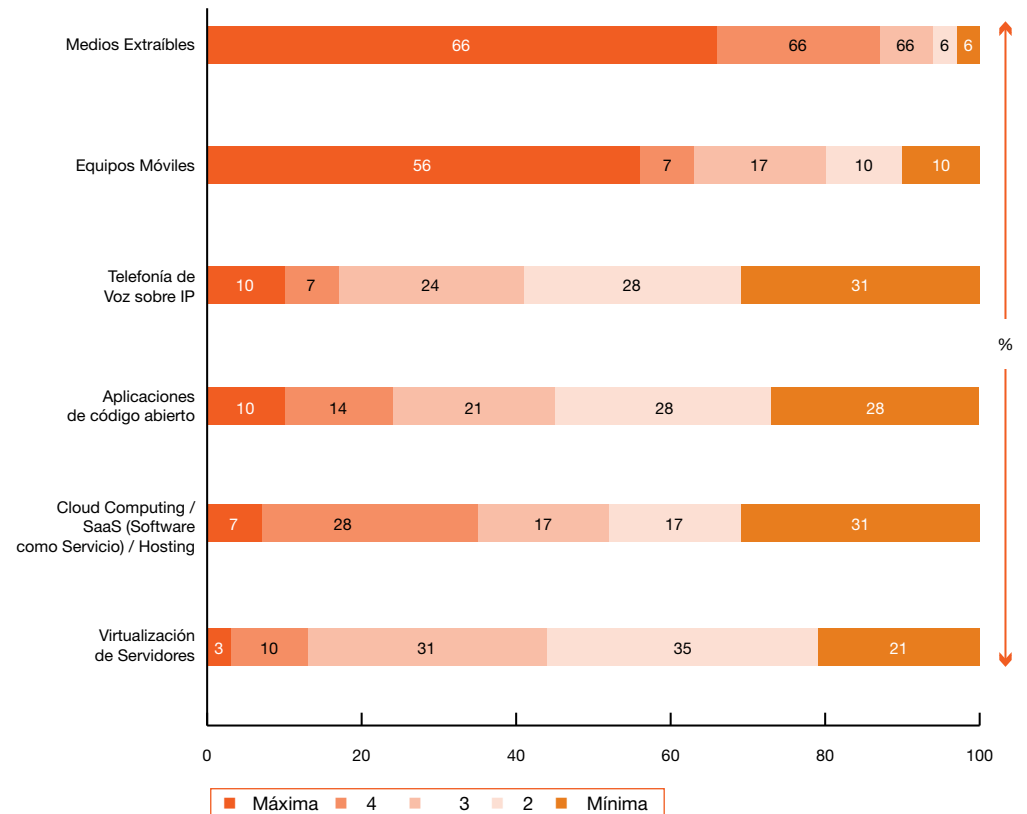
En cuanto a las principales preocupaciones en relación a los temas de seguridad de la información de las empresas encuestadas, se indagó sobre cuáles tecnologías han sido identificadas como una preocupación de seguridad de la información.

El resultado que muestra la Figura N° 14, revela como la mayor preocupación a los medios extraíbles (66%) y los equipos móviles (56%), tecnologías que si las comparamos con los resultados obtenidos de las dos últimas encuestas de Seguridad de la Información, continúan siendo las principales preocupaciones, pero notándose una disminución de diez puntos porcentuales en medios extraíbles y un crecimiento equivalente en equipos móviles.

Otro aspecto que destaca es el crecimiento de las soluciones de “Cloud Computing” y SaaS² como segunda mayor preocupación, así como la sensible reducción en los temas de virtualización, lo que podría interpretarse como un crecimiento en el interés y uso de las organizaciones en soluciones en la nube, y la confianza ganada por virtualización durante el año.

Figura N° 14: Nivel de riesgo en tecnologías según las empresas encuestadas

P. Indique, según una escala del 1 al 5, ¿Cuál de las siguientes tecnologías ha identificado como una preocupación en la seguridad de la información en su Organización? (5 representa la máxima atención y 1 la mínima)



²Software como servicio (*software as a service*)

Sección III: Brechas e incidentes de seguridad

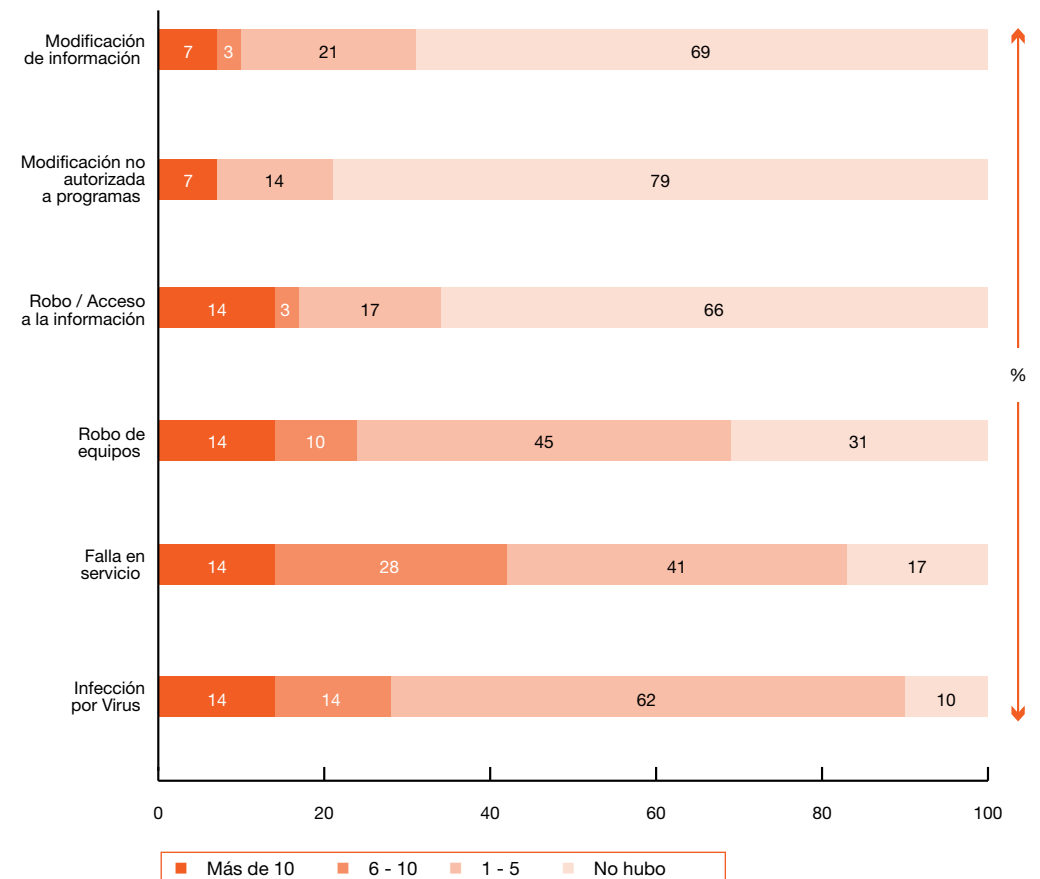
Incidentes de Seguridad: impacto, causas y efectos

