Instituto de Computación – Facultad de Ingeniería
Universidad de la República

Tesis de Maestría
en Ingeniería en Computación

Metodología de Implantación de un SGSI en un grupo empresarial jerárquico

Ing. Gustavo Pallas Mega

Tutor:	Dr. Gustavo Betarte
Tribunal:	Dr. Luis E. Sánchez Crespo MSc. María Urquhart MSc. Cristina Mayr

Montevideo, Uruguay
Diciembre 2009

Metodología de Implantación de un SGSI en un grupo empresarial jerárquico
Gustavo Pallas Mega
ISSN 1510 7264
Tesis de Maestría en Ingeniería en Computación
Instituto de Computación – Facultad de Ingeniería
Universidad de la República
Montevideo, Uruguay, Diciembre 2009

Agradecimientos:

Al Dr. Gustavo Betarte y la MSc. María Eugenia Corti, por sus aportes en los lineamientos, sus comentarios y el tiempo dedicado en la lectura de versiones preliminares.

Al Dr. Luis Enrique Sánchez Crespo, en su carácter de revisor internacional del presente trabajo, por su buena disposición, aportes y comentarios al mismo.

Al personal de Anteldata y de Antel, en especial al Ing. Eduardo Carozo – Gerencia de la Seguridad de la Información, y al Ing. Carlos Martínez - CSIRT, por la disposición y el tiempo otorgado en las entrevistas y consultas realizadas.

A Pati, por el apoyo incondicional y su comprensión.

A mis padres, por haberme dado todo lo necesario para llegar hasta aquí, y mucho más.

Resumen

Es un hecho que los sistemas de gestión y de información están muy arraigados en los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. Esta dependencia de los sistemas de información en general, requiere dotar de seguridad a los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de sus activos. Ya no es suficiente con establecer controles en forma aislada ni ad hoc, tampoco es suficiente actuar de modo meramente reactivo y defensivo, se requiere de un sistema de gestión de seguridad de la información (SGSI) y un accionar proactivo. Si consideramos un grupo empresarial, donde dos o más empresas se integran verticalmente, el desafío de gestionar la seguridad de una manera conveniente es aún mayor.

Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos (serie ISO/IEC 27.000), y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información (por ejemplo ISM3); sin embargo, en la especificación de las mismos no se afronta su aplicación a un grupo empresarial, lo cual requiere consideraciones adicionales.

En este trabajo, se analizan diferentes enfoques de estos estándares, con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI en un grupo empresarial jerárquico. Se presentan además diferentes alternativas estratégicas y se discute sobre su conveniencia o no. Se analizan diferentes métodos conocidos de análisis y gestión de riesgos.
Algunos de ellos promovidos por los gobiernos y/o industria de países de vanguardia y trayectoria reconocida en la seguridad de la información que han tenido gran aceptación.
Se promueve un enfoque sistémico y pragmático, no dogmático, en pro de una metodología eficaz y sostenible, primando un criterio de conveniencia costo-beneficio. Se enfatiza la necesidad de su orientación y adecuación a los reales requerimientos de seguridad del negocio.

Se presenta una metodología adecuada a un grupo empresarial, que busca integrar lo mejor de cada uno de los enfoques analizados; se incluye una propuesta de organigrama de Seguridad que compatibiliza la jerarquía estructural del grupo y las necesidades de un SGSI.
Adicionalmente se incursiona en la aplicación de técnicas de grafos para la valoración de activos; se formaliza el concepto en términos de propiedades y algoritmia de grafos, y se define con una visión propia del tema, un algoritmo para el ajuste contemplando valoraciones cualitativas y cuantitativas y dependencias parciales y/o totales entre activos.
También se describen características y funcionalidades deseables de una herramienta de software de apoyo a la metodología.

Finalmente se analiza la aplicación de la metodología a un Caso de Estudio, en particular, un 'Internet Service Provider' (ISP) integrado verticalmente con una 'TelCo' (empresa de Telecomunicaciones). En el mismo se analizan las particularidades del caso de estudio: los estándares y recomendaciones internacionales específicos, el modelo organizacional aplicable al negocio, datos estadísticos, y la seguridad requerida para este sector de la industria.

Palabras Clave: SGSI, ISO/IEC 27.001, Grupos Empresariales, Relación Jerárquica.

