Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica

Gustavo Pallas y María Eugenia Corti

Grupo de Seguridad Informática, Instituto de Computación, Facultad de Ingeniería,
Universidad de la República
J. Herrera y Reissig 565, Montevideo, Uruguay
gpallas@adinet.com.uy
mcorti@fing.edu.uy
http://www.fing.edu.uy/inco/grupos/gsi

Resumen Un Sistema de Gestión de la Seguridad de la Información (SGSI), definido por la norma ISO/IEC 27001, no sólo debe considerar el contexto de la industria y características culturales de la Organización, sino que también debe ser sostenible en el tiempo, con capacidad de incorporar mejoras de forma incremental y continua, con un beneficio comprobable para la Organización. Para ello se requiere de una metodología bien definida que acompañe el dinamismo necesario de la empresa/Organización y de la industria y a su vez respete las estrategias empresariales y vinculación estructural.
Este artículo describe lineamientos metodológicos, de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI para una empresa o grupo empresarial atendiendo a su estructura de grupo multiempresa y diversidad en los niveles y dominios de seguridad requeridos.

Palabras clave: Sistema de Gestión de la Seguridad de la Información, Seguridad de la Información, ISO/IEC 27001.

1. Introducción

Cada vez existe mayor conciencia y consenso de la importancia de la Seguridad de la Información en empresas y Organizaciones, cualquiera sea el sector de la economía o rol en la sociedad que desempeñen. Sin embargo, existen estructuras empresariales que requieren que éstos temas sean analizados con una estrategia diferente, ya sea por la criticidad de la información que manejan, su dimensión o su estructura empresarial.

Grandes corporaciones o grupos empresariales, como pueden ser: empresas del sector financiero, salud, operadoras de telefonía, gubernamentales, etc., poseen una dimensión de la problemática de la Seguridad, diferente a las de una pequeña empresa. Deben tener en cuenta además, motivos legales, regulaciones y contratos, y muchas veces, la seguridad de la información es parte del propio negocio. Además de la dimensión, el factor estructural es en muchos casos un

elemento diferenciador que amerita que este tipo de empresas sea analizado de forma particular al momento de adoptar un SGSI.

La seguridad de la información, no es un activo a comprar, ni un fin en si mismo, tampoco un estado a alcanzar haciendo una determinada inversión; debe gestionarse, deben existir metas concretas, criterios generales de evaluación y de decisión, y debe poder medirse. Es un sistema dinámico en constante evolución que debe ser evaluado y monitoreado, con métricas establecidas que permitan, comparar de manera consciente y objetiva escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos que se invierten. Todo esto se ve potenciado en un grupo empresarial.

Es necesario entonces lograr una metodología que conduzca a una solución eficaz y eficiente, desde el punto de vista técnico y económico, que provea los niveles de seguridad requeridos y brinde la confianza necesaria a las empresas, a los socios de negocios y a los usuarios. Esta metodología deberá considerar aspectos como las necesidades de los procesos del negocio con respecto a la información, aplicaciones y servicios, así como el uso eficiente de los recursos tecnológicos como soporte de estos procesos. Se requiere de un enfoque estratégica y económicamente proactivo y racional en la evaluación y tratamiento de riesgos, con un criterio amplio, considerando todos los aspectos y factores involucrados, pero concreto y consistente en las definiciones y decisiones más convenientes para la empresa con particular atención en la continuidad del negocio y los procesos estratégicos.

El presente trabajo aborda la problemática que se plantea al momento de implantar y gestionar un SGSI, tal como se define en la norma ISO/IEC 27001 [1], para una Organización perteneciente a un grupo empresarial.

Existen diversos trabajos, metodologías y herramientas que abordan la temática de la implementación y gestión de SGSI. Algunas de ellas como [2] son antecedentes incluso para la norma BS7799-3 [3] y por ende para la ISO/IEC 27005 [4]. Algunas declaran además de ser compatibles y cumplir los requerimientos de la norma ISO/IEC 27001, otras como [5] declaran tener objetivos diferentes a los de la norma pero igualmente ser compatibles con ésta, especialmente en la fase de Planificación, y en las otras fases, tener importantes aportes para los procesos y documentos requeridos. Por otra parte, en [6,7] se presenta una metodología de Análisis y Automatización de la Implantación de SGSI en empresas del tipo microempresas y PyMEs. Dicha metodología está enfocada "a cubrir a aquellas organizaciones que generalmente no poseen metodologías, prácticas, ni requerimientos de seguridad específicos o generales".

Sin embargo, no hemos encontrado un trabajo específico que abarque las características y necesidades de una empresa como la que nos planteamos en el presente caso de estudio, es decir, la de un grupo empresarial constituido por una empresa principal y otra/s subordinada/s, cuyas necesidades son de naturaleza diferente a una PyME por ejemplo, debido entre otras cosas, a su estructura, dimensión y relacionamiento jerárquico.

Este artículo esta estructurado como se describe a continuación. La sección 2 describe y analiza los aspectos asociados a la implantación de un SGSI en

una estructura empresarial jerárquica. La sección 3 describe la metodología propuesta, concentrándose en la etapa de planificación. En la sección 4 se señalan las características deseables de un software de apoyo a la implementación. La sección 5 concluye.