En relación con los incidentes de seguridad que han afectado a las empresas venezolanas en éste último año, se evidencia un reordenamiento en relación con los principales incidentes: Nuevamente aparece la infección por virus como la primera causa, seguida este año por la falla en servicio, que sube del cuarto al segundo lugar de los principales incidentes en las organizaciones. El robo de portátiles retrocede a un tercer lugar y robo o acceso a la información se ubica como el cuarto incidente de mayor ocurrencia en las organizaciones.

Es importante destacar que los resultados presentados en la Figura N° 15 evidencian que al menos 69% de las organizaciones encuestadas ha tenido al menos un evento de seguridad de cada tipo de los ubicados en los primeros tres lugares.

Figura N° 15: Número de incidentes de seguridad de SI en el último año

¿Cómo se ha visto afectada su Compañía con relación a incidentes de seguridad en el último año?



Sección III: Brechas e incidentes de seguridad

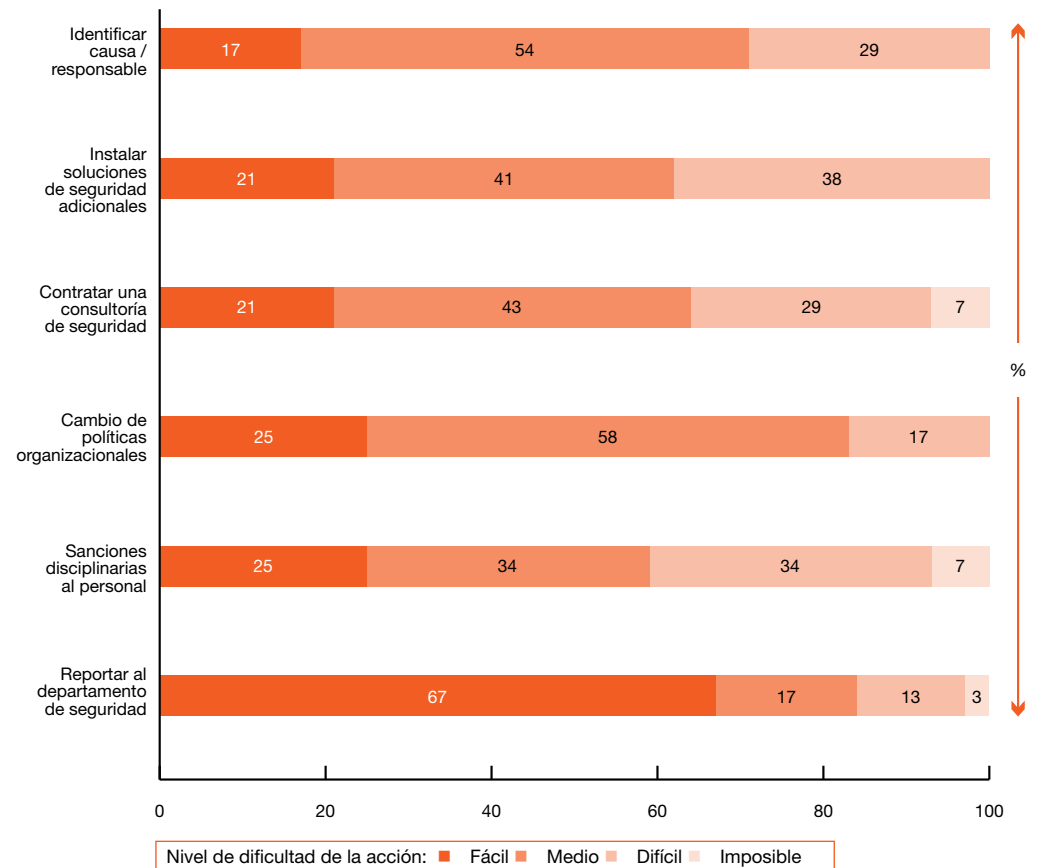
Acciones tomadas para la gestión de incidentes

Sobre las acciones realizadas, se le consultó a las empresas venezolanas ¿Cuál ha sido la acción tomada al detectar un incidente de seguridad de la información y el nivel de dificultad de su ejecución?, siendo los rubros con mayor porcentaje la acción de reporte al departamento de seguridad (67%), sanciones disciplinarias al personal (25%), cambio de políticas organizacionales (25%). En la figura N° 16 se describe la distribución de las respuestas.