TABLA DE CONTENIDO

INDICE DE ILUSTRACIONES

INDICE DE CUADROS

1 Introducción

En la actualidad, es un hecho incuestionable que la gran mayoría de los procesos de negocios e industriales son soportados, automatizados y gestionados por sistemas informáticos, así como los sistemas de información apoyan la actividad gerencial y la toma de decisiones; incluso muchas veces, es la propia información y el acceso a la misma, el producto / servicio que se intercambia como principal objeto del negocio. La seguridad de la información ya no puede ser concebida como el resultado de un accionar defensivo y reactivo para preservar los activos del negocio, ya que muchas veces, es un activo en si mismo, una condición para operar y/o competir en el sector, un generador de valor. Requiere un accionar proactivo y su incorporación como elemento estratégico. A modo de ejemplo, una empresa que gestione adecuadamente la seguridad de la información, por un lado da cumplimiento a sus obligaciones y regulaciones, y a su vez genera confianza en sus clientes y potenciales inversores.

Por lo tanto, cada vez hay más conciencia y consenso [82] en la importancia de la Seguridad de la Información en las empresas y Organizaciones cualquiera sea el sector de la economía o rol en la sociedad que desempeñen, en particular en las empresas medianas y grandes ([1]). Sin embargo, existen diversas industrias y estructuras empresariales que hacen que algunos temas deban ser analizados y estudiados con una estrategia diferente, ya sea por la criticidad de la información que manejan, su dimensión o su estructura empresarial.

A modo de ejemplo, pequeñas empresas, con una infraestructura limitada y sistemas informáticos de gestión que no requieran del almacenamiento y procesamiento de información confidencial o crítica ni están sujetos a estrictas normas regulatorias, normalmente van a enfrentar riesgos menores, deben considerar aspectos diferentes al de una gran corporación o grupo empresarial, y también una dimensión del problema diferente, tanto en la problemática como en la de la capacidad de gestión de la solución. Por lo tanto su estrategia y decisiones responderán a estas diferencias estructurales.

Organizaciones más grandes, como pueden ser: empresas del sector financiero, salud, operadoras de telefonía, gubernamentales, etc., deben afrontar la Seguridad de la Información de forma metodológica, planificada y con planes concretos, con un enfoque de continuidad del negocio y mejora continua. Además de parámetros y dimensiones diferentes en su relación costo – beneficio, existen motivos legales, regulaciones y contratos que requieren de la protección de información personal y sensible además de la crítica y estratégica del negocio.

De acuerdo a algunas encuestas internacionales [79], el mayor riesgo a la seguridad de la información, está dado por el factor humano, específicamente errores, conductas inapropiadas y/o negligencia generadas internamente.
También existen referencias [78] donde se asegura que la inversión en la gestión de seguridad (de IT) es más efectiva que la inversión en tecnología para mejorar los niveles de seguridad.

El desafío es 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

[1] Más de 250 empleados.

brinde la confianza necesaria a las empresas, a los socios de negocios y a los usuarios. Bajo este enfoque es necesario tener en cuenta:

- Las necesidades de los procesos del negocio con respecto a la información, aplicaciones y servicios telemáticos.
- El uso eficaz y eficiente de los recursos tecnológicos como soporte de estos procesos de negocios.
- Un enfoque proactivo, estratégica y económicamente racional en la evaluación y tratamiento de riesgos, con un criterio amplio, consistente y concreto de costo / beneficio. Amplitud en el análisis considerando todos los aspectos y factores involucrados, pero concreto y consistente en las definiciones y decisiones más convenientes para la empresa.
- La confiabilidad de las soluciones con particular atención en la continuidad del negocio y los procesos estratégicos (críticos y de mayor valor).

1.1 Motivación y Enfoque

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, debe existir una meta concreta, 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 concientemente y lo más objetivamente posible, escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos disponibles.

En el presente trabajo, abordamos la problemática que se plantea al momento de implantar, operar y mantener de forma evolutiva, un *Sistema de Gestión de Seguridad de la Información* (SGSI) para una empresa u organización perteneciente a un grupo empresarial, en una relación de subordinación con otra empresa principal. Es decir, existe un orden jerárquico establecido que no será ajeno a la seguridad de la información.