2. Aspectos relacionados a la estructura empresarial jerárquica

Este trabajo considera la problemática que surge al tratar de implantar un SGSI en un grupo empresarial, particularmente en empresas con una relación de dependencia jerárquica, con una empresa principal y una o más empresas subordinadas que podrían funcionar como un área de negocio especifica. Un ejemplo claro de este tipo de relación empresarial, es el de una empresa de Telecomunicaciones que se integra verticalmente con una empresa proveedora de servicios de Internet (ISP).

Si bien son dos empresas diferentes, existe una estructura empresarial en una relación jerárquica que se propaga o afecta a estrategias empresariales, infraestructura compartida, políticas, objetivos, recursos, etc. Esta relación no escapa a la Seguridad de la Información. Es así que, la empresa dependiente debe considerar lineamientos básicos de la empresa principal o dominante del grupo empresarial. Pero a su vez, como empresa en sí misma, tiene preocupaciones, objetivos, prioridades y riesgos propios e inherentes a su actividad, más allá de su incidencia en la empresa principal del grupo.

Pueden presentarse entonces la siguientes problemáticas:

- Los riesgos detectados y las prioridades percibidas, por la empresa principal, en la empresa dependiente, no coinciden con las prioridades y riesgos detectados por esta última. Esto puede darse porque la evaluación de prioridades local a la empresa menor, no siempre tiene en cuenta el impacto en la empresa principal, ya sea porque no están explícitamente alineados los objetivos empresariales o por falta de visión global. También puede suceder lo contrario, que globalmente no se consideren aspectos específicos o claves para la empresa cuando se baja el nivel de abstracción.
- Al existir infraestructuras compartidas, los servicios que involucran a ambas compañías pueden no estar explícitamente valuados y por ende las valoraciones de riesgo pueden no estar adecuadamente calibradas o pueden inducir a decisiones locales no alineadas con la conveniencia global.
- A veces los presupuestos de ambas empresas son independientes, y también los retornos de inversión, no se adecuan a políticas que son aplicadas por parte de la empresa principal.

Se hace necesario entonces armonizar o alinear los objetivos y prioridades en lo que a la Seguridad de la Información refiere y particularmente los SGSI de ambas empresas, de forma que, por un lado, se atiendan los lineamientos del grupo, los definidos por la empresa principal, sin ser percibidos como simples restricciones que deben cumplirse por mandato, sin un valor agregado.

Por otra parte, lograr la autonomía necesaria y la agilidad/capacidad de acción para la definición de un SGSI propio que permita gestionar la Seguridad de la Información y preservar los activos de acuerdo a las necesidades propias.

Es necesario, además, coordinar la asignación de recursos para atender prioridades del grupo y no de una sola de las empresas. Debe buscarse una metodología que permita que los SGSI de ambas empresas sean definidos, implantados y gestionados de forma cooperativa, de acuerdo a los intereses del grupo y que esta cooperación se dé de una forma eficaz y eficiente.

En la Figura 1 se ilustra esta necesidad de compatibilizar criterios en dos ejes, por un lado en el eje vertical, la jerarquía propia que responde al modelo general de seguridad establecido, hacia el interior de una empresa, donde el SGSI debe responder a los planes estratégicos y necesidades del negocio alineados con la misión y visión, respetando el marco legal vigente. Por otro lado en el plano horizontal, se refleja esta necesidad de armonizar y alinear las políticas de seguridad, hecho que se da con mayor énfasis en el SGSI de la empresa subordinada, que está a su vez comprendido o alcanzado, en su medida, por el SGSI de la empresa principal.

