Asesoría Gerencial
Seguridad y Tecnología

Prácticas de Seguridad de Información de las empresas en Venezuela*

Encuesta Nacional 2007 - 2008

*connectedthinking

Espiñeira, Sheldon y Asociados
Firma miembro de
PricewaterhouseCoopers

Introducción

Cuando se habla sobre seguridad de la información, es común asociarla con actividades cotidianas propias de la interrelación de los usuarios con los sistemas y la Tecnología de Información (TI), tal como cambiar la contraseña o dar acceso a una aplicación en particular.

En este sentido, la inadecuada comprensión en una organización de las labores de la Función de Seguridad de Información (FSAI) dificulta la justificación de las inversiones, sobre todo cuando su evolución sugiere concentrar sus esfuerzos en actividades de planificación y diseño, delegando sus funciones operativas en los usuarios o los administradores de TI.

En contraposición, la alta gerencia de muchas organizaciones ha evolucionado y reconocido que la administración de seguridad de la información, así como la administración del riesgo tecnológico, es parte integral en su gestión, y que manejada adecuadamente agrega valor al negocio.

Esta interpretación positiva del riesgo hace posible que la organización transite exitosamente en la conciliación de la administración entre la seguridad de la información y el logro de las metas del negocio, promoviendo en la FSAI una evolución en su enfoque fundamentalmente operativo hacia una visión estratégica.

Es así que la planificación estratégica de la FSAI requiere conocer sobre las tendencias del mercado, además de conocer cómo la seguridad de la información se desarrolla en el país y/o región.

Es por esta razón que Espiñeira, Sheldon y Asociados, firma miembro de PricewaterhouseCoopers, líder en la prestación de servicios de Asesoría Gerencial en seguridad de la información, y especializada en el estudio y evaluación de los riesgos derivados de la utilización de la tecnología, tiene el gusto de presentarle los resultados de la Sexta Encuesta Nacional de Seguridad de Activos de Información.

En este estudio se encuentran las tendencias y estrategias de las organizaciones venezolanas en materia de seguridad, así como los principales incidentes, obstáculos y aplicación de las mejores prácticas y estándares internacionales de seguridad y TI.

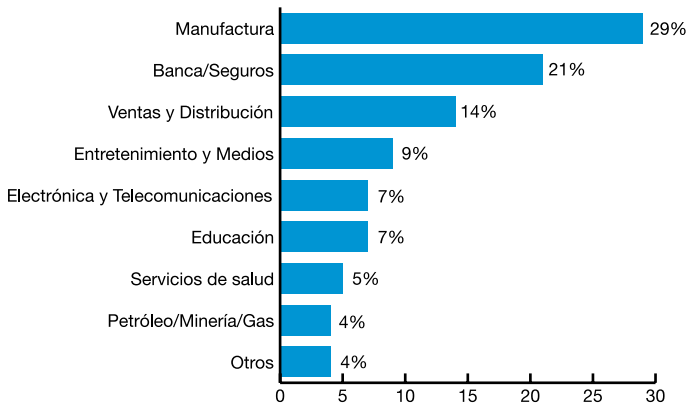
Ficha técnica

En esta edición de la encuesta denominada “Prácticas de Seguridad de Información de las Empresas en Venezuela”, participaron 378 empresas de diversos sectores de la actividad económica nacional, tanto del sector público como del privado.

Del total de entidades participantes, destacan los sectores Manufactura (29%) y Servicios Financieros (21%). Es importante mencionar que la muestra incluyó no sólo organizaciones de gran tamaño (más de 100 trabajadores), sino que al igual que en la encuesta anterior, se incorporaron representantes de la Pequeña y Mediana Empresa (Pymes).

Como todos los años, esta edición está orientada a obtener estadísticas locales, y conocer de los Oficiales de Seguridad, Vicepresidentes, Directores y Gerentes de TI, sus principales preocupaciones para la aplicación efectiva de la seguridad de activos de información en sus empresas, así como también las prácticas actuales, tendencias y el uso de mejores prácticas como parte de su gestión. La Figura N° 1 muestra la distribución porcentual de los diversos sectores que participaron.

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



Contenido:

Los temas sondeados en este estudio están categorizados en los siguientes tópicos:

I. Organización y planificación de la FSAI en las empresas

II. Estrategias de seguridad de información que están siendo aplicadas actualmente

III. Principales incidentes de seguridad de información y vulnerabilidades reportadas en los últimos doce (12) meses

IV. Controles de seguridad de información que han sido implantados a fin de mantener la confidencialidad, integridad y disponibilidad de la información

V. Uso de mejores prácticas y estándares internacionales para la gestión de la seguridad de información y TI

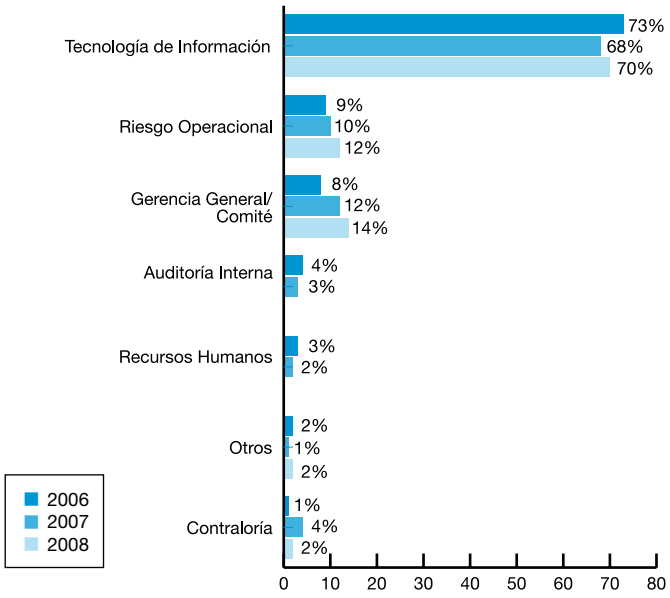
Sección I: Organización y planificación de Seguridad de la Información

Estructura organizativa y nivel de reporte

De acuerdo con la tendencia esperada, producto del comportamiento de años anteriores, se mantiene la existencia de una estructura organizacional encargada de dirigir y supervisar los procesos de la FSAI, y no se observan cambios significativos en cuanto al porcentaje de empresas con presencia de esta unidad, manteniéndose muy similar durante los últimos tres (3) años (alrededor de 60%).

En cuanto a la línea de autoridad o reporte, el 70% de las empresas participantes indicaron concentrar las actividades de la seguridad de la información en la unidad TI, mostrando un incremento de 2 puntos porcentuales con relación al año 2007, imputable a la adopción reciente de esta práctica en las empresas encuestadas. De igual forma, se observa un aumento de las empresas en donde la FSAI reporta directamente a un Comité o a la Gerencia General, o está adscrita a la Unidad de Gestión de Riesgo, así como la aparición de otras unidades de reporte, tal como se muestra en la Figura N° 2.

