Modelo Para Seguridad de la Información en TIC

Jorge Burgos Salazar[1], Pedro G. Campos[1]
[1] Universidad del Bío-Bío, Avenida Collao 1202, Casilla 5-C P:4081112, Concepción, Chile
Jorge.burgoss@vtr.net, pgcampos@ubiobio.cl

Resumen. Este trabajo presenta un modelo para facilitar la obtención de un adecuado nivel de control de riesgos en Tecnologías de Información y Comunicación (TIC), que permita entre otros evitar y/o disminuir las fallas en los sistemas, redes, Internet y todo el patrimonio informático (hardware, software y datos) de ataques o desastres, antes que éstos ocurran. Se muestra la importancia y urgencia de este tema hoy en día, se presentan las normas, estándares y leyes más relevantes relacionadas con el tema, y se discuten brevemente los diversos aspectos involucrados en la formulación del modelo. El modelo propuesto se fundamenta en los lineamientos entregados por las normas y estándares internacionales del área, lo cual permite él entregue las bases para que cualquier tipo de organización pueda realizar un uso seguro de sus TIC.

Introducción

Hoy en día son múltiples los riesgos asociados a que equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, es por ello la necesidad de una estrategia completa de seguridad, de manera de prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas

(misma organización), que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

No se pueden obviar los factores de riesgos por desastres que al no estar previstos eficientemente y sin planes de contingencia y/o de recuperación pueden provocar daños irreparables en tiempo y costos de recuperación. Esto, que es difícilmente cuantificable, puede incluso determinar la continuidad de una organización.

En este trabajo se presenta un modelo basado en estándares y normas internacionales, para evitar y/o disminuir las fallas en los sistemas, redes, Internet y todo el patrimonio informático (hardware, software y datos) de ataques o desastres, antes que éstos ocurran, a través de un proceso de establecimiento de políticas, procedimientos, registros, controles y documentación. Este modelo puede ser utilizado como base para que cualquier tipo de organización pueda realizar un uso seguro de sus TIC.

Un problema vigente

Hoy en día no es difícil encontrar en la prensa información respecto de problemas de seguridad en TICs en empresas de todo tipo y todo ámbito, Por ejemplo, en un hecho reciente, apareció en la prensa hablada y escrita de Chile el *hackeo* (alteración) de las bases de datos del estado chileno, dando cuenta de la publicación de los datos personales de más de 6 millones de Chilenos, los cuales quedaron disponibles en un sitio de acceso público en Internet [1]. Este pequeño ejemplo muestra la vigencia y relevancia que tiene la seguridad de la información sobre todo para quienes tienen la responsabilidad de resguardarla, tenerla disponible, utilizable y segura. Estas son tareas directamente relacionadas con la plataforma de TICs que posee una organización.

Según informes y publicaciones de distintos medios e inclusive algunos elaborados por la brigada de Ciber Crimen de Investigaciones de Chile [2][3], dan cuenta que sobre el 90% de las empresas Chilenas son ignorantes en temas de seguridad de la información, donde el 96% de ellas

son incapaces de detectar un ataque o intromisión a sus sistemas, y donde el 99% de ellas no posee especialistas ni herramientas para detectar el fraude informático. En Chile, con excepción de grandes compañías multinacionales que tranzan valores en la bolsa Chilena y/o en la de Estados Unidos de Norte América y el mayor porcentaje de las empresas bancarias, no existe la adecuada conciencia ni entendimiento de la seguridad de la información de las TIC.

Tanto dueños de empresas (empresarios), y ejecutivos, no están debidamente sensibilizados al respecto, lo cual, se refleja en que grandes empresas chilenas, no se alcanza al 1% de inversión de sus utilidades en recursos informáticos [2]. Los mayores esfuerzos son desarrollados por los profesionales informáticos que en general desarrollan múltiples labores como programación, análisis, seguridad básica, etc., por lo cual, no existe un uso eficiente de todos los aspectos de seguridad. y donde el pensamiento o creencia más recurrente de las empresas es: "Esto nunca nos ocurrirá a nosotros".