En comparación con los resultados del año anterior, se evidencia un crecimiento importante en la participación de la FSAI en la reacción ante el evento, y una disminución en el número de respuestas que indican como “imposible” ejecutar cualquiera de las acciones allí planteadas.

Figura N° 16: Acciones tomadas para gestionar los incidentes de seguridad

P. ¿Cuál ha sido la acción tomada al detectar un incidente de seguridad de la información y el nivel de dificultad de su ejecución?



Sección III: Brechas e incidentes de seguridad

Principales causas de ocurrencia de incidentes

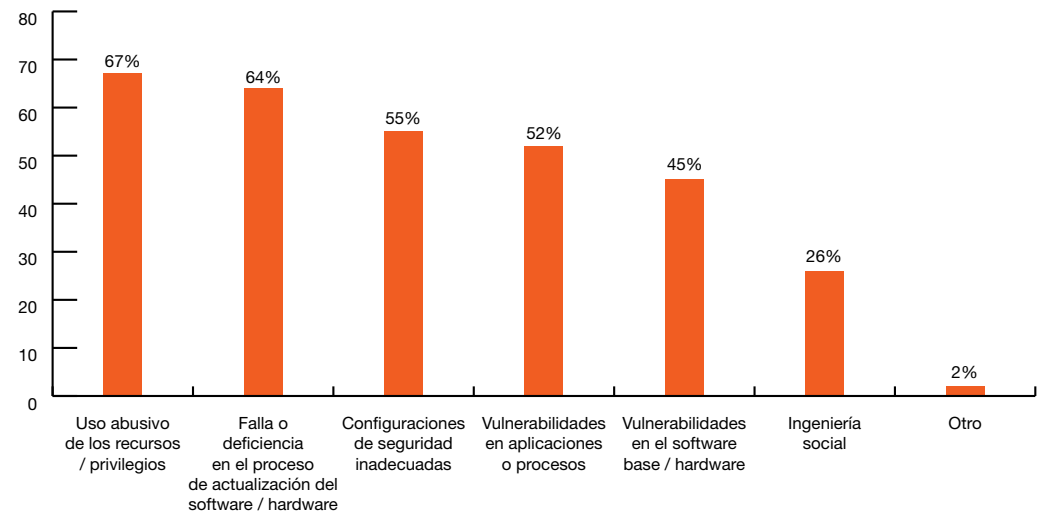
En relación con las causas que permitieron el incidente, encontramos un comportamiento consistente con las respuestas de preguntas anteriores, con ligeras variaciones con respecto a los resultados de años anteriores.

Las principales causas permanecen siendo el Uso abusivo de los recursos / Privilegios y Falla o deficiencia en el proceso de actualización del software / Hardware, seguido de configuraciones de seguridad inadecuadas.

La principal variación con respecto al año pasado -y que parece ser una tendencia, ya que se repite por tercer año consecutivo- es la disminución de “Configuraciones de seguridad inadecuadas”, como causa del incidente, la cual es desplazada al tercer lugar este año.

Figura N° 17: Principales causas de la ocurrencia de incidentes de SI

P. ¿Cuáles fueron las causas de la ocurrencia de los incidentes de seguridad? (Puede marcar más de una respuesta)



Sección III: Brechas e incidentes de seguridad

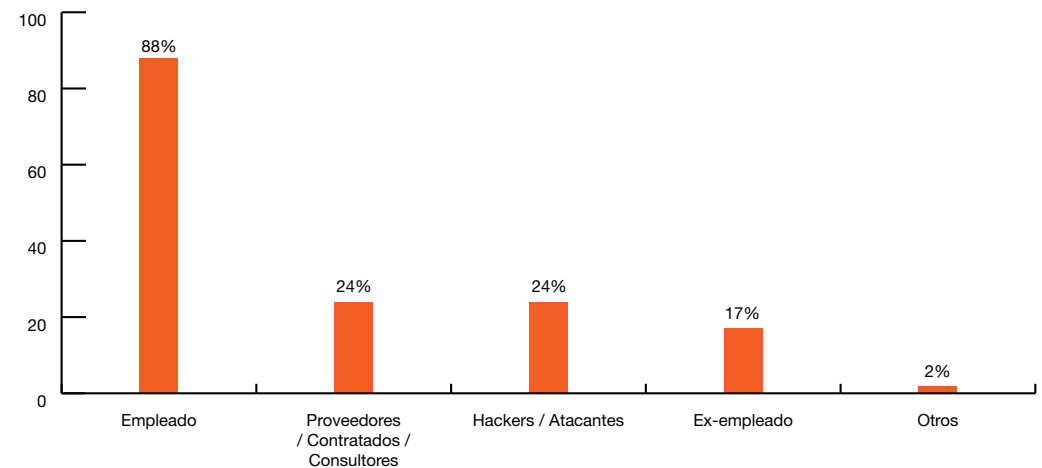
Origen de los incidentes reportados

Aunado al resultado anterior, tenemos que los encuestados manifiestan que éstos incidentes fueron imputados a personal empleado (88%), doce puntos porcentuales por encima que los dos últimos años, muy distanciado del resto del resto de los grupos causantes.

Este resultado es recurrente con respecto a años anteriores y ratifica que las empresas siguen siendo víctimas principalmente de su personal, situación que se ha visto incrementado notablemente en este año, reforzando de esta forma el criterio que que las personas que conocen a las organizaciones son potencialmente más riesgosos. Ver Figura N° 18.