Figura N° 2. Nivel de reporte de la FSAI



Estructura organizativa y nivel de reporte (continuación)

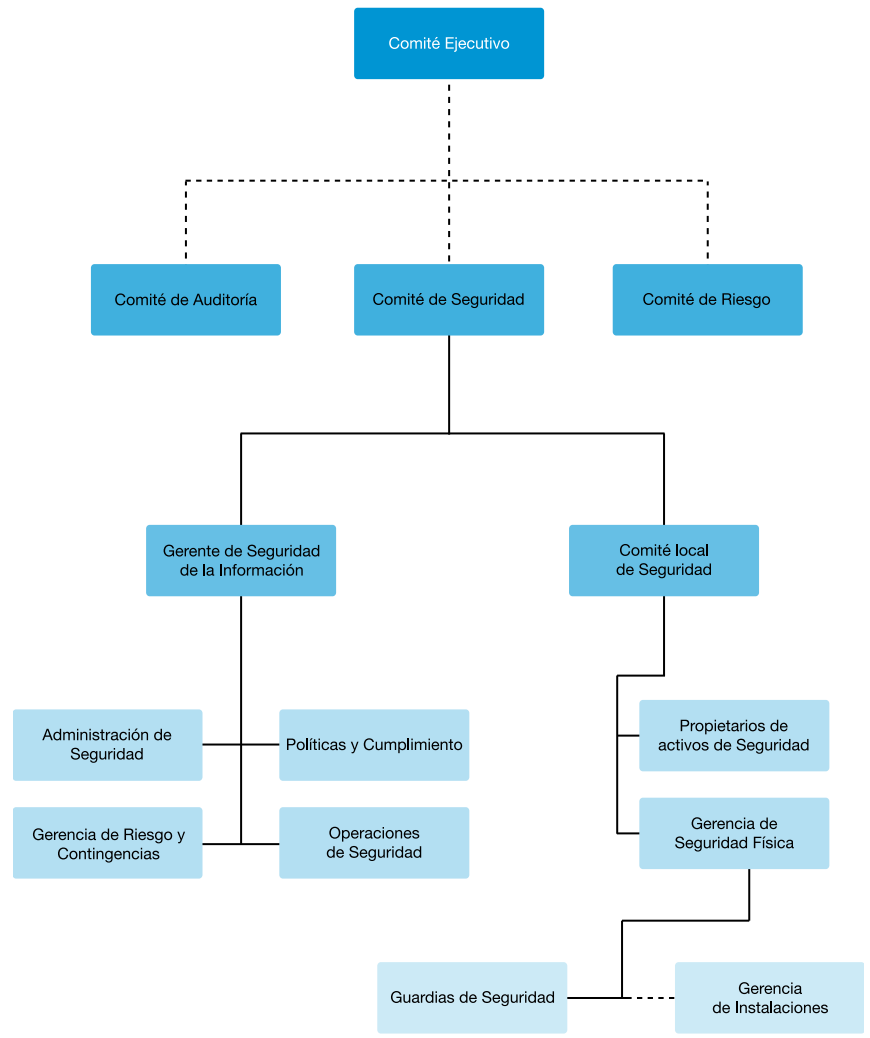
Es importante mencionar que existen mejores prácticas que establecen una estructura y niveles de reporte para la FSAI, tal como se muestra en la Figura N° 3.

Incluso para este análisis se deben considerar las regulaciones locales, como es el caso de la "Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras", que para el sector bancario, en su Artículo N° 39 establece que: "En la estructura organizacional del Ente supervisado, debe existir un área de seguridad de la información independiente de las unidades de Tecnología de la Información, Auditoría de Sistemas y Riesgo…".

Según la SUDEBAN, "En la estructura organizacional del Ente supervisado, debe existir un área de seguridad de la información independiente de las unidades de Tecnología de la Información, Auditoría de Sistemas y Riesgo…".

Artículo N° 39, Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras".

Figura N° 3. Estructura organizativa y nivel de reporte de la FSAI basada en mejores prácticas

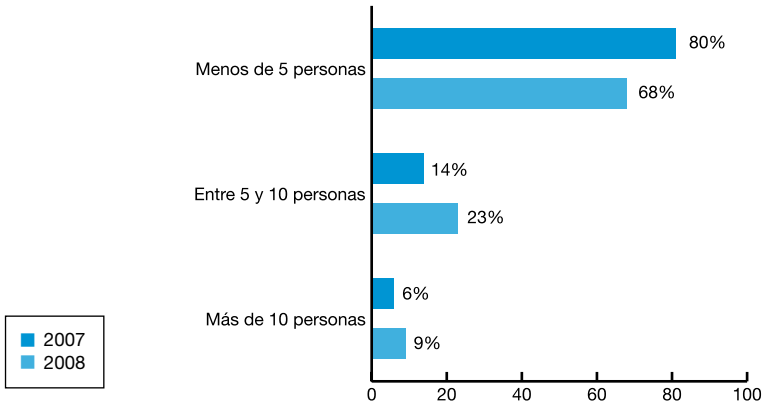


Fuente: www.iso27001security.com. Estructura genérica, basada en lo establecido en ISO 27000-series, familia de estándares para la gestión de seguridad de información.

Estructura organizativa y nivel de reporte (continuación)

Por otro lado, en aquellas organizaciones en las cuales la FSAI está formalmente constituida y tiene independencia en sus actividades, este estudio indica que existe un alto porcentaje en donde la estructura organizativa está conformada por menos de cinco (5) personas (68%). En la Figura N° 4 se evidencia un aumento de 9 puntos porcentuales en el rango de "Entre 5 y 10 personas", mientras que la categoría "Menos de 5 personas" disminuyó en 12 puntos porcentuales con respecto al año anterior.

Figura N° 4. ¿Por cuántas personas está conformada la FSAI en su empresa?



Inversión en Seguridad de Información

Con relación a la inversión en seguridad de la información, en la Figura N° 5 se muestra el comportamiento de los últimos tres (3) años. En particular se observa que el 58% de las empresas encuestadas, estima que habrá un incremento para el próximo año, lo cual ha sido la tendencia de las últimas tres (3) ediciones de nuestra encuesta.

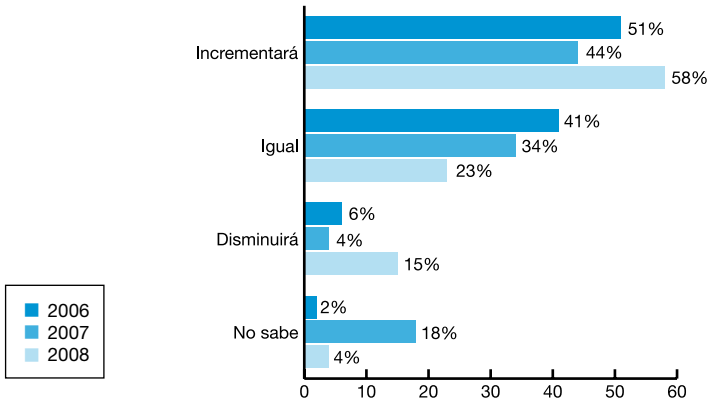
Esto es consistente con la formalización de la estructura y la necesidad de contar con presupuestos para lograr inversiones en materia de seguridad de la información que permitan solventar inconvenientes operativos, así como también optimizar el nivel de seguridad existente.

Sin embargo, resulta interesante la opinión del 15% de los encuestados, que considera ocurrirá una disminución del presupuesto con respecto al año anterior. Esto puede estar relacionado con la realidad en el marco regulatorio al cual se han visto sometidas las empresas venezolanas, quienes debieron direccionar sus presupuestos planificados, a la adquisición o adecuación de sus sistemas de información y procesos internos, para cumplir con normativas locales. Recordemos el caso de la Reconversión Monetaria en el año 2007, lo cual significó que la gran mayoría de los proyectos fueron diferidos, y en consecuencia, las inversiones en seguridad de la información se vieron disminuidas.

Otro aspecto que se observa en la Figura N° 5, es que en los últimos tres (3) años cada vez es menor el porcentaje de empresas que deciden mantener igual su presupuesto.