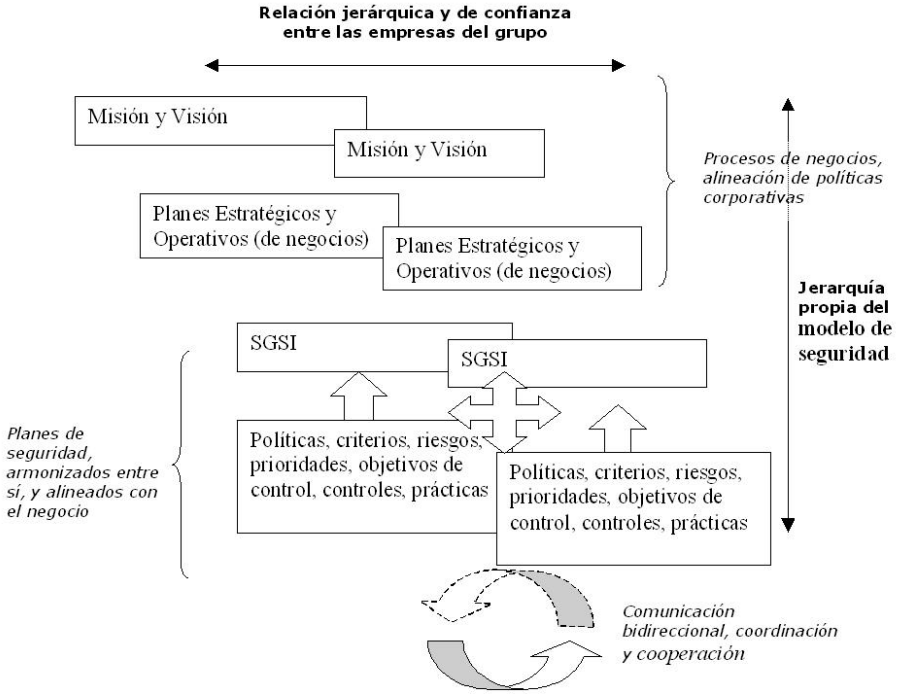

Figura 1. Posicionamiento jerárquico relativo del SGSI en un grupo empresarial

3. Metodología de implantación

En esta sección se describe la metodología propuesta para la implantación de un SGSI en un grupo empresarial con relación jerárquica, concentrándonos en la etapa de planificación del modelo PDCA (Plan Do Check Act), definido en la norma ISO/IEC 27001 [1]. Se presentan además diferentes alternativas de enfoque y estrategia y se discute su conveniencia o no.

3.1. Enfoque Centralizado, Distribuido o Mixto

La metodología definida busca ser eficiente, en recoger las directrices que vienen del SGSI de la empresa jerárquicamente mayor y a su vez, trasladar el *feedback* y las necesidades de la empresa subordinada. Por ello se hace necesario, definir y especificar la relación en términos de responsabilidades de Seguridad de la Información entre la empresa subordinada y la principal del grupo. Aquí pueden darse las siguientes alternativas:

Centralizado: Que exista un único SGSI y la Seguridad de la Información sea gestionada en forma central en el nivel más alto del grupo empresarial.

Distribuido: Que cada empresa tenga su propio SGSI y estos sean independientes.

Mixto: Un esquema mixto, donde existan dos SGSI pero relacionados e integrados. Donde se respete la naturaleza jerárquica estructural entre ambas empresas del grupo, pero también la autonomía operativa de cada una de ellas.

Un enfoque centralizado, si bien es más simple en su definición, se hace impracticable o muy complejo si la dimensión de la empresa, o grupo empresarial, es importante o de estructura más o menos compleja. La tarea de afrontar todos los riesgos y controles para todas las áreas o dominios de aplicación y todas las tecnologías parece ser muy ambiciosa e inabarcable de forma precisa, profunda y consistente.

Por otra parte, un enfoque totalmente distribuido e independiente, no parece responder a la naturaleza jerárquica y estructura empresarial. En este caso, si los planes estratégicos y objetivos no están precisamente alineados, pueden darse situaciones ambiguas, diferencias de percepción de prioridades en los riesgos o ineficiencia en la gestión y operativa de la Seguridad.

La metodología propone utilizar un enfoque mixto, de dirección centralizada pero con capacidad operativa distribuida. Un enfoque sistémico, con una visión de todo el conjunto, con sus relaciones jerárquicas y estratégicas de forma global, pero con la flexibilidad de afrontar las definiciones e implementaciones de forma más local y acotada, a los efectos de hacerlo manejable y atender las especificidades de sus ámbitos de aplicación, en términos del negocio, las tecnologías involucradas y los conocimientos requeridos.

3.2. Actividades de la etapa de Planificación

La Figura 2 ilustra la interacción y cooperación propuesta entre ambas empresas, para cada actividad del ciclo PDCA del SGSI. El objetivo es armonizar el SGSI de la empresa subordinada con el de la empresa principal del grupo.

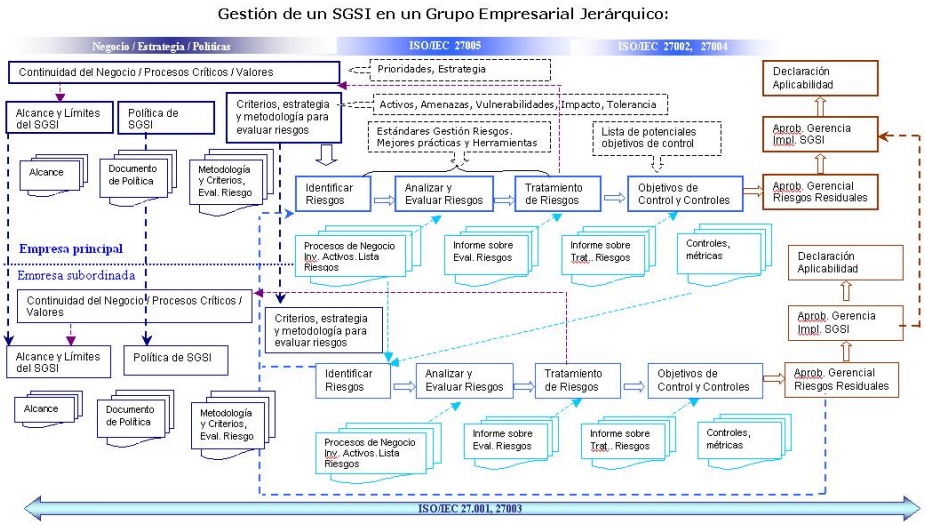

Figura 2. Propuesta metodológica

Alcance y Límites: La empresa principal, en general va a alcanzar a la empresa menor. Si esto es así, debe contemplarse el SGSI y política de la empresa principal a los efectos de ser más específicos en el detalle de políticas y controles si así se requiere y tratar las excepciones o propuestas que requieran de un tratamiento excepcional a lo que es la política general.