Figura N° 18: Origen de los incidentes de SI reportados entre los años 2008 y 2010

P. ¿Cuál considera Ud. fue el origen de los incidentes de seguridad de información reportado en su organización?
(Puede marcar más de una respuesta)



Sección III: Brechas e incidentes de seguridad

Incidentes de Seguridad: impacto, causas y efectos (continuación)

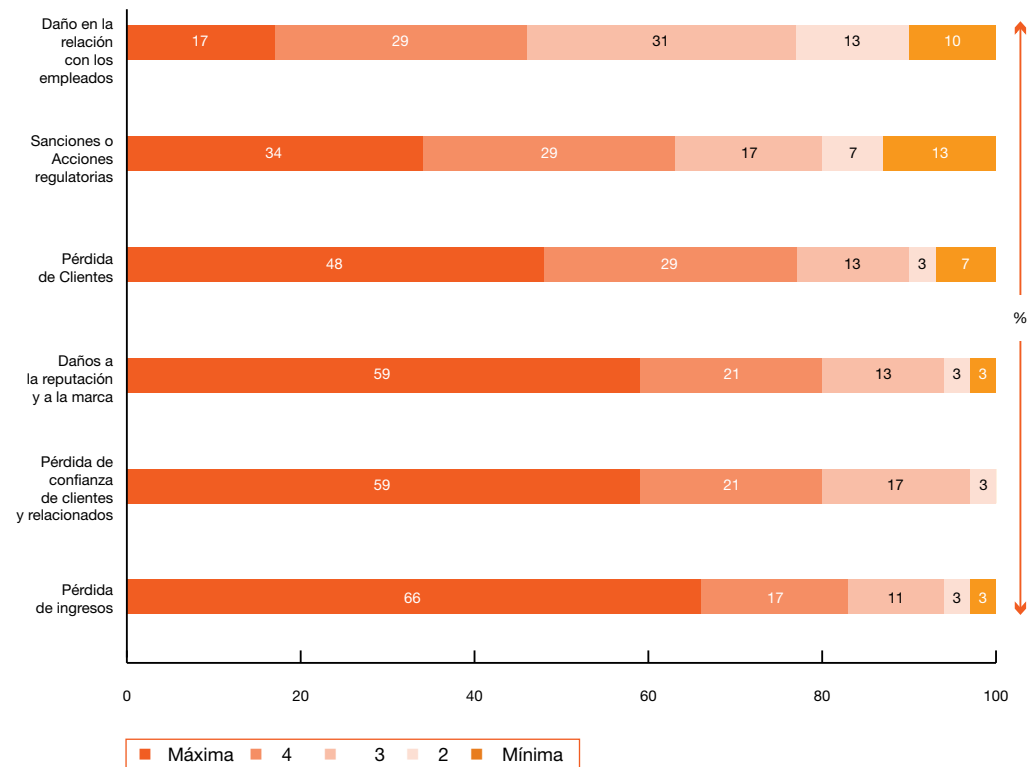
Las consecuencias pueden ser diversas, desde la pérdida de operatividad de la plataforma tecnológica, hasta la afectación de la imagen y reputación de la organización. En este contexto, se consultó a las empresas las potenciales consecuencias de perder o comprometer información sensible de su Organización, donde 5 representa la máxima atención y 1 la mínima.

El 66% de los encuestados coincide en señalar que la pérdida de ingresos es la principal consecuencia, seguida de la pérdida de confianza por parte de clientes y relacionados (59%) y daños a la reputación y a la marca (59%).

En la Figura N° 19 se puede observar la distribución de los resultados.

Figura N° 19: Consecuencias de la pérdida, falta de integridad y disponibilidad de información

P. Enumere, en orden de prioridad, en una escala del 1 al 5, las consecuencias si se perdiera, comprometiera o no estuviese disponible información sensible de su Organización. (5 representa la máxima atención y 1 la mínima)



Inversión en Seguridad de Información (SI)
Sección IV

Sección IV: Inversión en Seguridad de Información

Inversión en Seguridad de la Información

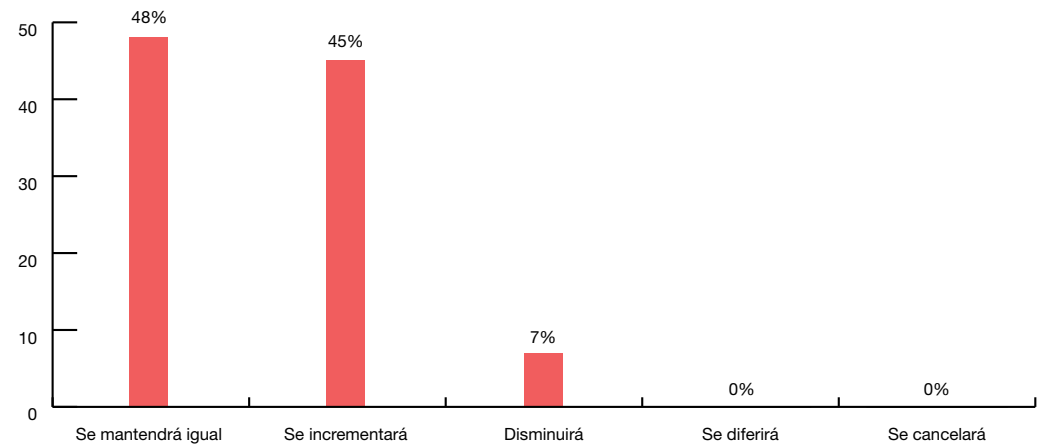
Con relación a la inversión de Seguridad de la Información, en la Figura N° 20 se muestra el comportamiento de la inversión de Seguridad de la Información en las empresas venezolanas para los próximos 12 meses.

Es así que el 45% de las organizaciones, estima que habrá un aumento de la inversión, incremento de dos puntos porcentuales en relación al año anterior.