Sin embargo, estos datos contrastan con el nivel de preocupación que genera este problema, según muestra un informe sobre seguridad de Cisco (ver Fig. 1), y que muestra a Chile como el segundo país de Latinoamérica con mayor preocupación en el tema, con un 56% de empresas "Muy preocupadas" por las amenazas de este tipo [4].

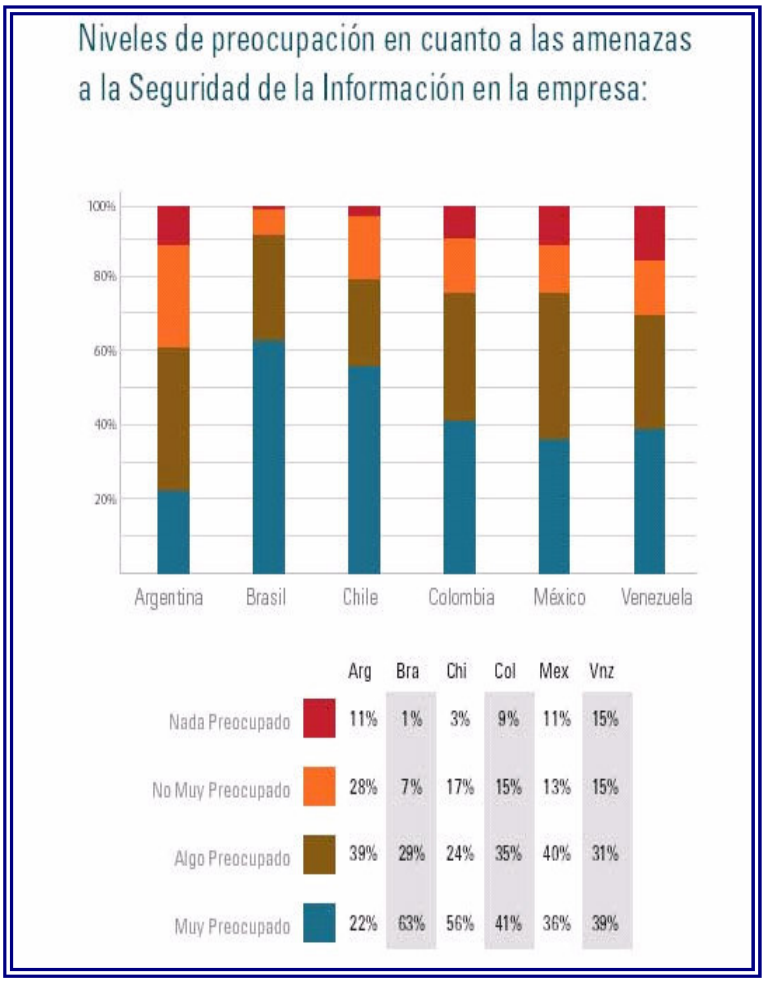

Fig.1 Niveles de preocupación por amenazas de seguridad de la información [4].

Estándares y Normas para Asegurar la Información

Para la correcta administración de la seguridad de la información, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, estos son [5]:

- **Confidencialidad**: Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

- **Integridad** : Busca asegurar:
  - Que no se realicen modificaciones por personas no autorizadas a los datos o procesos.
  - Que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos.
  - Que los datos sean consistentes tanto interna como externamente.

- **Disponibilidad**: Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

Diferentes organizaciones internacionales han definido estándares y normas que apoyan en diferente medida el cumplimiento de los requerimientos indicados anteriormente. A continuación se detallan los de mayor utilización a nivel mundial, y que fueron tomados como base para el modelo propuesto.

ISO 17.799

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización. Este estándar fue publicado por la *International Organization for Standardization* (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

COBIT

Acrónimo de "*Control Objectives for Information and related Technology*" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la *Information Systems Audit and Control Foundation* (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC. Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Esta organización realiza eventos y

conferencias, y desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante. En los últimos 5 años ha cobrado fuerza debido a que fue desarrollado en específico para el ámbito de las TIC.