Política del SGSI: La empresa subordinada, deberá corresponderse o ser consistente con la Política del SGSI de la empresa principal o del grupo empresarial. Esto no quiere decir que no pueda ser más específica, de hecho muy probablemente lo será, pero deberá respetar la política general. La Política de Seguridad es una política más de la empresa, por lo tanto, la estructura del grupo empresarial y políticas generales serán las que determinen, con que autonomía y bajo que lineamientos se relacionarán ambas empresas.

Evaluación de riesgos: Si bien la evaluación de riesgos de ambas empresas puede ser independiente, si se establecen parámetros de correspondencia o fórmulas de conversión de uno a otro, a los efectos de favorecer la interoperabilidad y cooperación, es conveniente que compartan la estrategia, criterios, metodologías y eventualmente herramientas de análisis y gestión de riesgos.

3.3. Estrategia de evaluación de riesgos

Atendiendo a la necesidad de alinear las estrategias y políticas generales con respecto a la seguridad de la información, y a una conveniente relación costo/beneficio en lo global, lo más adecuado es un enfoque de alto nivel que guíe la estrategia de identificación, evaluación y priorización de riesgos.

En este enfoque global, no se debería entrar en detalles tecnológicos concretos ni particularidades del dominio de aplicación. Este análisis, debería en principio estar delegado a los especialistas del dominio o "dueños" del negocio/aplicación/información, quienes tomarán como insumo las políticas globales, los lineamientos y evaluación de riesgos con un enfoque sistémico, de alto nivel. Posteriormente, en función de los mismos, y de las necesidades concretas del dominio (su ámbito de aplicación) y conocimientos específicos, deberán hacerse las evaluaciones locales así como la definición de controles y la estrategia de implementación.

Sin embargo, atendiendo a la especificidad y complejidad de cada área o dominio de aplicación, un análisis racional con un criterio de efectividad y eficiencia, conlleva a delegar las evaluaciones y establecimientos de controles concretos así como la percepción local de riesgos adicionales (relacionados o no con los definidos a nivel global), permitiendo enriquecer la evaluación con una visión técnica o de mayor proximidad con los profesionales competentes y especializados. En este caso, puede ser necesario eventualmente, elevar determinada percepción de riesgos si es necesaria su consideración a un nivel superior. Tendríamos una implementación de controles y aporte (como retorno) del riesgo percibido *Bottom Up*.

Proponemos utilizar una estrategia de evaluación de riesgo combinada. *Top Down* en las definiciones estratégicas de alto nivel, con foco en el negocio e independiente de las particularidades de cada área y de aspectos tecnológicos concretos, y *Bottom Up* en la implementación de controles y retroalimentación del riesgo percibido por los especialistas de cada área.

De esta forma se suman los beneficios obtenidos por la adecuación a los planes empresariales globales y alineación con los objetivos del negocio y la seguridad de la información, con la efectividad y eficiencia de los aportes que deben ser realizados por las áreas que dominan la especificidad requerida para los temas de más bajo nivel (tecnológicos por ej.).

En [8] se presenta una estrategia de evaluación de riesgos "de dos etapas" que justamente combina una primer etapa de alto nivel con una etapa posterior de bajo nivel. Esta estrategia se adapta muy bien a las necesidades detectadas para el caso que nos compete. En el documento referido se presenta la evaluación de riesgos como un par de fases combinadas con distinto enfoque en cuanto a su granularidad y refinamiento sucesivo, afinando el nivel de detalle donde los activos y procesos de negocio lo ameriten.

3.4. Organización, estructura y relacionamiento

Para cada una de las etapas del SGSI, a lo largo del ciclo PDCA, debe establecerse qué roles serán necesarios y cómo se vincularán entre sí. Estos roles

no tienen por qué coincidir exactamente con el organigrama de la empresa ni del grupo empresarial, pueden incluso constituirse a los efectos de la seguridad de la información.

Quienes deben participar en la definición del SGSI . En [9] se distingue entre tres niveles diferentes de gestión de la seguridad de la información:

Estratégico: - Dirige y Provee - Define los grandes lineamientos gerenciales para la seguridad de la información y política global del SGSI, coordina y aprueba los recursos.

Táctico: - Implementa y Optimiza - Diseño e Implementación del SGSI, establece objetivos concretos/específicos, gestiona los recursos.

Operacional: - Ejecuta y reporta – Intenta alcanzar los objetivos específicos mediante procesos técnicos.