Inversión en Seguridad de Información (continuación)

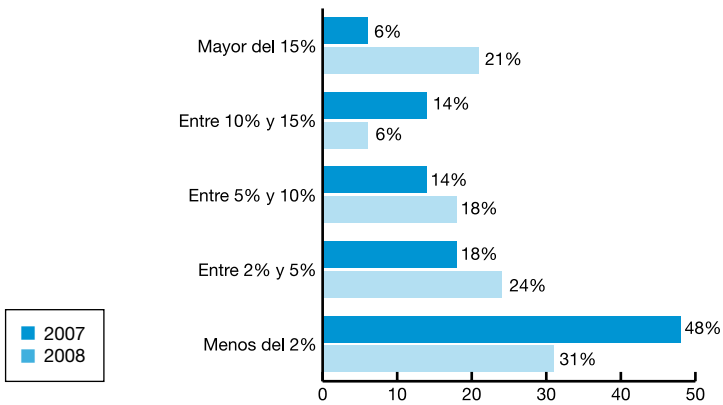
Figura N° 5. ¿Cómo será la inversión en seguridad de información en el año 2008 en comparación con el año 2007?



Si comparamos la proporción del presupuesto de seguridad de información con el de TI, y haciendo un comparativo con el año 2007, observamos que éste se ubica entre 2% y 5% para el 24% de las empresas encuestadas; sin embargo, resulta interesante analizar que actualmente existe un 21% de organizaciones cuyo presupuesto para seguridad de la información es mayor al 15% con respecto al presupuesto de TI, lo cual representa un incremento importante en el número de empresas con presupuestos de estas dimensiones en el año 2008 (ver Figura N° 6).

El 58% de las empresas estiman que el presupuesto en seguridad de información se incrementará. Otro 23% estima que permanecerá igual

Figura N° 6. ¿Cuál es la proporción porcentual del presupuesto de seguridad de información con relación al presupuesto de TI?

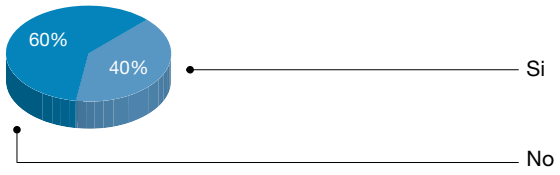


Cómo se planifica la seguridad de la información y sus principales obstáculos

El entorno cambiante de los negocios, la influencia de las nuevas tecnologías y la aparición de riesgos derivados de su uso, representa un reto importante que ocasiona que las actividades de desarrollar una estrategia empresarial y un plan estratégico, adquieran mayor relevancia.

En este sentido, la seguridad de la información no escapa a esta realidad, y con relación a la existencia de un plan que direccione la estrategia de la FSAI, un 40% de las empresas encuestadas manifestaron haber formalizado este plan, quedando un 60% que no ha emprendido las acciones necesarias para su desarrollo, tal como se muestra en la Figura N° 7.

Figura N° 7. Distribución porcentual de la existencia de plan estratégico de seguridad de información



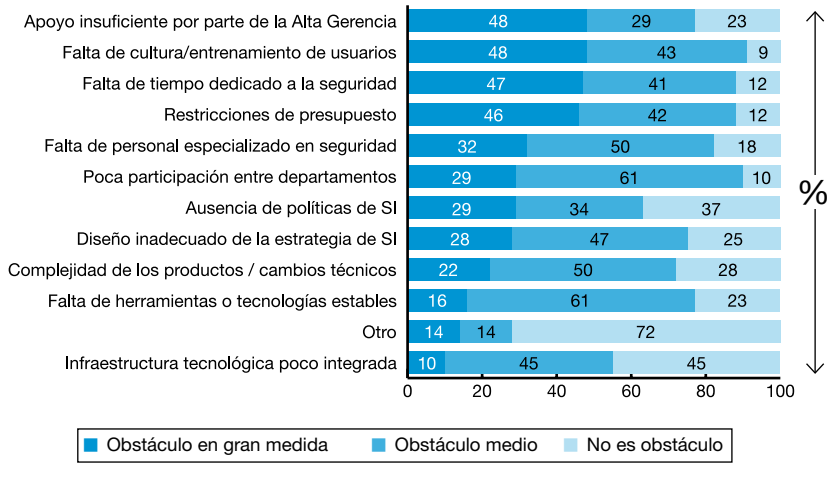
La ausencia de un Plan Estratégico, dificulta la determinación de las actividades de seguridad de la información que permitan identificar, crear, capturar y agregar valor a los procesos de negocio

Es importante mencionar que la ausencia de un plan estratégico de seguridad de información puede alejar a la FSAI del cumplimiento de los requerimientos y objetivos a ser alcanzados por la organización. Otro aspecto importante, es que la inexistencia de un plan estratégico, dificulta la determinación de las actividades de seguridad de la información que permitan identificar, crear, capturar y agregar valor a los procesos de negocio.

Si relacionamos lo anterior con el análisis de los principales obstáculos que presentan las empresas venezolanas para la práctica de seguridad de activos de información, los resultados obtenidos evidencian una clara incidencia del factor humano (ver Figura N° 8) y específicamente para este año 2008 la “Falta de Cultura y Entrenamiento de Usuarios” y el “Apoyo insuficiente por parte de la alta gerencia”, calificaron como los principales obstáculos.

Paradójicamente, al preguntarle a los encuestados si contaban con un programa de capacitación para usuarios finales, en temas de riesgo, TI y seguridad de información, sólo el 32% afirmó que había establecido esta actividad como mecanismo para fomentar la cultura de riesgo en la organización.

Figura N° 8. Principales obstáculos para la práctica de seguridad de información



Cómo se planifica la seguridad de la información y sus principales obstáculos (continuación)

Para el resto de los aspectos evaluados, se observó una distribución uniforme, evidenciándose por ejemplo, que los aspectos técnicos (tales como "Infraestructura tecnológica poco integrada" y "Ausencia de políticas de SI"), en gran medida no representan un obstáculo para la práctica de seguridad de la información. Para los próximos años se pudiera afirmar entonces, que la FSAI continuará mejorando en términos generales, si se enfoca en reforzar sus estrategias de divulgación de mejores prácticas y cultura de seguridad de información, así como la comunicación y búsqueda de consenso sobre sus iniciativas con la alta gerencia.

Finalmente en relación con los niveles de posicionamiento de la FSAI, existe una percepción entre las empresas encuestadas, que esta unidad se encuentra mejor valorada que en los últimos dos (2) años al agruparse en un 60% las respuestas de "Mucho mejor que antes" y "Mejor que antes".

Para las empresas encuestadas, la seguridad de la información está "Mucho mejor que antes" o "Mejor que antes" con respecto a los últimos dos (2) años

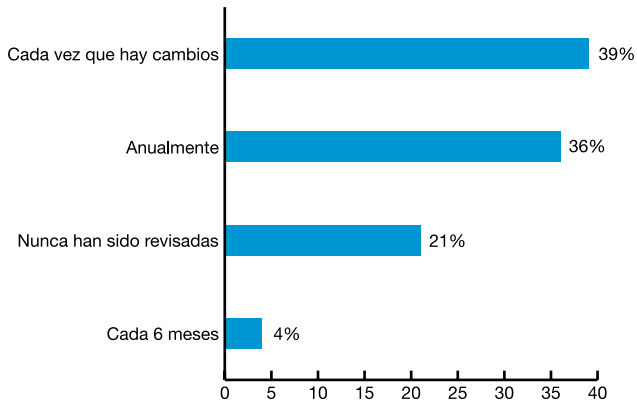
Sección II: Estrategias de Seguridad de la Información

Políticas y procedimientos: orientaciones que contribuyen a la gestión de la seguridad de la información

Una de las preguntas permanentes en nuestra encuesta, está relacionada con la existencia de políticas y procedimientos de seguridad de información y en el interés de conocer la adopción de esta práctica, debido a que son orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección.