ITIL

Acrónimo de "*Information Technology Infrastructure Library*", ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la *Office of Government Commerce*, una entidad independiente de la tesorería del gobierno británico. ITIL fue utilizado inicialmente como una guía para el gobierno de británico, pero es aplicable a cualquier tipo de organización.

LEY SOX

La Ley *Sarbanes-Oxley* (SOX), de EE.UU., nombrada así en referencia de sus creadores, obliga a las empresas públicas nacionales de dicho país, o extranjeras inscritas en la *Securities and Exchange Comission* a llevar un control y almacenamiento informático estricto de su actividad. La ley nace producto de grandes escándalos financieros ocurridos en compañías norteamericanas como *Enron* y *Worldcom*, durante el año 2002, en los cuales se comprobó que información financiera fue falsificada. Esta ha tenido un alto impacto a nivel mundial en empresas que transan sus valores en la bolsa de EE.UU.

COSO

La normativa COSO, acrónimo de *The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework*, está principalmente orientada al control de la administración financiera y contable de las organizaciones. Sin embargo, dada la gran cercanía que hoy existe entre esta área y los sistemas de información computarizados, es que resulta importante entender el alcance y uso de esta norma. Junto a esto son muchas otras las normas que

están directa o indirectamente relacionadas con ésta como por ejemplo COBIT.

En síntesis, el Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática.

ISO Serie 27000

A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (*Plan, Do, Check, Act*) [6] (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario (ISO 27799).

Por qué implementar controles

Un reporte de Deloitte [7], muestra como en los 12 meses previos al estudio, distintas compañías de gran tamaño enfrentaron crisis de seguridad de información.

Como conclusiones del informe se muestra que el 69% de los participantes dijo estar “confiado o muy confiado” sobre la efectividad de la organización para enfrentar retos de seguridad provenientes del exterior. Sin embargo, sólo el 56% mostró esta confianza para enfrentar las amenazas internas.

El estudio también muestra que las empresas, si bien están constituidas por activos físicos -edificios e infraestructura-, y activos de información -contenido digital-, muchas de las compañías administran los riesgos de seguridad físicos y de información como entidades separadas y distintas, lo que puede implicar pérdida de oportunidades.

Adicionalmente, las empresas deben evitar una serie de riesgos de seguridad, entre los que incluyen robo de identidad, fuga de información, fraude y otros, por lo que es necesario contar con un marco de gobernabilidad en relación a la seguridad de la información.

Del informe se desprende la necesidad de una estrategia de seguridad en la información alineada con las iniciativas de las organizaciones. De acuerdo con la encuesta, el 54% de las empresas cuenta con una estrategia, el 20% planea hacerlo en los próximos dos años; en tanto, el 17% considera que la falta de esta estrategia es una de las principales barreras para lograr seguridad en la información.

De esta forma, uno de los puntos más importantes para definir controles de seguridad de la información, es instaurar políticas claras al respecto, que establezcan un marco regulatorio para las actividades que deben ser llevadas a cabo en este contexto.

Parámetros para establecer Políticas de Seguridad de la Información (PSI).

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, por ende, debe estar avalado y contar con un fuerte apoyo de la dirección y/o máxima gerencia, ya que sin este apoyo, su implementación será más compleja e incluso puede fracasar.

Es importante que al momento de formular las políticas de seguridad de la información, se consideren por lo menos los siguientes aspectos [8]:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en proteger los activos críticos en su área.

- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.

- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Razones que impiden la aplicación de las políticas de seguridad informática. Se debe ser capaz de convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática, sino los esfuerzos de su implementación pueden ser desperdiciados [9].

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos de las empresas a no comprender exactamente la razón o motivos de las inversiones.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensible y por ende su imagen.

Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen

sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencia en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información (OSI) [10], es un rol que en general es muy reciente en las organizaciones de Chile (muy pocas lo tienen) y corresponde básicamente a quien se hará cargo de controlar y regular que toda la seguridad de la información esté y opere conforme a los lineamientos establecidos. Es quién se puede hacer cargo de todas las tareas de seguridad de TIC.

Este rol puede ser perfectamente desempeñado por una persona que esté certificada en temas de seguridad de la información (no técnica sino de administración o auditoria), sin embargo, dado el pequeño número de profesionales que obtienen este tipo de certificaciones y atendiendo a la realidad de las organizaciones, en general esta labor es cubierta por un profesional (no necesariamente informático) que se ha especializado en esta área.

La figura del OSI corresponde al encargado de coordinar, planear y promover las actividades que tengan que ver con la seguridad informática y al mismo tiempo con la seguridad de la información de toda la organización.

El propósito de tener esta figura es contar con alguien a quien se pueda recurrir en caso de algún problema de seguridad, un encargado de difundir

las alertas, así como de proponer y definir esquemas que reduzcan los incidentes de seguridad que se presenten.

El OSI tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización.

Implementar y Estructurar Controles

Con el propósito de enfrentar correctamente los procesos de auditoria y a la vez para satisfacer un adecuado nivel de control interno en las actividades de TIC, se deben diseñar controles, de manera que ellos abarquen a todos los procesos que se manejan por medio de las TIC en una organización. En todo este proceso el OSI juega un papel de relevancia, puesto que con su experiencia se pueden realizar estas implementaciones en forma adecuada y con la relevancia que la organización requiere.

En sí, los controles deben estar construidos en base a áreas (procesos) y objetivos de control de los cuales se deben desprender las actividades y finalmente los controles en si. Por ejemplo la norma ISO/IEC 27002 describe 39 objetivos de control. Sin embargo, otras normas o estándares como ISO 17799, ITIL y COBIT proponen un número distinto de controles.

De manera de apoyar la implementación del modelo propuesto y de modo de hacer práctico el proceso de estructurar e implementar controles, el modelo entrega una estructura, con una base de 85 objetivos de control de los cuales nacen 120 controles generales para TIC. Esta base de controles debe ser ajustada según el ámbito de la organización y los alcances de sus actividades en TIC.

Estos controles han sido establecidos conforme al estudio de los estándares antes citados, considerando especialmente las indicaciones de ISO 17799 e ISO/IEC 27002), y pretenden ser una guía para quien estime su activación. Es importante recalcar que los controles en si no bastan para tener un correcto gobierno de TI, ya que ello solo se puede alcanzar

cuando existe todo el marco compuesto por políticas, procedimientos, informes, registros, instructivos y controles.

Actualmente esta base de controles se encuentra operativa en algunas empresas de Chile (se reserva su identidad, por políticas de seguridad). Estos controles han sido revisados y aprobados en su implementación por distintas entidades de auditoria de renombre nacional e internacional, lográndose, por ejemplo, la reducción de las indicaciones. La aplicación de esta base de controles en algunas empresas de Chile ha permitido mejorar los resultados obtenidos en procesos de auditoria de estados financieros anuales, disminuyendo considerablemente las indicaciones hacia áreas de TIC. Algunas mediciones con base ISO muestran importantes mejoras en niveles de seguridad al implementar estos controles, midiendo aspectos tales como implementación de PSI, organización de la seguridad, gestión de activos, seguridad del recurso humano, gestión de continuidad, gestión de comunicaciones y operaciones, destacándose que al implementar PSI se alcanza una diferencia mayor a 20 puntos porcentuales sobre el promedio de empresas Chilenas evaluadas, otro ejemplo es la gestión sobre la continuidad operaciones en donde se alcanza una diferencia de poco mas de 17 puntos porcentuales sobre el promedio. No obstante el nivel de mejora respecto a empresas del mismo sector y el buen nivel del manejo de riesgo, al comparar los resultados con el sector bancario, en algunos casos los resultados están bajo 30 puntos porcentuales, esto debido a que el sector bancario ha realizado los mayores esfuerzos en este sentido, dado lo significativo de este aspecto en sus actividades.