Este enfoque sintetiza la necesidad de estructurar las definiciones de seguridad según su alcance y nivel jerárquico. También se adecua con el enfoque sistémico y la estrategia – multifase - elegida, por refinamiento desde lo global hacia dominios específicos.

Por otro lado, en [10] se presentan diferentes estructuras u organigramas posibles para la Seguridad de IT de organizaciones de diferentes dimensiones. En particular nos interesa la propuesta para organizaciones medianas y grandes. Allí se presenta la necesidad de tener un responsable de seguridad para cada orden o contexto jerárquico de la empresa, es decir: un responsable global de la seguridad de IT, un responsable de la seguridad de IT por Área, y un responsable de la seguridad por proyecto/ sistema. Adicionalmente se presenta la necesidad de un comité responsable de la coordinación de la seguridad de IT, y un equipo responsable de gerenciar la seguridad de IT. Este último coordina actividades globales a la organización, da lineamientos globales y gerencia las diferentes fases del sistema de gestión de seguridad, dando soporte a los oficiales de seguridad de los diferentes contextos (global, área, proyecto/ sistema).

Adicionalmente, la norma ISO/IEC WD 27003 [11] alineada también con la ISO/IEC (FDIS) 27005 [4], presenta las necesidades con respecto a la organización, roles requeridos y presenta también un ejemplo de organización posible.

Teniendo presente, estas recomendaciones, atendiendo a la estructura empresarial objeto de este trabajo y a las necesidades de coordinación propuestas hasta el momento entre las empresas, proponemos una estructura como la que se ilustra en la Figura 3 y cuyos roles se describen a continuación.

Dirección y Gerencia General: La alta Dirección y Gerencia es la encargada de aprobar la Política de Gestión de Seguridad de la Información, asignar los roles en materia de seguridad y coordinar el seguimiento de los planes de la Seguridad en la Organización.

Comité de Seguridad: Lleva un rol de liderazgo del SGSI, en sus lineamientos directrices y debe tener un rol ejecutivo para asegurar que se cumplan las actividades y etapas requeridas. Planifica y gestiona los recursos y el

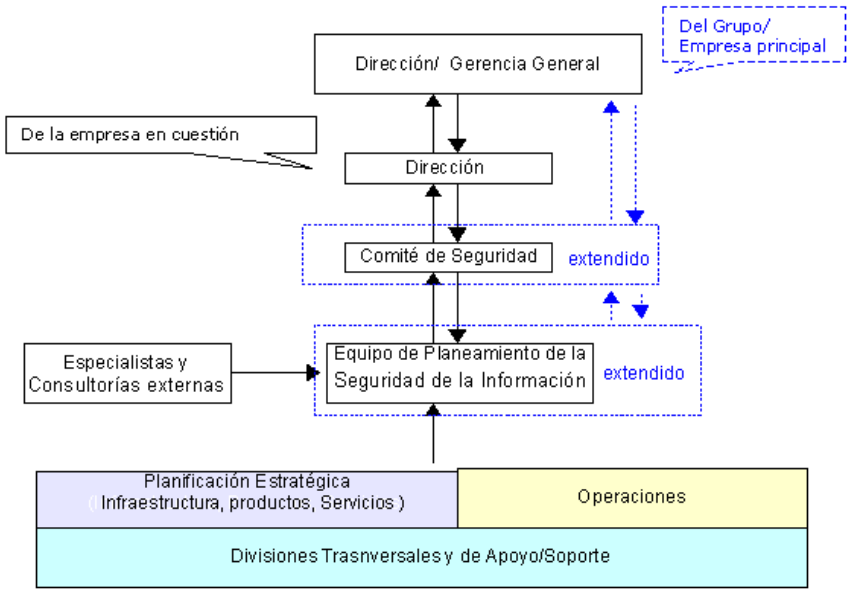

Figura 3. Esquema de Organización

ambiente para llevar adelante la gestión de riesgos y el establecimiento del SGSI. Planifica y define los documentos y contenidos del SGSI y gestiona la aprobación de la Dirección. Considera mejoras al SGSI en función de los resultados y métricas. Es deseable que estén representados aquí los intereses de seguridad de la información de todas las áreas funcionales, Divisiones y Departamentos, así como los procesos prioritarios. Debido a la estructura del grupo empresarial, y a las necesidades de alinear los SGSI de la empresa subordinada con el grupo empresarial, y que muchas veces comparten Divisiones de Apoyo o Soporte a las actividades sustantivas de la empresa, este Comité deberá integrarse tanto por profesionales de la empresa en cuestión como por responsables de la Gerencia de la Seguridad de la Información de la empresa principal del grupo (Comité de Seguridad extentido) y eventualmente de la Gerencia General si fuera necesario. Particularmente en lo que refiere a la decantación de las políticas corporativas, y los lineamientos estratégicos para arminizar ambos SGSIs. Sin embargo, de acuerdo al alcance de los temas a tratar, y para darle la flexibilidad necesaria a la organización, este Comité podrá funcionar en su forma extendida o reducida según se acuerde y se requiera, y así sea convocado. De todas formas es deseable que el Comité se reúna en su modalidad extendida así sea menos frecuentemente, por ejemplo, al menos una o dos veces al año.