A pesar de la crisis económica, sólo un 7% de los encuestados estima que ocurrirá una disminución del presupuesto de inversión en relación al año anterior, lo que sigue ratificando el compromiso de las empresas en mantener controles de seguridad eficientes que garanticen la protección de la información.

Figura N° 20: Nivel de inversión en SI para el año 2011

P. En su opinión ¿Cómo considera usted que será la inversión en Seguridad de la Información para los próximos doce (12) meses comparado con el último año?



Sección IV: Inversión en Seguridad de Información

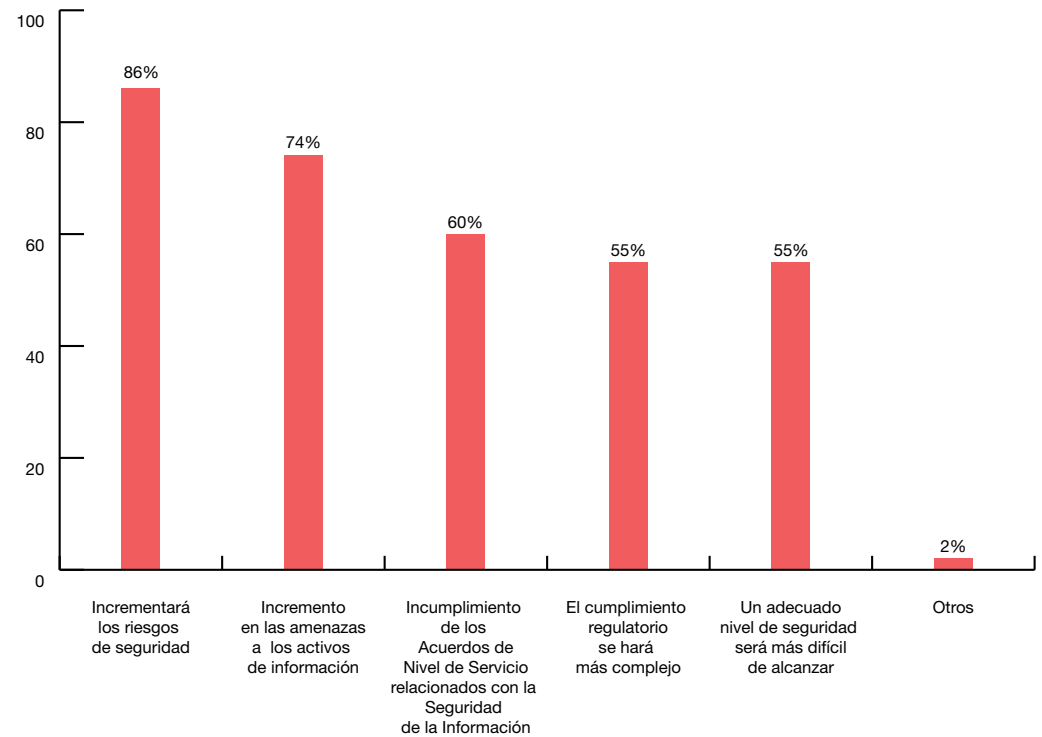
Impacto de una reducción del presupuesto de SI

En el caso de una eventual disminución en el presupuesto de Seguridad de la Información, el 86% de las organizaciones encuestadas manifestó que tal acción traería como consecuencia un incremento en los riesgos de seguridad, seguido de

un 74% que considera que tal acción propiciaría un incremento en las amenazas a los activos de información y un 60% preve incumplimiento de los Acuerdos de Nivel de Servicio relacionados con la Seguridad de la Información.

Figura N° 21: Impacto de una posible reducción del presupuesto de SI

P. ¿Cómo cree usted que puede impactar la reducción de la inversión en Seguridad de la Información? (Puede marcar más de una respuesta)



Sección IV: Inversión en Seguridad de Información

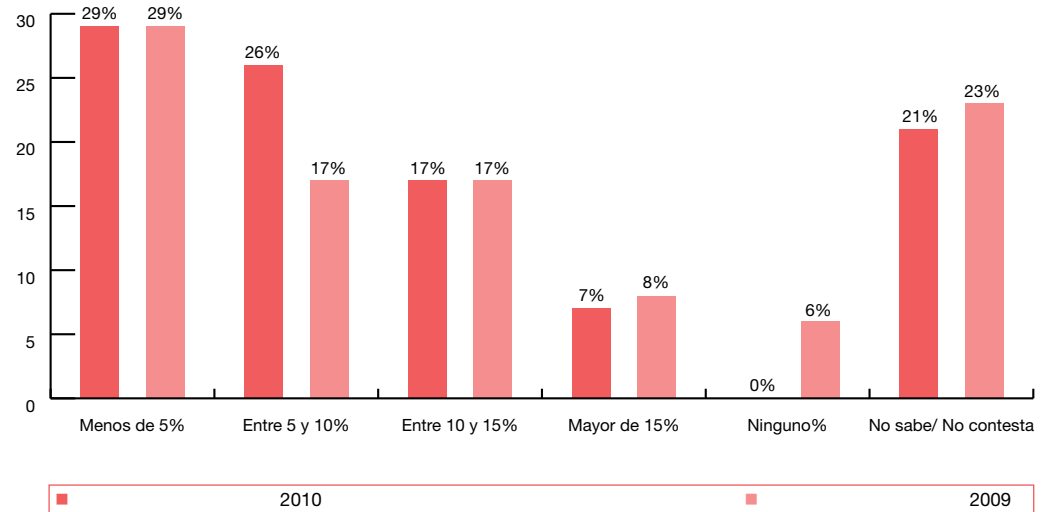
Proporción de presupuesto de SI en relación al presupuesto de TI

Si se compara la porción del presupuesto de Seguridad de la Información con relación al presupuesto de Tecnología de Información, se observa que la mayoría de los encuestados coincide en que esta representa menos del 5% del presupuesto de TI.