Bajo este contexto, se observa una mayor conciencia en el mercado venezolano sobre los beneficios de la documentación, debido a que 80% de las empresas encuestadas manifestaron que contaban con políticas y procedimientos de seguridad de información formalmente documentados; y aun cuando representa un desafío importante el mantener esta documentación actualizada, al sondear la frecuencia de actualización, el 39% afirmó que cada vez que existen cambios en la organización, estos son incorporados a la documentación existente, tal como se muestra en la Figura N° 9. Otro 40% de las empresas manifestaron que se revisan una vez al año o cada seis (6) meses (con 36% y 4% respectivamente).

Figura N° 9. Frecuencia de actualización de las políticas y procedimientos de seguridad de información



Soluciones estratégicas en su Organización

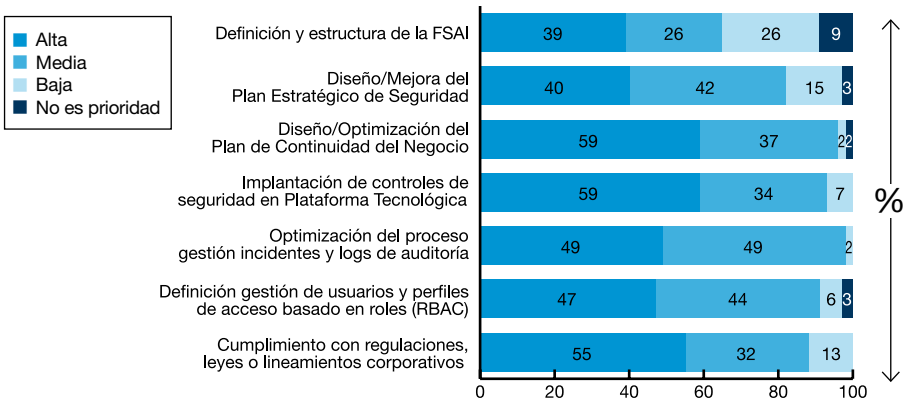
La adopción de soluciones estratégicas en una organización, muchas veces implica la aplicación de controles, los cuales pueden ser muy robustos, otros débiles, a tal punto que al hacer una evaluación, pudieran llegar a comprometer la operatividad en mayor o menor medida.

En este sentido, lo que diferencia el nivel de control de una compañía a otra, es el tipo de estrategias que se utilizan para determinar dónde enfocar sus esfuerzos en el reforzamiento de su ambiente de control, y que se adapten a la realidad de cada organización.

Soluciones estratégicas en su Organización (continuación)

Este estudio incluye estadísticas relacionadas con las soluciones estratégicas que en materia de seguridad de información están siendo aplicadas por las empresas venezolanas, entre las cuales destacan con una importancia “alta”, la implantación de controles de seguridad en la plataforma tecnológica, el diseño u optimización del plan de continuidad del negocio y el cumplimiento de regulaciones, leyes o lineamientos corporativos, tal como se muestra en la Figura N° 10. Por el contrario, la definición u optimización de la FSAI, resultó tener un menor porcentaje en cuanto a importancia (39%).

Figura N° 10. Importancia de las soluciones estratégicas de seguridad de información

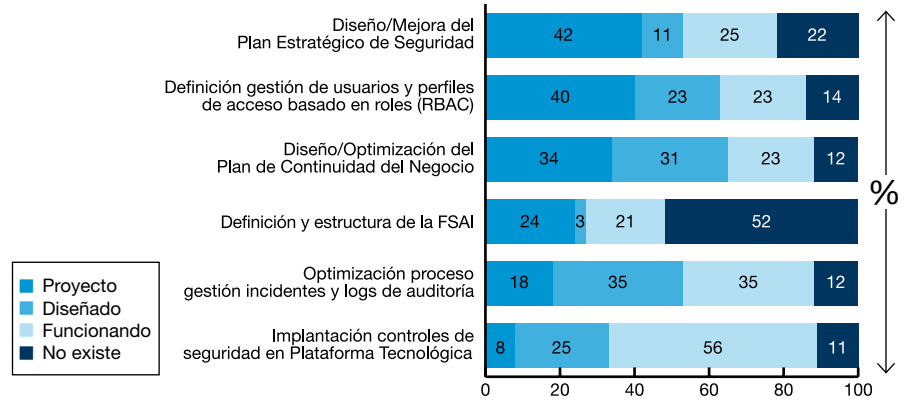


Para obtener un análisis completo de las cifras anteriores, hemos revisado además el estatus en el cual se encuentran estas soluciones estratégicas en las empresas, a fin de medir y obtener estadísticas locales, acerca de hacia dónde se direccionan los esfuerzos y recursos en materia de seguridad de información.

En la Figura N° 11 podemos observar que los proyectos con mayor presencia en las empresas encuestadas son: “Diseño o mejora del Plan Estratégico de Seguridad” con un 42%; “Definición o mejora de las gestión de usuarios y perfiles de acceso basado en roles” con 40%; y “Diseño/optimización del Plan de Continuidad del Negocio” con un 34%.

Por el contrario, la solución que mayormente se encuentra en funcionamiento, está representada por la “Implantación de controles en la plataforma tecnológica” con un 56%, lo cual sugiere que las empresas en Venezuela, han adoptado la práctica del reforzamiento de los controles de seguridad, como medida de protección para la información de sus clientes, empleados y relacionados.

Figura N° 11. Estatus de las soluciones estratégicas de seguridad de información

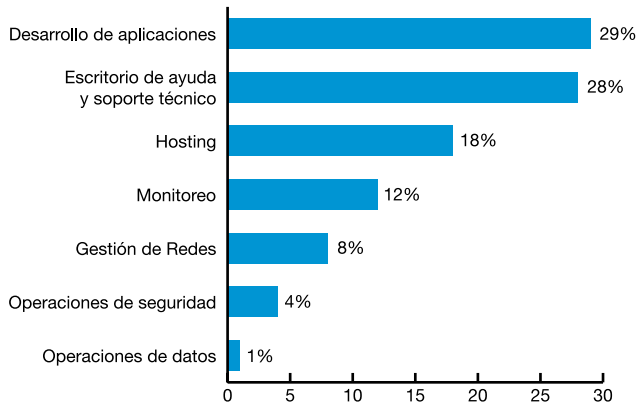


Estrategia: ¿Tercerizar o no tercerizar?

Gran parte del esfuerzo de los ejecutivos de hoy en día, está dirigido al logro de una gestión efectiva que agregue valor al negocio y maximice los beneficios, lo que implica en ocasiones, la reducción de costos. En este sentido, el outsourcing constituye una estrategia de negocios que aporta a las organizaciones las ventajas competitivas para una mayor efectividad, productividad y rentabilidad. Adicionalmente, representa un beneficio integral que permite delegar en socios externos especializados parte de las funciones del negocio, que si bien son necesarias, no necesariamente son parte del núcleo fundamental de valor.