Sin perder generalidad, como Caso de Estudio, y a los efectos de ilustrar los aspectos relevantes de la metodología, se considerará un Proveedor de Servicios de Internet (ISP) integrado verticalmente a una empresa de Telecomunicaciones (TelCo) atendiendo a su estructura de grupo multiempresa y la diversidad en los niveles de seguridad y dominios involucrados.

Bajo un enfoque costo – beneficio y de análisis de riesgos, una empresa debe preguntarse: ¿ Cuanto invertir ?, ¿ Hasta dónde / cuando parar ?, ¿ Cuál es el riesgo asumido en las condiciones actuales ?, ¿ Vale la pena mitigar los riesgos a los que estamos expuestos ?,
¿ Fueron consideradas todas las amenazas posibles ?
Se requiere un enfoque metodológico para dar respuesta a estas interrogantes.

1.2 Propósito

El propósito es dar lineamientos metodológicos, de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI según la norma ISO 27.001, para una empresa perteneciente a un grupo empresarial, la cual además está

subordinada con respecto a una empresa principal del grupo. Además se ilustra con un Caso de Estudio, los principales aspectos de aplicación de la misma.

1.3 Alcance

El ámbito de aplicación del presente trabajo, es amplio en el sentido que alcanza a grupos empresariales y organizaciones donde existe una relación jerárquica o de subordinación, relación que condiciona la gestión de la seguridad de la información y que debe incorporarse como tal a un SGSI.

Este trabajo, y la metodología que en él se propone, se centra en una empresa subordinada como parte constitutiva de un grupo empresarial jerárquico, donde existe otra, que denominaremos principal. Ésta última, eventualmente podría tener ya, un SGSI implantado y será considerada en cuanto al contexto y cómo condiciona al SGSI de la primera, pero no será el objeto principal de análisis.

La metodología tiene un amplio campo de aplicación, donde exista una relación de dependencia o integración vertical entre empresas. También puede aportar aspectos metodológicos, en lo referente a la jerarquización de los lineamientos de seguridad, para una entidad gubernamental en su rol de regular o generar lineamientos y/o (meta)políticas en seguridad de la información para empresas y organismos estatales. No obstante, este no es el fin perseguido en este trabajo.

1.4 Estructura del documento

En el Capitulo 2 se presenta el Estado del Arte del tema objeto de este trabajo, en particular, el marco normativo y los estándares internacionales. Se hace referencia además a los antecedentes y trabajos relacionados.

En el Capítulo 3 se analizan de forma crítica diferentes estrategias y alternativas de enfoque para una propuesta metodológica en general y el porqué del enfoque elegido para la que se define, así como nuestro posicionamiento o visión con respecto a los estándares que se referencian. Se presenta la metodología, tomando las recomendaciones de las normas internacionales, fundamentalmente la serie ISO/IEC 27.000 [25]; basándose en el ciclo PDCA (*Plan Do Check Act*) que se aplica en la norma ISO/IEC 27.001 [26] así como las guías de implementación de la ISO/IEC 27.003 [28]. Se pone énfasis en el análisis del negocio alineado con ISM3 [66] y en la gestión de riesgos, para lo cual se toma como base la norma ISO/IEC 27.005 [30] y referencias a los principales métodos conocidos. Se atienden aspectos de organización, estructura y el relacionamiento jerárquico empresarial objeto de la metodología. De forma complementaria, se describen además las características deseables que debería tener un software que apoye la metodología.

En el Capítulo 4 se presenta el Caso de Estudio, el cual es el de un ISP integrado verticalmente con una TelCo como parte de un mismo grupo empresarial. Se aplican los principales componentes de la metodología, atendiendo a las particularidades del sector de la industria así como recomendaciones y estándares internacionales que aplican al sector. Se explicitan las características inherentes del negocio, un modelo descriptivo funcional y organizacional

específico para empresas de Telecomunicaciones, las principales amenazas y riesgos más relevantes de acuerdo a estadísticas internacionales para el sector.

El Capítulo 5 concluye y hace una breve reseña que se propone para trabajo futuro.

El documento tiene ocho Anexos que se describen a continuación.

En el Anexo A se caracteriza y contextualiza el caso Anteldata, en lo que respecta a información pública citada en este trabajo así como características generales.