Sin embargo, resulta interesante analizar que para el 26% de las empresas encuestadas el presupuesto se ubica entre un 5% y 10%, aumentando este grupo en nueve puntos porcentuales en relación al año anterior.

Figura N° 22: Proporción de presupuesto de SI en relación al presupuesto de TI

P. ¿Cuál es la proporción porcentual, en promedio, del presupuesto de Seguridad de la Información con relación al presupuesto de Tecnología de Información?



Sección IV: Inversión en Seguridad de Información

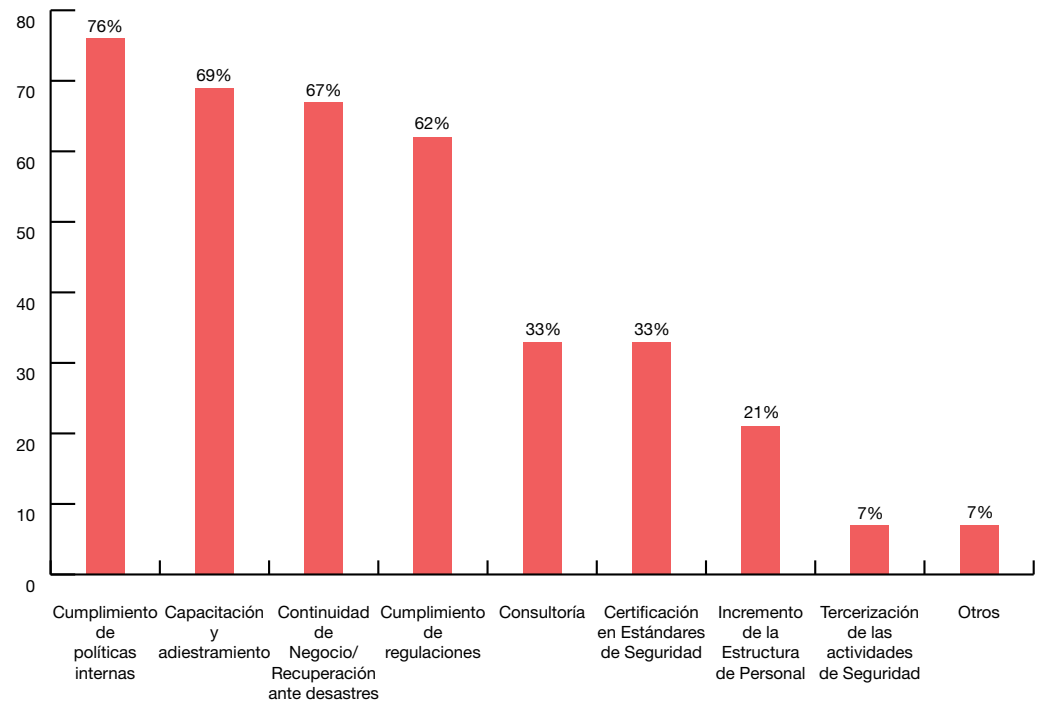
Distribución y uso del presupuesto de SI

La distribución y uso del presupuesto se concentra en el cumplimiento de políticas internas (76%), capacitación y adiestramiento (69%) y la Continuidad de Negocio / Recuperación ante desastres (67%).

Sólo un 7% por ciento de las empresas estima utilizar el presupuesto para la tercerización de las actividades de Seguridad, lo cual parece una respuesta cónsona con las opiniones sobre que la confiabilidad de la información pudiera verse afectada por la tercerización de los procesos o actividades de la FSAI según se reporta en la Sección II de esta encuesta, Figura N° 13.

Figura N° 23: Distribución y utilización del presupuesto de SI

P. ¿Hacia dónde considera usted que está orientada la inversión de Seguridad de la Información en su Organización?
(Puede marcar más de una respuesta)