Bajo este contexto, se le preguntó a las empresas participantes si utiliza los servicios de terceros (outsourcing) en procesos o actividades de tecnología y/o seguridad. A esta pregunta, un 27% de las empresas encuestadas manifestaron tener al menos un servicio de gestión de tecnología o seguridad de la información manejado por un externo. Al preguntar sobre los servicios que son tercerizados, de acuerdo con los resultados obtenidos, los más utilizados están relacionados con: el Desarrollo de aplicaciones con un 29%, así como el Escritorio de Ayuda (Help Desk) y Soporte con un 28%, tal como se muestra en la Figura N° 12.

Figura N° 12. Servicios que usualmente son dados en outsourcing



Ahora bien, el outsourcing no sólo transfiere un proceso a un tercero: también se transfieren los riesgos que se derivan de su ejecución sin que esto represente que su impacto se limite únicamente al contratista. Considerando que el impacto en reputación y patrimonio puede afectar inevitablemente al contratante, organismos reguladores han establecido normas orientadas a reforzar la responsabilidad de las empresas en las actividades delegadas a terceros. Tal es el caso de la normativa emitida por la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN)[1], la cual obliga a sus entes regulados a trasladar el cumplimiento de la misma hacia sus proveedores.

Entre los principales riesgos que perciben las empresas participantes en la encuesta al tercerizar, se obtuvo que el incumplimiento de los términos y condiciones establecidos en los acuerdos de servicio o contratos, destaca con un 21%, así como también la posibilidad de la pérdida de control del proceso cedido en outsourcing y el incumplimiento con regulaciones o políticas internas, con un 14% cada una.

[1] Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras

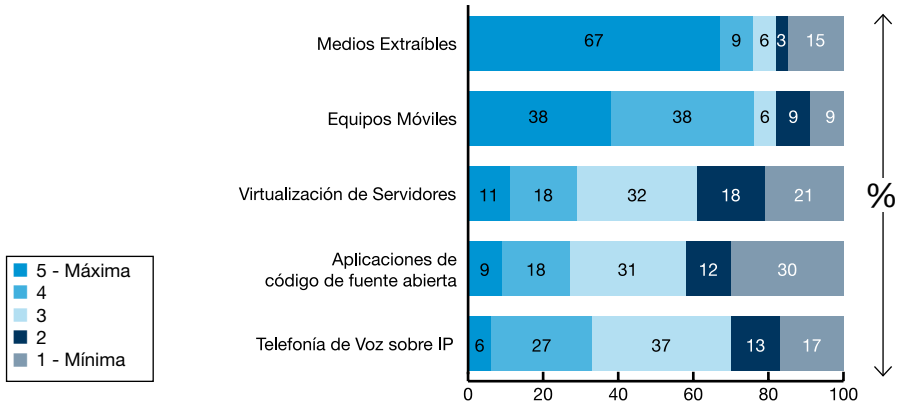
Sección III: Brechas e incidentes de seguridad de información

Tecnologías bajo la atención de la FSAI

Nuestro estudio ha recopilado cuáles son las principales preocupaciones que en materia de seguridad de información tienen las empresas encuestadas. A este respecto, se les preguntó en orden de prioridad (en una escala del 1 al 5, donde el 5 representa la máxima atención y el 1 la mínima), cuáles de las tecnologías utilizadas en su organización han sido identificadas como una preocupación en materia de seguridad de información.

En la Figura N° 13 se observa que aun cuando los medios extraíbles y los equipos móviles aportan una gran cantidad de ventajas en la operativa diaria, un 67% y un 38% de los encuestados, respectivamente, afirmaron que estas tecnologías son las que representan un nicho importante de riesgo, debido a que las medidas de protección trascienden la frontera del control lógico, y por el contrario, se hace necesario centrar la atención en los controles físicos que puedan ser aplicados. Mención interesante de esta encuesta es la baja percepción de riesgo sobre el uso de telefonía IP y aplicaciones de código abierto, tecnologías que pese a su reciente ingreso al mercado, no parecen ser centro de interés en temas de seguridad de información.

Figura N° 13. Tecnologías que se han identificado como una preocupación en seguridad de información



Incidentes de seguridad de información: impacto, causas y consecuencias

Pese a que los incidentes de seguridad de información han evolucionado en forma y en impacto hacia los negocios, por 6° año consecutivo, las empresas encuestadas manifiestan que la “infección por virus” y el “acceso no autorizado”, representan de manera importante, los principales eventos de seguridad en las organizaciones, con un 28% y 26% respectivamente. Sin embargo, en este último año, surgen nuevas categorías tales como:

- La implantación de código malicioso, con un 12%
- La negación de servicios, con un 10%; y
- La deducción de contraseñas, con un 8%

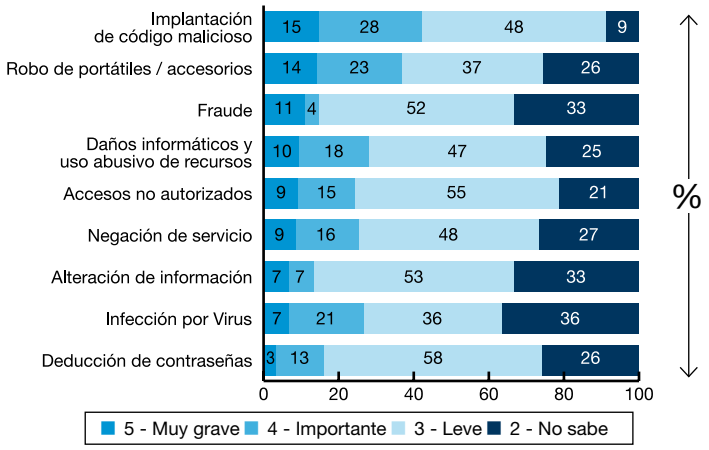
El otro 16% está principalmente distribuido en eventos tales como: fraude, alteración de la información, robo de portátiles y uso abusivo de recursos.

Al indagar acerca del nivel de afectación de la organización por la ocurrencia de estos eventos, en la Figura N° 14 se observa que el incidente con mayores consecuencias lo representa la implantación de código malicioso, el cual reporta un 43%, entre las categorías “muy grave” e “importante”.

Incidentes de seguridad de información: impacto, causas y consecuencias (continuación)

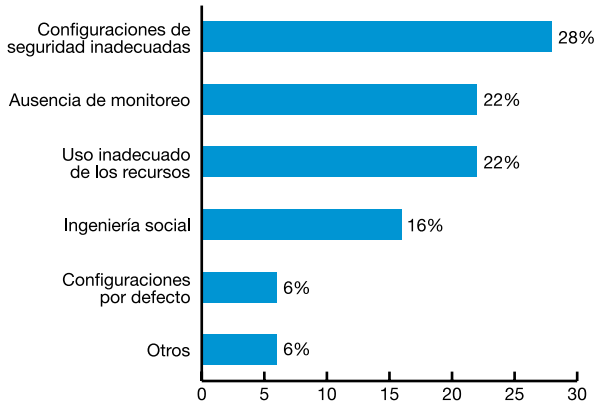
Los rubros que obtuvieron mayor porcentaje en la categoría “leve” lo representan: “la deducción de contraseñas” con un 58%, así como “los accesos indebidos” con un 55%, lo cual hace suponer que son eventos que, si bien es cierto que representan un riesgo importante, cada día se han aplicado mayores controles que han redundado en acotar el efecto de su ocurrencia.

Figura N° 14. Nivel de severidad con relación a incidentes de seguridad de información en el último año



Otra conclusión que se obtiene, está relacionada con el alto porcentaje de los encuestados que afirma no saber del nivel de severidad o estragos causados por un incidente de seguridad ocurrido en su organización, lo cual sugiere que el monitoreo y análisis de estos eventos siguen siendo actividades muy débiles como parte de la operativa diaria de la FSAI. En este sentido, las principales causas de los incidentes ocurridos están representadas por configuraciones de seguridad inadecuadas (28%) y la ausencia de monitoreo (22%), tal como se observa en la Figura N° 15.