Las organizaciones que tienen mayor interés en asegurar y demostrar menor riesgo son las instituciones y organizaciones bancarias-financieras [10] (el activo de información en este caso, puede efectivamente determinar la continuidad de sus operaciones). Ellas están en obligación de implementar estándares y metodologías de clase mundial que permitan el resguardo a sus clientes (como los citados anteriormente), en contrapuesto a una Pyme, que si bien tiene el foco comercial bien establecido, está claramente muy por debajo de esta línea de confianza respecto a la seguridad de sus TIC, ya que no tiene este nivel de obligación, que sin embargo, puede ser un diferenciador de mucha relevancia. La aplicación del esquema de controles que presenta este

modelo puede ser aplicado en organizaciones grandes y pequeñas, en las cuales, los resultados de su implementación retornarán beneficios de seguridad, confiabilidad, integridad y disponibilidad de la información que resguarde y/o utilice por medio de TICs. Esto, junto al giro de la organización puede significar un aumento de confianza de sus clientes respecto a la información que de ellos se maneja, y pudiera en definitiva ser un aspecto "diferenciador" de otras organizaciones.

Cada control o grupo de controles forma parte de su objetivo de control, del cual se desprenden las actividades de control que dan origen al control en sí. A su vez cada objetivo forma parte de una agrupación mayor que es el proceso. Los procesos están agrupados en 7 grandes áreas que son: *Mantención*, *Seguridad*, *Operaciones*, *Desarrollo*, *Acceso General*, *Recuperación de Desastres*, y *Computadores*. Por ejemplo, para el proceso de *Seguridad*, uno de los objetivos de control considerados es *Toda la información es respaldada en forma oportuna y adecuada*; uno de los controles asociados a este objetivo es *Monitoreo de errores en respaldos en servidores*.

La tarea que debe asumir cada organización, conforme a su propia realidad es la de identificar cuál es la evidencia que cubre al respectivo control, lo que es particular y propio a cada organización; inclusive es altamente probable que uno o varios controles no apliquen al contexto de la organización. Ante esta situación lo que se recomienda es mantener el control, pero indicar en su evidencia o actividad que éste, dado el contexto particular de la organización "no aplica". Junto a esto se debe realizar lo indicado por COBIT y COSO en base a definir si los controles serán de efecto primario o secundario para los estados financieros de la organización, lo cual, permitirá dar la criticidad a cada uno de ellos.

La concreción de las tareas de control se pueden plasmar en un solo documento, en el cual se identifique la lista de procesos, objetivos de control y controles de TIC, la cual será la base de revisión que debe ser monitoreada con la periodicidad que defina la organización donde la evidencia de cada control constituirá el elemento central que probará la efectividad del control.

La actividad anteriormente señalada debería ser realizada por el OSI y/o por un auditor interno o externo, además se recomienda realizar el proceso en conjunto con la alta dirección y con él área de finanzas a fin de evaluar que controles serán clasificados como primarios y secundarios en orden a alinearse conforme a la normativa COSO y determinar así cuáles son los reales impactos en los estados financieros. Así se podrá dar relevancia y prioridad a los controles. En todas estas actividades de definición de controles debería participar activamente el OSI de forma tal que pueda ser el interlocutor válido ante procesos de auditoría interna o externa.

Estos controles deben estar abalados por políticas, procedimientos e instructivos que permitan operar de manera clara, precisa y sin ambigüedades de tal forma de asegurar el correcto cumplimiento de los controles y de la evidencia que de ellos se desprenda.

Modelo de Control de Riesgos de Seguridad de la Información en Áreas de TIC.