Sección IV: Inversión en Seguridad de Información

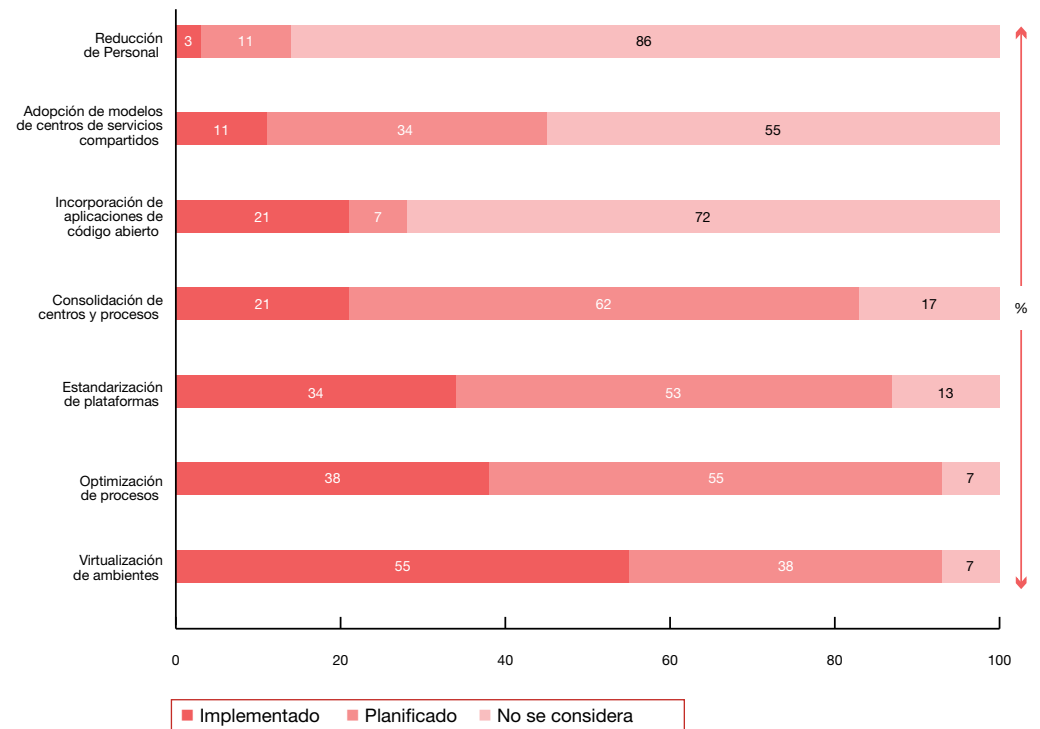
Estrategias para la reducción de costos

Al consultar a las organizaciones ¿Cuál de las siguientes estrategias ha sido considerada por su Organización con el fin de reducir los costos asociados a Tecnología de Información?, respondieron que la virtualización de ambientes (55%) es la estrategia mayormente empleada, seguida de un 38% de la optimización de procesos y un 34% con la estandarización de plataformas.

Contrario a lo que se pudiera pensar, la última estrategia que consideran los encuestados para la reducción de costos en Seguridad y Tecnología de Información es la reducción de personal con un 86%, lo que nos lleva a pensar que las estructuras actuales de se encuentran optimizadas o reducidas a su menor tamaño, requiriendo evaluar otras alternativas.

Figura N° 24: Estrategias utilizadas por las empresas para reducir los costos asociados a TI

P. ¿Cuál de las siguientes estrategias ha sido considerada por su Organización con el fin de reducir los costos asociados a Tecnología de Información?



Sección V: Mejores prácticas de seguridad

Implantación de estándares y mejores prácticas

Al indagar sobre el estatus de adopción e implantación de estándares y mejores prácticas, se observa que el 34% de las empresas venezolanas cuentan con la adopción y operación de ITIL³, nueve puntos porcentuales por encima del año anterior.

Beneficios de la adopción de mejores prácticas

Al consultar a los encuestados sobre los beneficios de la adopción de estos estándares, los resultados indican que el mayor de los beneficios está representado por la estandarización de los procesos de TI y la continuidad del negocio con un 70% cada una, seguido de la mejora en la calidad de los servicios de TI (53%), tal como se muestra en la Figura N° 26.

Esto afirma la efectividad de los esfuerzos en cuanto a la implementación de mejores prácticas.

Figura N° 25: Estatus de implantación de estándares y mejores prácticas de TI

P. Indique el estatus de implantación de los siguientes estándares y mejores prácticas en su organización

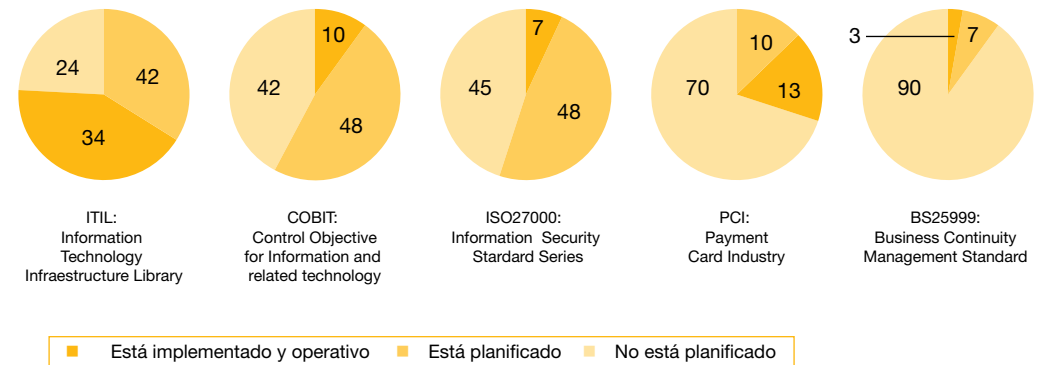
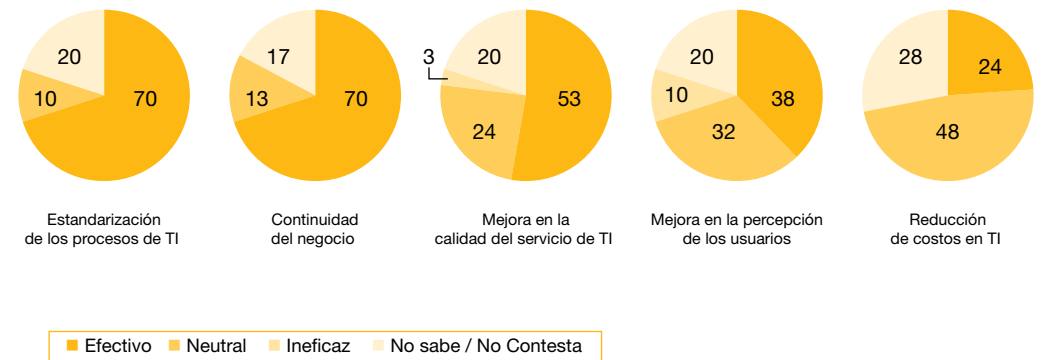


Figura N° 26: Beneficios de la adopción de estándares y mejores prácticas

P. ¿Cuán efectivo ha sido la adopción de estos estándares en la atención de los siguientes requerimientos?



³ITIL: Information Technology Infrastructure Library

Consideraciones finales

Consideraciones finales

Los resultados obtenidos este año con esta encuesta a las organizaciones venezolanas sobre la Seguridad de la Información, reflejan avances en la Gestión de la Seguridad, así como también, la consolidación de la FSAI como un participante importante dentro de las organizaciones, que agrega valor al negocio. Es importante mencionar que cada año se hace mayor la necesidad de la definición y normalización de un Plan Estratégico de Seguridad de la Información, con lo que sin duda alguna, se puede afirmar que existe un apoyo real a la consecución de las metas y objetivos del negocio.