Figura N° 15. Principales causas de la ocurrencia de los incidentes de seguridad de información

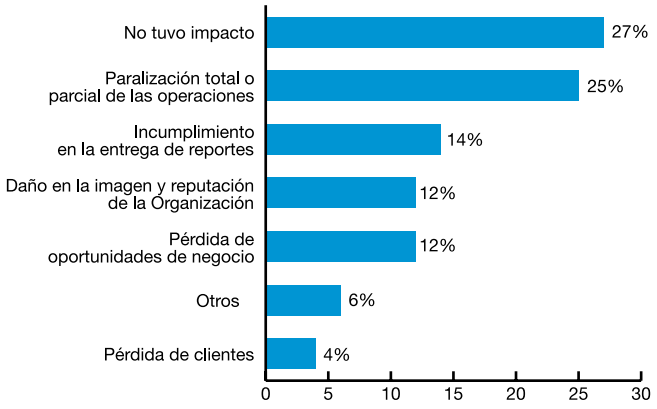


Incidentes de seguridad de información: impacto, causas y consecuencias (continuación)

Las consecuencias de los incidentes de seguridad de información pueden ser diversas: desde la pérdida de operatividad de la plataforma tecnológica, hasta la afectación de la imagen y reputación de la organización, pasando por pérdidas de clientes, de oportunidades de negocio, entre otras.

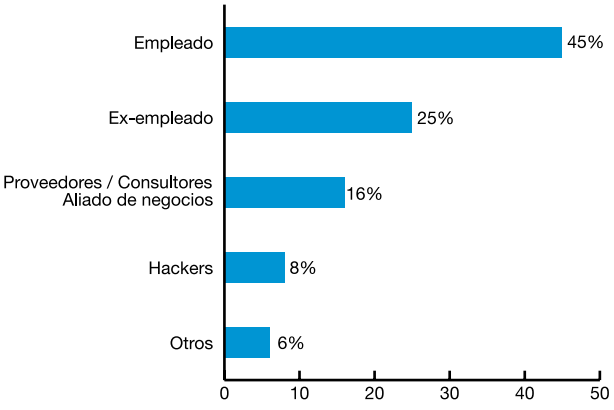
Bajo este contexto, a la pregunta de ¿cuáles fueron las consecuencias de los incidentes de seguridad ocurridos?, el 27% de los encuestados coincidieron en señalar que la ocurrencia del incidente de seguridad, “no tuvo impacto” en la organización. Sin embargo, la mayor ponderación de las consecuencias identificadas, está representada en la paralización total o parcial de las operaciones con un 25%, lo cual a su vez, puede incidir de manera indirecta, en cualquiera de las otras respuestas. Para conocer la distribución de los resultados obtenidos a este respecto, ver la Figura N° 16.

Figura N° 16. Principales consecuencias de la ocurrencia de los incidentes de seguridad de información



En cuanto al origen de los incidentes de seguridad reportados, las empresas han advertido que la principal fuente está dentro de la organización, lo cual se ratifica en la Figura N° 17. Sobre este resultado, existe una notable ocurrencia de eventos relacionados con empleados, situación que coincide con consultas similares realizadas a nivel internacional, y que refuerza la premisa que las personas que conocen la organización son potencialmente más riesgosas.

Figura N° 17. Origen de los incidentes de seguridad de información reportados



Luego de la identificación, ¿cuál es el siguiente paso?

¿Cuál es la capacidad de respuesta de su organización frente a un incidente de seguridad de información? ¿Cuan rápido puede estabilizar la situación?. La respuesta a estas preguntas es la clave para que una compañía pueda minimizar el impacto en caso que ocurra un incidente de seguridad. PricewaterhouseCoopers establece dentro de su Modelo Integral de Seguridad de la Información, la respuesta a incidentes como un “conjunto de medidas proactivas y reactivas que debe tomar una organización para asegurarse que los incidentes son detectados y solucionados a tiempo, evitando mayores daños y evitando que dicho evento se repita en el futuro”.

Al indagar acerca de las acciones tomadas, luego de haber sido identificada la ocurrencia de un incidente de seguridad, observamos que éstas pueden ser categorizadas como soluciones tácticas que abordan de manera puntual el evento. En la Figura N° 18 se observa la distribución de las respuestas, en donde destaca que principalmente lo que se hace es la identificación del responsable (con un 25%), lo cual no necesariamente evita que el incidente pueda ocurrir nuevamente.

Figura N° 18. Principales acciones tomadas al identificar un incidente de seguridad de la información

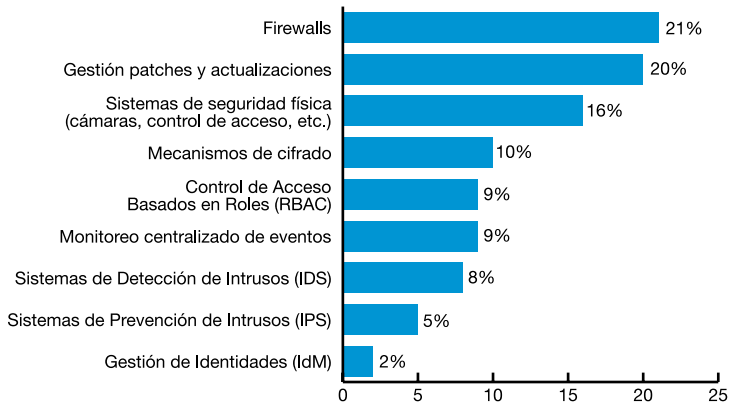
Sección IV:
Controles de seguridad de la información

Controles que han sido implantados en las empresas venezolanas para mitigar riesgos

Al preguntar sobre cuáles controles han sido aplicados para la mitigación de riesgos, destacan con un 21% la implantación de firewalls y la aplicación de patches y actualizaciones con un 20%, lo cual se corresponde con la realidad que experimentan las unidades de seguridad de información y tecnología, debido a los constantes ataques y nuevas amenazas que surgen día tras día.

En la Figura N° 19, se observa la distribución de los controles utilizados, siendo el menos aplicado la gestión de identidades (IdM), con tan sólo un 2%. Si bien las cifras difieren con relación a los resultados en años anteriores, la ubicación de las dos primeras opciones se ha mantenido en el tiempo.

Figura N° 19. Controles que han sido aplicados/implantados en su organización para mitigar riesgos



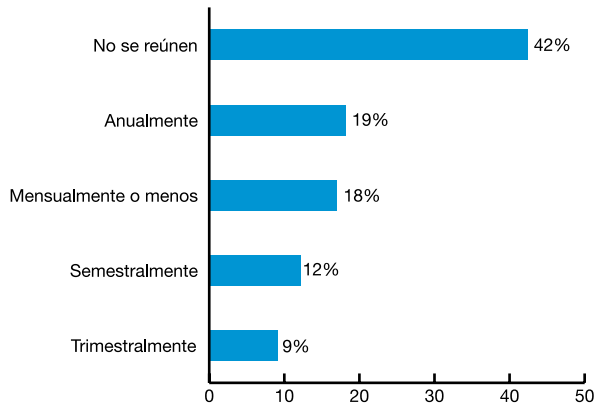
Otra de las preguntas estuvo orientada a indagar las soluciones para la continuidad operativa, en la cual el 72% de las empresas encuestadas señalaron que sólo cuentan con redundancia de equipos y telecomunicaciones, logrando así una alta disponibilidad, y sólo un 22% respondieron tener planes de continuidad operativa formalmente diseñados. Entre los planes indicados se encuentran: Planes de Continuidad de Negocio (BCP), Planes de Recuperación de Desastre (DRP) y Planes de Recuperación del Negocio (BRP).