En el Anexo B se presentan las referencias legales que corresponden al sector del caso de estudio (ISP / TelCo) en lo que respecta a la seguridad de la información.

En el Anexo C se describe un conjunto de controles específicos para el sector de ISP / TelCo extraídos de la Recomendación internacional ITU-T Rec. X.1051 – *Anexo A - Telecommunications extended control set.*

En el Anexo D se presenta el modelo de Dimensiones, Capas y Planos de Seguridad, descrito en la Recomendación X.805 de la ITU-T: "*Security architecture for systems providing end-to-end communications*"

En el Anexo E se describe el modelo o mapa de operaciones (eTOM) para una empresa de telecomunicaciones..

En el Anexo F se presentan e ilustran grafos y subgrafos de Valoración de Activos.

En el Anexo G se detallan las propiedades del Grafo de Valuado de Dependencias introducido en este documento.

En el Anexo H se presentan los códigos de estado de las normas ISO.

2 Estado del Arte

Existen diferentes enfoques para abordar la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información. Algunos de ellos incluso con un enfoque crítico sobre otros.

Por un lado está la familia de normas de la serie ISO/IEC 27.000([2]), que agrupa una serie de normas / estándares, complementarias entre sí, relativas a un Sistema de Gestión de la Información. Las mismas están alineadas con los Requerimientos especificados en la ISO/IEC 27.001, e incluyen además, normativas sobre gestión de riesgos, métricas, auditoría, directrices / guías de implementación, etc.

Por otro lado, más recientemente ha surgido la concepción de modelos de madurez, en particular ISM3 [66] ([3]), alineado con la gestión de la calidad de la seguridad de la información. Este modelo es compatible con la norma ISO 9.001 e ISO/IEC 27.001, no obstante promueve una mayor orientación a las necesidades del negocio y es en cierta forma crítica de la norma ISO/IEC 27.001 en cuanto afirma que la misma es una norma orientada a controles, y no tanto así a las necesidades propias de la organización.

En la norma ISO/IEC 27.001 se indica que debe implementarse un sistema de gestión de riesgos que cumpla con determinados requerimientos, pero no se indica la metodología ni herramientas a utilizar. La norma ISO/IEC 27.005 establece una guía metodológica a tales efectos. Y ese es el espíritu de este conjunto de normas aplicables a cualquier sector de actividad que se describen a continuación, en la sección "2.1 Marco y Contexto Normativo – Estándares".

Sin embargo, en ninguna de estas normas se plantea el problema de una empresa vinculada a otra como parte de un grupo empresarial, donde además existe una relación jerárquica / de subordinación, relación que se proyecta a la seguridad de la información, y más específicamente, debe reflejarse en un Sistema de Gestión de la Seguridad de la Información (SGSI).

Por otra parte, existen estándares específicos para determinados sectores de la industria o rubros de actividad. Algunos de ellos homologados por la ISO/IEC y otros, de buenas prácticas y recomendaciones de Organizaciones específicas del sector de la industria, como lo son las recomendaciones de la ITU-T para el sector de las Telecomunicaciones.

En [52] puede encontrarse una breve descripción y una comparación entre un conjunto importante de métodos y herramientas de análisis y gestión de riesgos. La mayoría de estos métodos utilizan un ciclo de PDCA (*Plan Do Check Act*) o de mejora por refinamiento sucesivo y muchas de ellas son compatibles con la norma ISO/IEC 27.001. Algunas están más orientadas al sector de IT específicamente y otras son más generales, presentando incluso plantillas de controles y amenazas por dominio a los efectos de facilitar la auditoría o revisión de cumplimiento y asimismo también, actuar como línea base de seguridad, como punto de partida que cubre la gran mayoría de amenazas y riesgos comunes. Algunas de estas

[2] Desarrollada por el ISO/IEC JTC 1/SC 27.
[3] Desarrollado por Vicente Aceituno y su equipo de expertos asociados.

herramientas admiten la configuración e integración con una base de datos específica del dominio o sector de la industria involucrado.