Equipo de Planeamiento de la Seguridad de la Información: Especia - listas de Seguridad internos. Es deseable la participación y el asesoramiento profesional de especialistas de la Seguridad de la Información y sería de valor contar con ellos en la empresa (de forma interna). Deben tener buen conocimiento de los activos de información importantes de la empresa en el alcance del SGSI. Debe coordinar posibles conflictos de intereses entre Divisiones y Departamentos en lo que refiere a la Seguridad de la Información. Como se dijo anteriormente, el dimensionamiento y cantidad de personas asignadas en cada una de estas estructuras o grupos, dependerá del tamaño y tipo de la organización/ empresa. En el caso extremo por ejemplo, el Equipo de Planeamiento de la Seguridad de la Información, puede ser un Oficial/ Responsable de Seguridad que eventualmente convoca la participación de otras gerencias; manteniendo la responsabilidad sobre el primero que deberá ser un cargo independiente de las otras gerencias para preservar los intereses de cada rol y no comprometer las decisiones con diferentes intereses sobre la misma persona.

Asesoramiento y Vínculos externos: También es un aporte importante el intercambio, colaboración y asesoramiento de especialistas y grupos externos de Seguridad de la Información tanto de la industria como del sector académico (Consultoras, Facultad de Ingeniería, especialistas, etc.), de forma de seguir las tendencias de la industria, el uso de estándares, métodos y herramientas de forma de poder incorporar la evolución de la disciplina, la evolución de la industria e incorporar las lecciones aprendidas (propias y por otros). En ese sentido es muy importante el aporte y experiencias (propias y ajenas) de las organizaciones y los profesionales en torno a los incidentes de seguridad (CSIRT / CERT). En particular, los incidentes en organizaciones comparables a la empresa o grupo empresarial en cuestión, del mismo sector industrial. Debería promoverse un enfoque sistémico y multidisciplinario y no sesgado al área tecnológica o únicamente de IT.

Debe precisarse que algunas características de estos roles y estructuras, como ser su dimensionamiento, su grado de autonomía en sus funciones, su carácter de permanente o convocados a demanda, así como la frecuencia de su intervención, dependerán del tamaño y características de las empresas, su autonomía y verticalidad en la relación institucional. No obstante, es importante que la responsabilidad de la Seguridad recaiga sobre un rol que es independiente de los otros roles de gestión, a los efectos que no haya conflictos de intereses por compartir roles o responsabilidades ajenas a la seguridad por una misma persona, responsabilidades que no siempre están alineadas con la seguridad, con intereses diferentes.

3.5. Documentación

Tal como lo establece la norma ISO/IEC 27001, se requiere de un respaldo documentado de las decisiones tomadas así como una trazabilidad o correspondencia entre las decisiones de la gerencia de alto nivel en cuanto a objetivos, políticas, principios y lineamientos de la seguridad de la información, y las acciones

tomadas en referencia a la definición de procedimientos, criterios de evaluación de riesgos, registros, etc.

Los registros son la evidencia, de que los controles surgen de la evaluación de la mejor alternativa como consecuencia del análisis de riesgos y responden a objetivos de control fijados previamente. Los registros permiten hacer esta cadena de decisiones y definiciones, además de trazables, reproducibles y sirven además como referencia en la comunicación y coordinación con la empresa principal del grupo.

Estructura de la documentación Es deseable que un SGSI sea claro, preciso y fácil de entender. Por otra parte, debe comprender a todos los requisitos de la norma y todo lo que se defina en su alcance y la política misma.

Por todo lo expuesto en la necesidad de un enfoque combinado con necesidades de actualización con diferentes niveles de frecuencia y con contenidos de naturaleza diferente en su relevancia y detalles técnicos, resulta natural proponer una estructura de documentación, que se adapte a estas características. Un documento principal con los lineamientos básicos, dados por la Dirección, más estables en el tiempo y que guía la cobertura de todos los aspectos del SGSI y las etapas sucesivas, y una serie de documentos anexos, que eventualmente variarán con mayor frecuencia y requieren de análisis más detallado y de conocimiento específico del dominio.

Más allá de las revisiones inevitables, esta estructura propuesta tiene por objetivo lograr que el documento no pierda rápidamente vigencia, y lograr consistencia en la granularidad de la profundidad conceptual y niveles de abstracción o detalle en lo que a seguridad refiere. Se gana así en claridad y en la propia mantenibilidad del mismo.

El documento principal no debería contener detalles propios de cada dominio de aplicación, ni de instrumentación de políticas específicas ni tampoco procedimientos o detalles operativos. Es conveniente separar esta documentación específica en documentos de soporte al documento principal. De esta manera tendremos:

Un documento maestro o principal del SGSI
Documentos de soporte al SGSI:
- `Políticas técnicas (de dominio, alcance y cometido específico)`
- `Procedimientos`
- `Guías e instructivos de operación`

En el caso general, el documento maestro o principal del SGSI de la empresa principal y el de la empresa subordinada coincidirán, de forma que compartirán los lineamientos macro de la política de la seguridad de la información. Eventualmente podrían ser documentos diferentes, pero en cualquier caso, el documento maestro del SGSI de la empresa subordinada deberá respetar y comprender al documento maestro de la empresa principal. El mismo podrá contener algún agregado o ser más específico dado que su dominio de aplicación es menor, pero

en ningún caso deberá incluir políticas específicas ni procedimientos y prácticas tecnológicas, que deberán ser documentos anexos y de soporte.