Sobre este tema, el sector financiero y algunas de sus empresas relacionadas están obligadas por la SUDEBAN al desarrollo de planes de contingencia tecnológicos. Si bien el impacto de esta resolución no se percibió al momento del desarrollo de esta encuesta, el empresariado venezolano se verá afectado en el corto plazo, pudiéndose proyectar en el futuro, un incremento sensible en el número de empresas que adopten esta práctica.

Controles que han sido implantados en las empresas venezolanas para mitigar riesgos (continuación)

Finalmente, es fundamental el involucramiento de la alta gerencia en los temas de seguridad de la información y riesgos, y en este sentido, al preguntar ¿con qué frecuencia, la alta gerencia, Comité de Seguridad, Riesgo o Tecnología se reúnen para discutir las necesidades de la seguridad de la información vs. objetivos del negocio?, un 42% de las empresas encuestadas indicó que no se reúnen, lo cual evidencia un sector importante donde la seguridad de la información no forma parte de los temas de interés en las organizaciones para apoyar al cumplimiento de los objetivos del negocio. En la Figura N° 20 se muestra la distribución de respuestas para esta pregunta.

Figura N° 20. Frecuencia de reunión para revisar necesidades de seguridad de información vs. objetivos del negocio



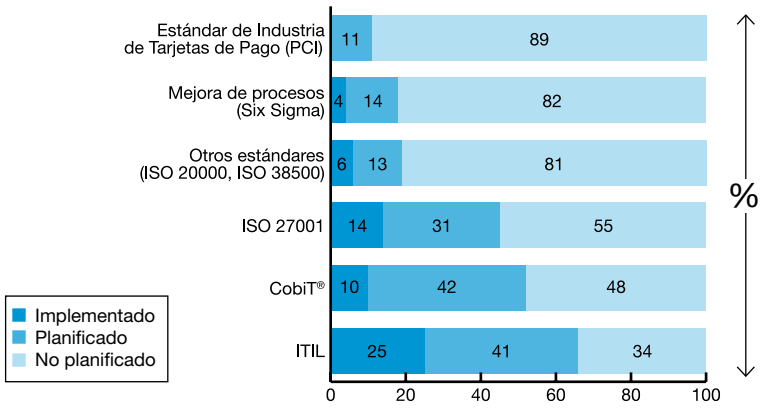
Sección V: Mejores prácticas en seguridad de información y TI

El uso de estándares internacionales como elemento diferenciador

Uno de los instrumentos más efectivos para que las organizaciones incrementen la probabilidad del éxito en su gestión, es aplicar conceptos asociados a “Mejores Prácticas”, para lo cual un 91% de las empresas encuestadas coincidieron en señalar que conocen de la existencia de referencias internacionales tales como: ITIL, ISO 20000, ISO 27001, CobIT®, entre otros.

Al indagar sobre el estatus de la adopción e implantación de estos estándares como parte de la gestión, se observa en el mercado venezolano un largo camino por recorrer: sólo para los temas de gestión y calidad del servicio de tecnología de información, se vio una diferencia al obtener que un 25% de las empresas han implantado ITIL, e incluso un 41% está planificando implantarlo. En la Figura N° 21 se observa la distribución del estatus de implantación de los estándares estudiados.

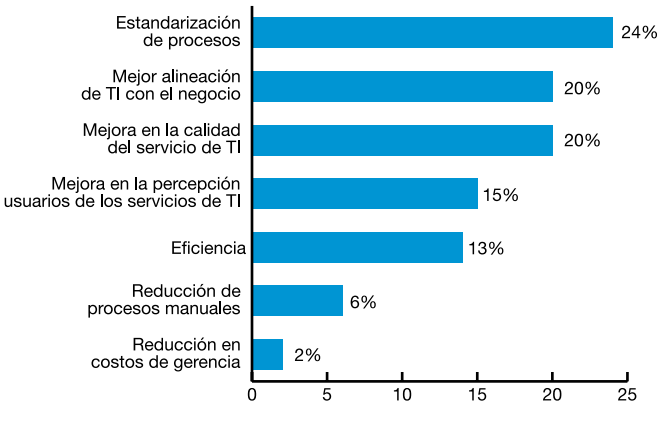
Figura N° 21. Estatus de implantación de los estándares de seguridad y tecnología



Un 91% de los participantes manifestó conocer las mejores prácticas y estándares internacionales de seguridad y tecnología de la información

Ahora bien, considerando el número de empresas que han implementado ITIL, un 24% señaló que uno de los mayores beneficios está representado por la estandarización de los procesos de TI, seguido por la mejora en la calidad y la alineación de TI con los objetivos del negocio, con un 20% cada uno, tal como se muestra en la Figura N° 22. Esto sugiere que existen esfuerzos comprobados en cuanto a la implementación de mejores prácticas, al observar las ventajas reportadas por las organizaciones que las han adoptado.

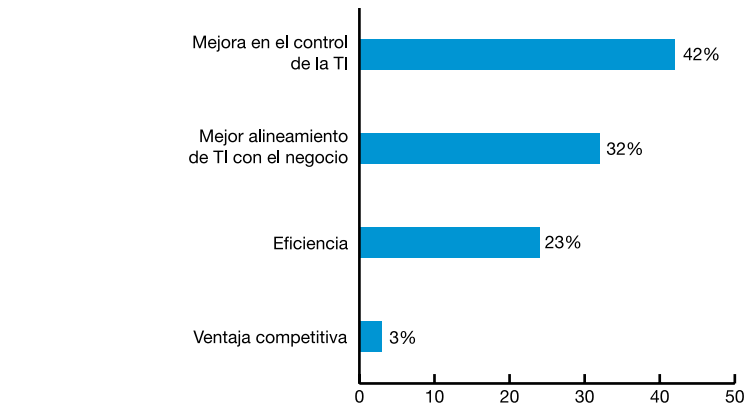
Figura N° 22. Principales beneficios obtenidos con la implantación de ITIL



El uso de estándares internacionales como elemento diferenciador (continuación)

De las empresas que respondieron haber implantado CobIT®, un 42% señaló que uno de los grandes aportes para su organización ha sido mejorar el control sobre la tecnología de información, además de lograr una mejor alineación con el negocio (32%). Para mayor detalle, ver la Figura N° 23.

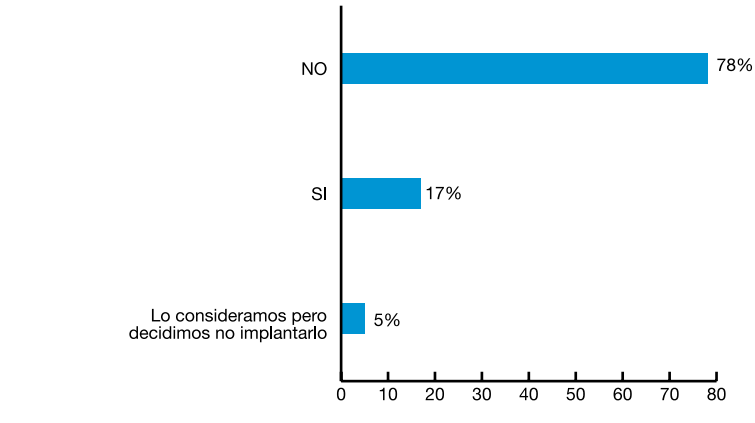
Figura N° 23. Principales beneficios con la implantación de COBIT



Estas últimas gráficas denotan una mayor conciencia en cuanto a la utilización de estándares de tecnología de información, y que además existen organizaciones que se están diferenciando por las ventajas que se obtienen.