Se analizan además en este trabajo, estándares y metodologías de gestión de la seguridad que fueron inicialmente o son promovidos, algunos por gobiernos y otros por la industria de países de vanguardia y de trayectoria reconocida en la seguridad de la información (UK, Alemania, USA)[25][49][73][78], otros de países con un marco legal comparable al de Uruguay (España) [3] y otros que, también como los anteriores, tienen amplia aceptación en la industria y difusión internacional (Francia). [48]

2.1 Marco y Contexto Normativo - Estándares

En la Figura 2.1 se ilustra el marco normativo de los diferentes estándares que, de una u otra manera, están vinculados a un Sistema de Gestión de la Seguridad de la Información.
En él se ven representados estándares internacionales de diferente naturaleza y con diferente alcance. Algunos de ellos, como por ejemplo la serie ISO/IEC 27.000 e ISM3, son específicos de la gestión de seguridad de la información, generales y aplicables a cualquier sector de actividad. Pero también deben tenerse en cuenta otros estándares y recomendaciones que son específicas del sector. Incluso puede existir la necesidad de alinear más de un estándar, como por ejemplo ITIL [75][76] con la familia ISO/IEC 27.000, o de esta última con la ISO 9001, por citar otro ejemplo.

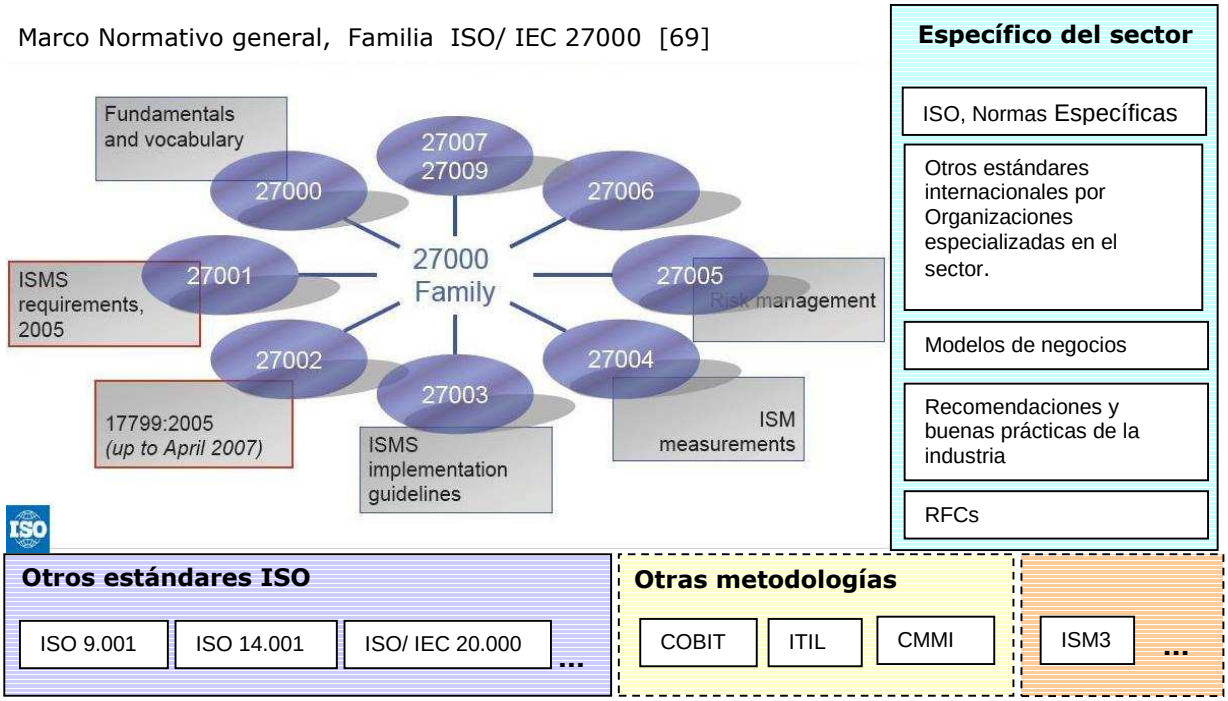


Figura 2.1 – Contexto Normativo de un SGSI

Un SGSI, como sistema de gestión que es, de una disciplina específica como lo es la seguridad de la información, debe relacionarse con otros sistemas de gestión, por ejemplo de Gestión de Calidad entre otros. Es así que también deben considerarse en el contexto, estos otros sistemas y los respectivos estándares metodológicos en los que se apoyan.