Entendemos que esta estructura brinda los siguiente beneficios:

- Simplifica la lectura y facilita la comprensión, separando los conceptos o lineamientos y política general del SGSI por un lado, de los detalles de políticas específicas en documentos diferentes.
- Separa los conceptos medulares, que varían menos frecuentemente, de las políticas y detalles de instrumentación específicos, de variación más frecuente.
- Flexibilidad a la hora de modificar, revisar el SGSI. Facilita su mantenimiento, revisión y auditoría.
- Permite complementar e integrar políticas específicas fácilmente sin alterar la estructura del documento principal.
- Facilita la capacitación, difusión y entendimiento.
- Favorece la estrategia *Top Down* en el nivel macro, alineándose con los planes de negocios y dirección de la empresa y a su vez la efectividad de definir los controles y políticas específicas en los niveles propios de su dominio (controles y procedimientos *Bottom up* en su instrumentación).

4. Características deseables de Software de Apoyo al SGSI

En esta sección, se describen las características del software que apoye el establecimiento, gestión y mejora de un SGSI en una empresa de las características que nos ocupa. No se especifican formalmente los requerimientos, sino tan sólo se brindan una lista de funcionalidades deseables de acuerdo a lo analizado en las secciones anteriores.

El software referido debería brindar funcionalidades que permitan:

- Heredar todos los lineamientos, metapolíticas y recomendaciones aplicables ya sean de la ISO/IEC (UNIT) así como aquellas más específicas del área o gobierno.
- Facilitar la armonización y eficiencia del proceso de acoplamiento e integración del SGSI de la empresa subordinada con el de la empresa principal sin duplicar costos, ni controles innecesariamente, y ayudar a establecer una correspondencia (y cumplimiento en lo que corresponda) entre las políticas establecidas para la empresa principal y la/s subordinada/s.
- La Gestión de Documentos con definición de roles, gestión de permisos de consulta y modificacón, de forma que la documentación sea tratada como un activo más, preservando sus requerimientos de Confidencialidad, Integridad y Disponibilidad.
- Funcionalidades de workflow donde se puedan identificar roles, etapas de relevamiento, definición, comunicación y delegación, supervisión, escalamiento, etc., que comprenda la naturaleza jerárquica del grupo empresarial.

- Heredar clasificaciones de activos y riesgos realizadas por la empresa principal del grupo, que alcancen particularmente a activos y procesos dentro del dominio del SGSI de la empresa subordinada. Estas clasificaciones podrán ser ponderadas por parte de ésta última, en función de la jerarquía establecida y la criticidad percibida en forma corporativa (o por la empresa principal) o podrán tratarse como un mínimo aceptable (cota inferior) en el caso que las clasificaciones heredadas sean obligatorias. El software debería ser configurable, y tratar esto mediante coeficientes de ponderación, roles y permisos para cambiar ciertos valores asignados.
- Identificar y clasificar los procesos y sus activos asociados, valorizando los mismos en función de la escala establecida en cuanto a su necesidad de: confidencialidad, integridad y disponibilidad. Puede resultar interesante filtrar el grafo (o matriz) de dependencias para los procesos de negocios de determinada categoría (por ejemplo críticos o estratégicos, de alta prioridad).
- Analizar riesgos aplicando una estrategia combinada como la descrita. Es decir, una estrategia Top-Down en los lineamientos de alto nivel y corporativos que pueda refinarse de forma sucesiva, pero también la posibilidad de elevar ciertos riesgos detectados y percibidos a niveles técnicos y de dominios de aplicación específica que requieran ser considerados a un nivel superior.
- Enfocar el análisis y tratamiento de riesgos en cualquiera de los atributos interesantes para el análisis de seguridad: confidencialidad, integridad y disponibilidad. Es decir, posibilidad de filtrar o visualizar el grafo de dependencias y valoración de procesos y activos según el atributo de seguridad que se desea analizar. Esto puede realizarse si el software ofrece la posibilidad de visualizar layers o subgrafos a este nivel.
- Ayudar a detectar e identificar procesos y activos críticos así como ayudar a lograr eficiencia operativa y eficacia en el establecimiento de controles y salvaguardas atendiendo a las dependencias entre procesos y activos.
- Realizar revalorizaciones de activos de forma periódica
- Facilitar el establecimiento y comparación de escenarios de riesgos, ya sea con el transcurso del tiempo (evolución), o en etapa de planificación, evaluación y diseño de controles.
- Establecer vistas y trabajar por capas de abstracción, en el sentido de estar alineado con la Recomendación ITU-T X.805 [12], gestionando layers (Infraestructura, Servicios y aplicaciones), planos (gerencial, control y usuario final) y las ocho dimensiones de seguridad establecidas en la Recomendación.