En contraste, nuestro estudio también incluyó la apreciación sobre la adopción del estándar ISO 27001[2]. A este respecto, un 78% de las empresas encuestadas, señalaron no tener implantado formalmente el estándar vs. un 17%, tal como se muestra en la Figura N° 24.

Figura N° 24. Proporción de empresas que han adoptado el estándar ISO 27001

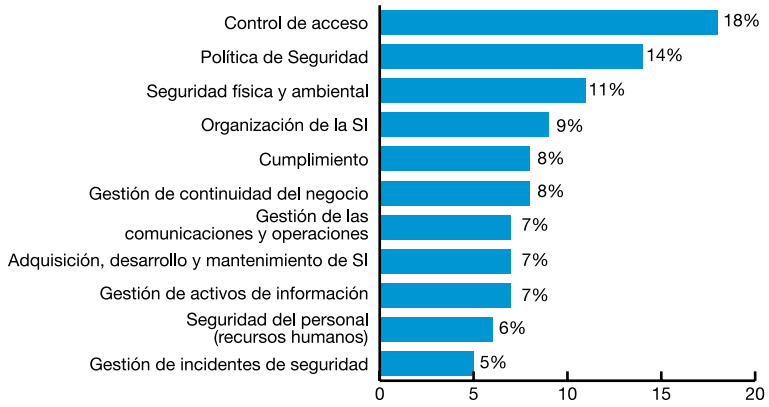


[2] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements

El uso de estándares internacionales como elemento diferenciador (continuación)

Es importante resaltar que este estándar es aplicable en toda organización independientemente de su tamaño, sector, y tecnología utilizados. Gracias a su estructura basada en controles agrupados en once (11) dominios según lo establece el Código de Práctica ISO 27002, se les preguntó a las empresas participantes cuál de estos dominios estaba mayormente definido y estructurado en sus organizaciones. Las respuestas están presentadas en la Figura N° 25. En estos resultados llama la atención que el dominio que obtuvo menor porcentaje fue la gestión de incidentes de seguridad de información, pese a que se reconoce la existencia de estos eventos, así como su impacto, causas y consecuencias.

Figura N° 25. Dominios de la norma de seguridad de la información que han sido implantados



Notas finales

Sobre la correlación de los resultados obtenidos en este estudio, es claro que la seguridad de información hoy en día tiene lugar determinante dentro de la gestión de la tecnología, y se ha convertido en un elemento fundamental a ser considerado en toda estrategia de negocio con miras a lograr metas importantes a corto, mediano y largo plazo. Asimismo, la FSAI está experimentando la necesidad de definir estrategias efectivas que garanticen una gestión segura de los procesos del negocio a fin de darle mayor resguardo a la información, y al mismo tiempo gestionar los obstáculos para adaptarse a los continuos cambios como consecuencia de las exigencias del mercado.

Buscando nuevas respuestas

Para alcanzar la excelencia que muchas de las organizaciones están buscando en materia de seguridad de información, algunos ejecutivos de negocio, Gerentes de Seguridad, de Tecnología y de Sistemas están haciendo un esfuerzo para organizar de forma adecuada sus recursos con base al entendimiento que se tiene hoy día en lo que respecta a seguridad de información. Es por esto que un enfoque apropiado implica el tratamiento de la seguridad desde su 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. 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.

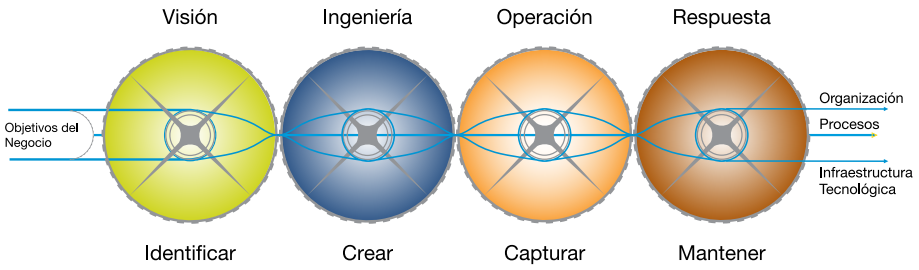
El enfoque de seguridad de PricewaterhouseCoopers (PwC)

Tomando en cuenta las realidades expuestas y los resultados obtenidos desde que iniciamos la realización de este estudio, hace seis (6) años, Espiñeira, Sheldon y Asociados, firma miembro de PricewaterhouseCoopers, impulsa la siguiente definición de seguridad:

La Seguridad de Activos de Información es un proceso estratégico de negocio que incluye a la organización, los procesos y la tecnología que habilita el acceso a, y brinda protección a los activos de información de la empresa.

Ya sea que una organización esté en busca de una plataforma integral de seguridad, mayores ingresos, ventajas competitivas en el sector del mercado o todos los aspectos antes mencionados, el alcanzar estas metas requiere de la definición de un marco integral que permita la gestión de la práctica de seguridad de información a lo largo y ancho de la empresa, por lo cual PwC ha desarrollado una representación de las actividades de seguridad, como una cadena de valor para las organizaciones, conocida como el “Enterprise Security Business Model” (ESBM) (ver Figura N° 26).

Figura N° 26. Enterprise Security Business Model (ESBM)



De igual forma, es necesario apuntar que en general, las mejores prácticas son simplemente la mejor manera de desempeñar un proceso de negocio y la seguridad de información y gestión de la tecnología no escapa a esta realidad.

A su vez, son la manera que las empresas líderes han alcanzado el éxito, logrando obtener muchos beneficios. Algunos de los beneficios perseguidos por las organizaciones al adoptar, mantener y comunicar un marco de referencia son:

- Presentan una ventaja significativa desde la perspectiva de la seguridad y control sobre aquellas que no han adoptado algún marco de referencia.

- Si se utiliza un criterio estándar para la configuración y administración de los sistemas de la organización, se puede minimizar la posibilidad que una debilidad en uno de ellos pueda comprometer los controles de acceso de los restantes (pese a que éstos cuenten con medidas de seguridad robustas).

- Adoptando estándares y marcos de referencia internacionales, la organización puede construir una arquitectura de seguridad que permita minimizar las brechas que se puedan registrar entre las amenazas detectadas y los controles existentes, mitigando el riesgo asociado a una eventual ocurrencia de dicha amenaza.

Para comentarios sobre la encuesta o demás aspectos relativos a Prácticas de Seguridad de Información (SI), no dude en contactar con cualquiera de las siguientes personas:

Omer Useche B.
Socio encargado de la
Línea de Servicios de Asesoría Gerencial
Teléfono: (0212) 700 6225
omer.useche@ve.pwc.com

José E. Sánchez
Socio de la
Línea de Servicios de Asesoría Gerencial
Teléfono: (0212) 700 6243
jose.sanchez@ve.pwc.com

Roberto Sánchez V.
Socio de la
Línea de Servicios de Asesoría Gerencial
Teléfono: (0212) 700 6222
roberto.sanchez@ve.pwc.com

Hildemar Martínez Díaz
Socio de la
Línea de Servicios de Asesoría Gerencial
Teléfono: (0212) 700 6183
hildemar.martinez@ve.pwc.com

pwc.com