2.1.1 Serie ISO/IEC 27.000

Las normas de la familia ISO 27.000 [25], destacando fundamentalmente la ISO/IEC 27.001 e ISO/IEC 27.002, tienen como principales objetivos:

- Establecer un marco metodológico para un SGSI.
- La adopción de controles proporcionales a los riesgos percibidos.
- La documentación de políticas, procedimientos, controles y tratamiento de riegos.
- Identificación y asignación de responsabilidades al nivel adecuado.
- Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica.
- Generación y preservación de evidencias.
- Tratamiento de los incidentes de seguridad.
- Revisión y mejora continua del SGSI.
- Gestión de Riesgos
- Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio SGSI.

Los lineamientos metodológicos y los requerimientos de la norma ISO/IEC 27.001 son propuestos bajo el enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA)([4]).

Entre ellas existen normas que son básicamente una especificación de Requerimientos como la ISO/IEC 27.001 e ISO/IEC 27006. Otras son guías de implementación o lineamientos guía que son soporte del ciclo PHVA para los sistemas de gestión de la seguridad de la información, como la ISO/IEC 27003 o ISO/IEC 27.005.

A continuación, se describen brevemente los más relevantes para este trabajo [61]:

"ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary", provee información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI

"ISO/IEC 27001:2005 - Information technology - Security techniques - Information Security Management Systems - Requirements", es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un SGSI.

"ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management" - provee una guía de implementación de los controles aplicables a la seguridad de la información. Presenta once (11) cláusulas de control de la

[4] O la correspondiente sigla en inglés PDCA (Plan, Do, Check, Act)

seguridad que contienen un total de treinta y nueve (39) categorías de seguridad y por lo tanto igual número de indicaciones de Objetivos de Control, con varios Controles por cada uno de ellos. Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27.001.

"ISO/IEC 27003 ([5]) - Information technology - Security techniques - Information security management system implementation guidance" - provee información práctica y una guía de implementación de la norma ISO/IEC 27001.

"ISO/IEC 27004 ([5]) - Information technology - Security techniques - Information security management measurements" provee una guía y consejos para el desarrollo y uso de métricas para evaluar la efectividad de un SGSI, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, de acuerdo con la norma ISO/IEC 27001.

"ISO/IEC 27005:2008 - Information technology - Security techniques - Information security risk management" – provee una guía metodológica para la Gestión de Riesgos de una Organización, alineada con los requerimientos de la norma ISO/IEC 27001.

"ISO/IEC 27006:2007 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems" – establece los requerimientos para Organismos que prestan servicios de auditoría y certificación.

"ISO/IEC 27007([5]) - Information technology - Security techniques - Information security management systems - Auditor guidelines" - provee una guía para la realización de las auditorías de un SGSI y la competencia de los auditores, de acuerdo a la norma ISO/IEC 27001.

2.1.2 Otras normas referenciadas

A continuación se describen algunas normas que si bien no son de seguridad, están referenciadas en el presente trabajo [61].

"ISO/IEC 20000 – Service Management" es el estándar internacional reconocido para la gestión de los servicios de TI.

"Serie ISO 9000 – Sistemas de Gestión de Calidad" es la serie para la gestión de calidad. Se destaca la ISO 9001 que establece los Requerimientos que debe cumplir un Sistema de Gestión de Calidad.

"Serie ISO 14000 – Sistemas de Gestión Medioambiental" es una serie de normas para la gestión medioambiental. Se destaca la ISO 14001 aceptada internacionalmente que establece los requerimientos para un sistema de gestión medioambiental eficaz.

[5] Under development

2.1.3 Recomendaciones específicas del sector

Son Recomendaciones, buenas prácticas y estándares de otras organizaciones especializadas en el sector de actividad específico de la industria que se analiza.
Para una mayor claridad del documento estas Recomendaciones serán referidas en el Caso de Estudio.