5. Conclusiones

Un grupo empresarial, con una estructura de relación jerárquica o de subordinación, requiere de una metodología que permita gestionar la seguridad de la información y que la misma considere su estructura empresarial y su relacionamiento vertical. Es necesaria la cooperación de los SGSIs de las empresas, en todas las fases del ciclo PDCA, fundamentalmente en la fase de Planificación,

pero a su vez cada SGSI requiere de la flexibilidad y agilidad operativa suficiente para alcanzar los niveles de seguridad necesarios y los objetivos propuestos respetando los lineamientos corporativos.

Proponemos un enfoque mixto, de dirección centralizada pero con la autonomía necesaria a nivel de cada dominio y cada empresa, fundamentalmente en la gestión de controles y en la percepción del impacto de los riesgos locales. Esto permitirá aunar criterios y optimizar recursos cuando los riesgos deban afrontarse en forma conjunta. Entendemos que debe primar fundamentalmente un enfoque costo/ beneficio orientado a las necesidades de seguridad de la información del negocio, y que a los efectos de (re)dimensionar adecuadamente el alcance del SGSI de manera efectiva, se opta por una estrategia multifase, de refinamiento sucesivo, desde lo global a los dominios locales. Esta estrategia determinará en una primera etapa los procesos y activos críticos, y permitirá, en fases posteriores dedicar el esfuerzo y recursos a los activos y procesos que así lo ameritan, dotando así a la metodología de eficiencia además de eficacia. El redimensionamiento del alcance, es necesario para dar cumplimiento a la norma ISO/IEC 27001 en cuanto a la clasificación de todos los activos alcanzados por el SGSI. A los efectos de alinear el modelo de negocios, puede resultar de utilidad, la adopción de estándares, eventualmente específicos para el sector.

Atendiendo a la estructura empresarial, a su naturaleza de relacionamiento jerárquico entre las empresas, pero también a una estructura física muchas veces distribuida, sería muy importante poder disponer de un software que apoye la metodología definida, fomentando esta coordinación y cooperación, con procedimientos e hitos bien definidos, promoviendo los lineamientos directrices corporativos y una retroalimentación de las fuentes de seguridad de la información específicos de las diferentes áreas.

Un enfoque y estrategia de planificación *Top Down*, favorece la alineación de criterios, compatibiliza los modelos de negocio, los lineamientos de carácter estratégico y política de alto nivel de la seguridad de la información, permitiendo una fácil armonización de los SGSIs, separando lineamientos corporativos de políticas específicas de dominio. Esto es aplicable tanto a la metodología de evaluación de riesgos como a la estructura de la documentación.

En cada etapa del ciclo PDCA del SGSI cada una de las empresas del grupo debería tener la mayor información posible a los efectos de aplicar criterios y lineamientos corporativos o ajustar los parámetros adecuados para la percepción y estimación de riesgos, tanto locales como corporativos. Debería permitir escalar riesgos locales percibidos, así como heredar los riesgos percibidos y priorizados desde los estratos superiores, de manera de alinear los planes de Seguridad de la Información de la forma más conveniente en función de los recursos, objetivos concretos y condicionantes.

Referencias

1. International Organization for Standarization. Information technology - Security techniques - Information security management system - Requirements (ISO/IEC 27001:2005), 2005.

2. CRAMM. Information security toolkit. http://www.cramm.com, 04 2009.
3. British Standards Institute. Information Security Management Systems.Guidelines for information security risk management (BS 7799-3:2006), 2002.
4. International Organization for Standarization. Information technology - Security techniques - Information security risk management (ISO/IEC 27005:2008), 2005.
5. MEHARI. Information risk analysis and management methodology. https://www.clusif.asso.fr/en/production/mehari/, 04 2009.
6. María Eugenia Corti. *Análisis y automatización de la implantación de SGSI en Empresas Uruguayas*. Tesis de maestría, Universidad de la República, Facultad de Ingeniería, 2006.
7. G. Betarte M. E. Corti, R. de la Fuente. Hacia una Implementación Exitosa de un SGSI. In *Actas del 3º Congreso Iberoamericano de seguridad Informática (CIBSI'05)*, pages 457–471, 2005.
8. Krzysztof Lisek Andrzej Bialas. Integrated, business-oriented, two-stage risk analysis. In *Proceedings of the International Multiconference on Computer Science and Information Techonology*, pages 617–628. Institute of Innovations and Information Society, 2007.
9. ISM3. Information Security Management Maturity Model. http://www.ism3.com/, 04 2009.
10. Federal Office for Information security - Germany. BSI Standard 100-2 IT-Grundschutz Methodology, 04 2009.
11. International Organization for Standarization. Information technology - Security techniques - Information security management system implementation guidance (ISO/IEC FCD 27003), 2005.
12. Telecommunication Standardization Sector (ITU-T). Recommendation X.805 Security architecture for systems providing end-to-end communications. http://www.itu.int/rec/T-REC-X.805-200310-I/en, 2009.