Si bien el modelo PDCA [6], es el estándar formal de ISO, éste se construye sobre una base que no necesariamente se aplica a todas las organizaciones, sobre todo cuando éstas no se han involucrado en procesos relacionados con normas ISO, por ello, con una base práctica se presenta el siguiente modelo, el cual no omite ni restringe las actividades señaladas en el modelo formal, sino que se vale de ellas para sustentar un formato práctico de actividades que deben ser abarcadas para lograr un adecuado nivel de seguridad de la información en las áreas de TIC en cualquier tipo de organización.

Este modelo puede ser perfeccionado y modificado en el futuro dado que su estructura se debe ajustar a los constantes cambios que surgen de las organizaciones como sistema dinámico.

La particularidad del modelo que se presenta a continuación reside en su aspecto operativo y práctico, puesto que se considera su estructuración, formación e implementación bajo dos grandes fases.

- Fase de Elaboración
- Fase de Aplicación

Estas fases contemplan el conjunto de actividades que de ellas se desprenden y están ligadas mediante la secuencia de actividades que es necesario desarrollar a fin de elaborar y aplicar correctamente el modelo.

Este modelo considera los principales elementos incluidos en las diversas normas y estándares internacionales relacionados con la seguridad de la información, por lo que creemos que apoya la concreción de un "Gobierno de TIC", lo que a su vez abarca un aspecto mayor al que su diseño se orientó inicialmente, ya que esto implica que no solo cubre temas de seguridad y de riesgos, sino a que al mismo tiempo apoya a lograr aspectos de estructura organizacional, descripciones de cargo y tareas, definiciones de misión y visión, no solo a nivel gerencial, sino que a nivel de cada área de TI.

La Fig. 2 presenta el modelo en forma esquemática. El esquema presentado resume y agrupa todas las actividades y se debe entender que muchas de ellas llevaran un ciclo continuo de mejora.

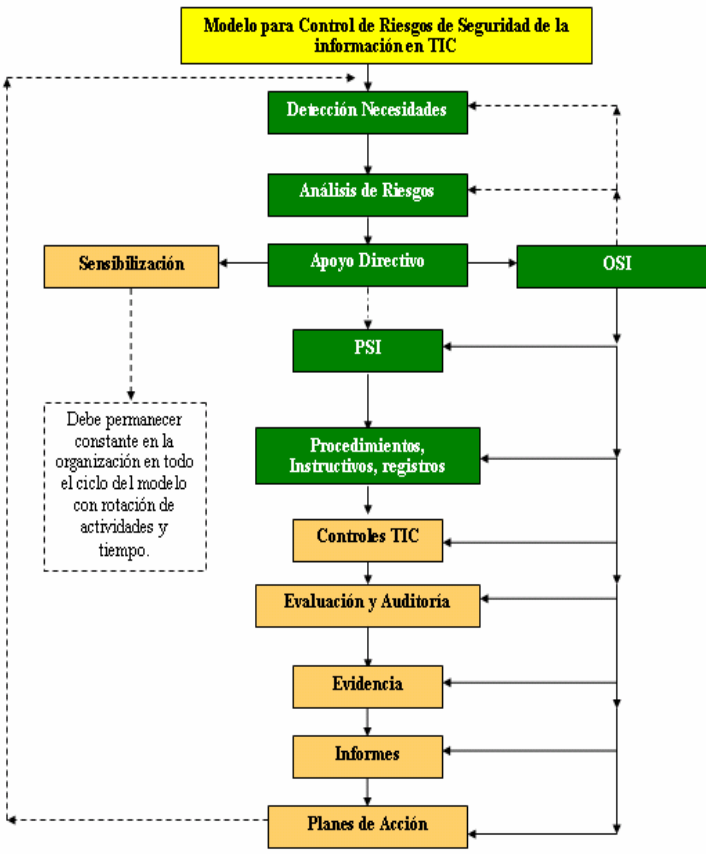

Fig. 2. Modelo de Control de Riesgos de Seguridad de la Información en Áreas de TIC

Las actividades son secuenciales y a la vez se comportan en un estado cíclico con periodos de tiempos en su ciclo que varían dependiendo de cada organización y del estado de avance que ella tenga respecto a temas de seguridad de la información.