2.1.4 ISM3

ISM3 [66] es un modelo de gestión de madurez de la seguridad de la información alineado con los principios de gestión de calidad de la ISO 9.001 y aplicados a los sistemas de gestión de seguridad de la información (SGSI) .
En él se establecen diferentes niveles de seguridad, donde partiendo desde un nivel inicial en el que se identifica el posicionamiento de la empresa, ésta puede plantearse como meta alcanzar determinado nivel que considere conveniente para sus necesidades de seguridad y adecuado para su disponibilidad de recursos.
Es un modelo basado en procesos con foco en las necesidades de seguridad del negocio, de forma de establecer la seguridad requerida en forma *top down* basado en las funciones de negocio. Para ello sigue un criterio de efectividad de las medidas de seguridad tomadas y su impacto en el mismo, estableciendo la necesidad de métricas y apoyándose en el paradigma: "*lo que no se puede medir no se puede gestionar*" .
Sus creadores y seguidores tienen una visión crítica de la norma ISO/IEC 27.001 porque la conciben como una norma basada en controles (y no en procesos) y no lo suficientemente alineada con las necesidades del negocio. No obstante, declaran la compatibilidad de ISM3 con la norma referida para la implementación y mejora de un SGSI, aplicando el modelo propuesto por ISM3 y dando cumplimiento a los requerimientos de la norma ISO/IEC 27.001.

2.1.5 CObIT

CObIT [74] define una metodología y un marco de trabajo adecuado para la gestión de Tecnología de la Información (IT), orientado en el negocio y en procesos, y basado en controles. Para ello considera tres dimensiones: a) los dominios, procesos y actividades de IT; b) los requerimientos de la información del negocio; y c) los recursos de IT.
Define cuatro dominios, con sus procesos (34) que a su vez describen actividades concretas y especifican una serie de objetivos de control. Estos dominios son: *Planificación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (ES),* y *Monitoreo y Evaluación (ME).*
En particular, en el dominio *PO,* se centra la atención en la alineación de IT con los objetivos y estrategia del negocio, y en la gestión de riesgos. Así como en *ES,* se especifica un proceso de "*Aseguramiento de Continuidad del Servicio / Operaciones*".
A los efectos de satisfacer los objetivos de negocio se definen siete criterios en términos de requerimientos de la información, ellos son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento (marco legal y reglamentario, normas, contratos, etc.), y confiabilidad.

En cuanto a los recursos, y para el fin propuesto, se consideran los siguientes: aplicaciones, infraestructura, información y recursos humanos.
En [97] se analiza la compatibilidad y complementariedad de CObIT con la norma ISO/IEC 17.799 (en la actualidad ISO/IEC 27.002), donde se establece un mapeo y cierto sincronismo entre ambos, y por ende con los objetivos de control y controles incorporados en el Anexo A de la ISO/IEC 27.001.

2.1.6 Norma ISO/IEC 27.001 y el Ciclo de Deming.

La norma ISO/IEC 27.001 es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Especifica además los requerimientos para la implementación de controles de seguridad para las necesidades de una organización, un sector de la misma, o un proceso, según el alcance del SGSI. Establece entre otras cosas, la documentación exigida para su certificación en el caso del cumplimiento de todos los requisitos.
Sin embargo, si bien sugiere un enfoque para su cumplimiento, no establece una metodología concreta para lograr los productos y esa documentación requerida, ni especifica un flujo de trabajo (*workflow*) con procesos bien definidos.

En [62] se establece un mapeo de las etapas del ciclo de Deming y los productos o entregables exigidos por la norma.

En el Cuadro 2.1, se especifican los principales procesos que indica la referida norma, mapeados con las etapas del ciclo PHVA.

Ciclo PHVA	**Procesos**
Planificar (***P**lan*)	Establecer el contexto. Alcance y Limites Definir Política del SGSI Definir Enfoque de Evaluación de Riesgos Identificación de riesgos Análisis y Evaluación de riesgos Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad
Hacer (***D**o*)	Implementar plan de tratamiento de riesgos Implementar los controles seleccionados Definir las métricas Implementar programas de formación y sensibilización Gestionar la operación del SGSI Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad
Verificar (***C**heck*)	Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y

	del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI
Actuar (***Act***)	Implementar las mejoras identificadas para el SGSI Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.

Cuadro 2.1 – Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 27.001

2.1.7 Norma ISO/IEC 27.005 y el Ciclo de Deming.

La norma ISO/IEC 27.005 [30] es otra norma de la familia o serie ISO/IEC 27.000, y como tal está alineada con la ISO/IEC 27.001. La misma propone también el enfoque del Ciclo de Deming (PHVA) aplicado a la Gestión de Riesgos.

El Cuadro 2.2 resume el mapeo entre el ciclo referido y la Gestión de Riesgos.