Cada día las empresas se enfrentan a nuevos retos en donde salvaguardar la privacidad, confidencialidad y disponibilidad de la información se hace más arduo, y donde la preparación ante la ocurrencia de eventos es cada vez más exigente. Es por ello que existe la necesidad de incorporar una FSAI que defina y dirija eficientemente estrategias y controles que garanticen una gestión segura de los procesos de negocio.

Buscando respuestas

Para alcanzar los objetivos y metas que de acuerdo a su estrategia mantienen muchas de las Organizaciones, éstas realizan esfuerzos a través de la definición de una FSAI, organizar de forma adecuada sus recursos con base al entendimiento que hoy en día en lo que respecta a Seguridad de Información se tiene de acuerdo a las mejores prácticas, aplicación de estándares y experiencias en la aplicación de éstos a nivel global.

Es por esto que un enfoque apropiado implica el tratamiento de la seguridad desde un rol estratégico en los procesos de negocio, buscando el equilibrio adecuado entre la protección y la habilitación de acceso a los activos de información en línea con los objetivos estratégicos del Negocio.

La noción de Seguridad de Información como un habilitador de negocios es, en la actualidad, un concepto esencial para las organizaciones de cualquier sector de la economía nacional.

Espiñeira, Sheldon y Asociados

Caracas Oficina Principal

Avenida Principal de Chuao
Edificio del Río
Apartado Postal 1789
Caracas 1010-A
Teléfonos: 58 212 700-6666
Fax: 58 212 991-5210

Barquisimeto

Urbanización El Parque
Calle Los Comuneros
Centro Ejecutivo Los Leones
Piso 5, PH 5-2
Apartado Postal 3001
Teléfonos: 58 251 255-4983
58 251 255-0061
58 251 255-0404
Fax: 58 251 254-6284

Maracaibo

Avenida 9B entre Boulevard 5 de
Julio y Avenida Dr. Portillo
Edif. Banco Industrial, Piso 6
Apartado Postal 490
Teléfonos: 58 261 797-9805
58 261 797-9806
58 261 798-3869
Fax: 58 261 798-8194

Maracay

Avenida Las Delicias,
Urbanización El Bosque
Edificio Banvenez, Centro
Financiero, Piso 2
Apartado Postal 4700
Teléfonos: 58 243 232-2742
58 243 232-2745
Fax: 58 243 232-2742

Puerto La Cruz

Av. Intercomunal Andrés Bello
Sector Las Garzas
Centro Comercial MT (CCMT)
Piso1, local 39
Lecherías
Teléfonos: 58 281 267-0845
58 281 418-7935 al 38
Fax: 58 281 286-9616

Puerto Ordaz

Avenida Guayana
Sector Alta Vista
Torre Colón
Piso 6, oficinas 2, 3 y 4
Teléfonos: 58 286 962-6451
58 286 962-4995
58 286 962-5926
Fax: 58 286 962-6875

Valencia

Avenida Bolívar Norte
Centro Comercial y Profesional
El Camoruco
Piso 21
Apartado Postal 541
Teléfonos: 58 241 823-2321
58 241 824-1383
Fax: 58 241 824-4905

Espiñeira Sheldon y Asociados 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.

Aún 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.

Contactos

Si está conectado a internet, haga click sobre el nombre o el icono

Página web:
www.pwc.com/ve

Consultoría Gerencial
consultoria.gerencial@ve.pwc.com

Facebook
(<http://facebook.com/pwcVenezuela>)



Twitter
(http://twitter.com/pwc_venezuela)



LinkedIn
(www.linkedin.com/companies/pwc-venezuela)



Espiñeira Sheldon y Asociados 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.

Aún 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.

Al editar este informe únicamente en formato digital, contribuimos con:



6 árboles preservados para el futuro



798 kilos netos de gases de efecto invernadero (CO2) no emitidos



25.316 litros de agua salvados



2.344 kW no consumidos



300 kilos de desechos sólidos no generados

Los estimados de la conservación de recursos fueron realizados utilizando la Calculadora de Uso de Papel del Environmental Defense Fund. Para mayor información visite <http://www.papercalculator.org>.

www.pwc.com/ve

Espiñeira, Sheldon y Asociados es Firma miembro de PricewaterhouseCoopers (www.pwc.com) presta servicios profesionales de asesoría gerencial, auditoría y asesoramiento tributario, con foco en las diferentes industrias, destinado a clientes del sector público y privado. Más de 163.000 personas, en 151 países, conectan su conocimiento, experiencia y soluciones para acrecentar la confianza pública y generar mayor valor para sus clientes y quienes invierten en ellos.

© 2011 Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a Espiñeira, Sheldon y Asociados. A medida que el contexto lo exija "PricewaterhouseCoopers" puede referirse a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. Cada firma miembro es una entidad separada e independiente y Espiñeira, Sheldon y Asociados no será responsable por los actos u omisiones de cualquiera de sus firmas miembro ni podrá ejercer control sobre su juicio profesional ni tampoco podrá comprometerlas de manera alguna. Ninguna firma miembro será responsable por los actos u omisiones de cualquier otra firma miembro ni podrá ejercer control sobre el juicio profesional de otra firma miembro ni tampoco podrá comprometer de manera alguna a otra firma miembro o a PwCIL. R.I.F.: J-00029977-3