A continuación se presenta una descripción de cada una de las fases y actividades que ellas consideran [11]:

- Detección de Necesidades: Corresponde al levantamiento de todas las actividades relacionadas con los impactos que la organización pueda tener en relación con su seguridad de la información.

- Análisis de Riesgo: Corresponde a evaluar todos los potenciales riesgos en los cuales se pueda ver envuelta la organización por aspectos emanados de las TIC y que impactan en la seguridad de la información.

- Apoyo Directivo: Corresponde a la presentación del resultado de las etapas anteriores con el fin de conseguir el apoyo para concretar la implementación de la seguridad de la información (presupuestos, personal, capacitación, etc.)

- OSI: La organización debe designar a un OSI para que realice, apoye, dirija y pueda llevar el control de implementación y posterior seguimiento a todo el modelo de seguridad de la información. Además el OSI estará presente en todas las actividades y con énfasis en la fase de aplicación en la cual participa en forma activa en todas las actividades que se indican de aquí en adelante.

- Confección PSI: Corresponde al diseño de las Políticas de Seguridad de la Información de la organización.

- Confección de procedimientos, instructivos y registros: Corresponde al desarrollo de documentos que formalicen como se deben realizar las actividades y que información es la que se debe retener como evidencia para dar conformidad a las PSI.

- Controles TIC: En esta etapa se diseñan y definen los procesos, objetivos de control, controles y evidencias formales de las actividades de seguridad que darán sustento a los procesos de revisiones o auditorias del modelo.

- Evaluación y auditoria: En esta etapa se debe realizar, preparar y desarrollar la revisión que avale que todos los procesos de TI se están cumpliendo y llevando a cabo adecuadamente, lo cual será evaluado por el mismo proceso de auditoria (interna y/o externa).

- Evidencia: En esta etapa se busca verificar de manera adecuada que todos los registros de TI para todos sus procesos y controles estén disponibles para cualquier tipo de revisión, particularmente a los procesos de auditoria.

- Informes: Esta etapa contempla la confección de informes del proceso de revisión que derivarán en actividades de mejora al modelo y con

revisiones por parte de la dirección de la organización que permitan confeccionar adecuados planes de acción.

- Planes de Acción: Esta etapa consiste en la aplicación de los planes de acción conforme a los plazos y actividades que fueron indicados en el proceso de auditoria. Estos planes de acción pueden conformar la revisión y ajustes de todo tipo de actividades ya sea a nivel de procesos de seguridad, de evidencias, de políticas o de cualquier otra actividad que sea identificada.

- Sensibilización: Esta etapa (incluida en ambas fases del modelo) permite entregar constante información (alertas) a la organización sobre la importancia de mantener la seguridad de la información y el resguardo de todas las actividades de TI. Recibe un apoyo directo de la dirección de la organización.

Aporte del Modelo

Este modelo se apoya en el análisis de los estándares y normas de la seguridad de la información presentados, junto a los alcances y formas de implementación, más el rol del OSI y la implementación de controles.

Su principal aporte es ser un facilitador en la implementación y/o aplicación de la seguridad de la información para TIC en cualquier tipo de organización.

La estructura que presenta el modelo se basa sobre la implementación práctica y concreta relacionada con las actividades que permitan dar seguridad a la organización, la cual, en base a sus propias necesidades, lineamientos y perspectivas de negocio, busca mantener su información asegurada.

Otro aspecto importante que aporta este modelo, es que, por su presentación simple puede ser correlacionada sin mayor dificultad con las actividades que realiza cualquier tipo de organización, de manera que ella logre asegurar la información en conformidad a la realidad de TIC que disponga.

En la implementación del modelo se debe tener conocimiento de las funciones, tareas, actividades y diseño relacionadas con cada una de las etapas, por lo cual, se enfatiza en el rol de un OSI, ya que con su aporte la

organización podrá estructurar de forma adecuada su seguridad. El rol del OSI es relevante en el control, monitoreo y seguimiento de los planes de acción, ya que esto permite el ciclo continúo de perfeccionamiento y de vida del modelo.

El presente modelo, avalado en los estándares presentados en este artículo, pretende ser una solución y aporte en la implementación de la seguridad de la información de cualquier organización.

El modelo además considera los tipos de documentos (procedimientos, registros) necesarios para implementar un adecuado nivel de control de las TIC, para esto, se entregan ejemplos y opciones basados en que su desarrollo se adapte al tamaño y avance de las TIC en cualquier empresa o institución (detalles en [11]). El modelo no entrega documentos desarrollados (procedimientos, instructivos), sino que sienta las bases para su desarrollo. Esto se justifica en que cada empresa u organización tiene sus propios entornos y realidades, por lo cual, el desarrollo acabado de este tipo de implementaciones requiere de un detalle superior que escapa al alcance de este estudio.

Conclusiones

En este trabajo se han descrito los principales elementos considerados en la definición de un Modelo de Seguridad de la Información en TIC. Se expuso un breve análisis de la relevancia y urgencia del tema, y se presentaron las principales normas, estándares y leyes relacionadas con la gestión de seguridad de información, y que fueron consideradas como base para este modelo. Además, se discutió brevemente los diversos aspectos involucrados en la definición de un modelo de seguridad de información, y se presentó un esquema del modelo propuesto. Si bien este modelo puede parecer muy simple, esto se debe a que todas sus actividades engloban de una u otra forma lo detallado en las normas y estándares presentados, pero bajo un esquema generalizado y adaptable a cada organización. Se debe tener presente que este modelo es totalmente perfectible, ajustable y que puede ser dimensionado conforme a las particularidades y tamaño de la organización en la cual pueda ser implementado. Dada la gama de actividades consideradas en el modelo, consideramos que este puede ser la base para establecer un “Gobierno de TI” en las organizaciones que lo utilicen.

Referencias

[1] Terra. "Publicados en Internet los datos personales de seis millones de chilenos", fecha de actualización: 11/05/2008, fecha de consulta: 15/07/2008, disponible en http://actualidad.terra.es/articulo/publicados_internet_datos_personales_chilenos_2465456.htm

[2] S. Miranda, A. Ibarra y L. M. Astorga. "Empresas minimizan peligro informático". Diario El Mercurio, Chile, Ed. 29/04/2008

[3] Microsoft Latino América. "Vivir para el cambio", fecha de actualización: 18/09/2006, fecha de consulta: 15/07/2008, disponible en http://www.microsoft.com/latam/technet/articulos/tn/sep06-16.mspx.

[4] Cisco. "Cisco 2007 Annual Security Report". 2007.

[5] Borghello, C. "Seguridad Informática: sus implicacncias e implementación". Tesis de Licenciatura en Sistemas, Universidad Tecnológica Nacional, Argentina, 2001.

[6] W. E. Deming. "Calidad, Productividad y Competitividad: La Salida de la Crisis". Ed. Díaz de Santos, España, 1989.

[7] I. Brightman, J. Buith. "Treading Water. The 2007 Technology, Media & Telecommunications Security Survey", Deloitte, 2007.

[8] M. Farias-Elinos, M. C, Mendoza-Diaz y L. Gómez-Velazco. "Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática". Techno-Legal aspects of Information Society and New Economy: an Overview. Information Society book series, 2003.

[9] IT Governance Institute. "Information Security Governance: Guidance for Boards of Directors and Executive Management", 2º Ed. EE. UU., 2006.

[10] Peltier, T. R. "Information Security Risk Analysis", CRC Press, 2005.

[11] J. Burgos. "Modelo para el Control de Riesgos de Seguridad de la Información en Áreas de Tecnologías de la Información y Comunicaciones (TIC)", Informe de Proyecto de Título, Ing. (E) Computación e Informática, Universidad del Bío-Bío, Concepción, Chile, 2008. Disponible en Biblioteca y/o Departamento de sistemas de información la facultad de ciencias empresariales.