Ciclo PHVA *(PDCA)*	**Procesos de gestión de riesgos**
Planificar (***Plan***)	Establecer el contexto Identificación y evaluación de riesgos Plan de tratamiento de riesgos Aceptación de riesgos
Hacer (***Do***)	Implementación de los controles y del Plan de tratamiento de riesgos.
Verificar (***Check***)	Monitoreo y revisión continua de riesgos y del plan. (métricas, análisis, etc.)
Actuar (***Act***)	Mantener y mejorar el proceso de gestión de riesgos

Cuadro 2.2 – Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 27.005

2.2 Antecedentes y trabajos relacionados

Existe un conjunto importante de metodologías y herramientas cuyo objetivo es gestionar la seguridad de la información, en particular, orientadas al Análisis y Gestión de Riesgos [52].

Además de la familia de normas ISO/IEC 27.000 ya mencionadas, a continuación se nombran algunas de estas metodologías y/o métodos que además son objeto de análisis y referencia para el presente trabajo en lo que concierne a la gestión de riesgos:

- CRAMM: "*CCTA Risk Assessment and Management Methodology*" originalmente desarrollado por el gobierno del Reino Unido, dispone de una herramienta que apoya la metodología. Actualmente propiedad de Siemens;
- MAGERIT "*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*" desarrollado por el Ministerio de las Administraciones Públicas de España;
- MEHARI: "*MEthode Harmonisée d'Analyse de Risque*" es una metodología de análisis y gestión de riesgos desarrollada por CLUSIF ("*Club de la Sécurité de l'Information Français*");
- NIST([6]) SP 800-30: es una Guía de Gestión de Riesgos para los Sistemas y Tecnologías de la Información;
- NIST SP 800-39 "*Managing Risk from Information Systems - An Organizational Perspective*" ([7]);
- OCTAVE: "*Operationally Critical Threat, Asset, and Vulnerability Evaluation*" es un conjunto de métodos, herramientas y técnicas del CERT para la planificación estratégica y evaluación de la seguridad de la información;
- IT GRUNDSCHUTZ: " *IT Baseline*", desarrollado por la Oficina Federal de Seguridad de la Información de Alemania.
- ISM3-RA: Es el método de valoración de riesgos propuesto por el modelo de madurez la seguridad de la información ISM3.

Algunas de ellas como CRAMM [65] son antecedentes incluso para la norma BS7799-3 y por ende para la ISO/IEC 27.005 después. [67]
Algunas declaran además de ser compatibles, cumplir los requerimientos de la norma ISO/IEC 27.001 [65], otras como Mehari [48] 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 la misma.

Por otra parte, en [10] se presenta una metodología de "Análisis y Automatización de la Implantación de SGSI en Empresas Uruguayas", las cuales son en su amplia mayoría microempresas y PyMEs como se referencia en el mismo. Dicha metodología está enfocada a "*a cubrir a aquellas organizaciones que generalmente no poseen metodologías, prácticas, ni requerimientos de seguridad específicos o generales*".

[6] *National Institute of Standards and Technology -USA*
[7] segundo draft disponible

En esa línea de investigación, de una metodología de implantación de SGSI para PyMEs, existen diversos trabajos relacionados como [98][99][100][101], donde además se incursiona en un tablero integral de mando para la gestión de la seguridad de la información, métricas e indicadores de madurez para las mismas. El modelo es soportado además por una herramienta de software y ha sido mejorada de forma empírica en función de los resultados obtenidos en el sector.

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 trabajo de tesis, 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.

En [93] se presenta un artículo con una síntesis parcial de este trabajo, donde se delinea el enfoque, estrategia y principales conclusiones de la metodología para grupos empresariales de relación jerárquica. Artículo que constituye una de las ponencias del “V Congreso Iberoamericano de Seguridad Informática (CIBSI’09)” desarrollado en Montevideo, Uruguay, en noviembre de 2009.

3 Propuesta Metodológica

En este capítulo se presenta, por un lado, los desafíos que deberán ser resueltos, motivados en ciertas particularidades de una estructura empresarial como la propuesta. Desafíos y particularidades que no son especificados ni resueltos por la familia de normas ISO/IEC 27.000, pero que deben ser tenidos en cuenta al momento de implantar y gestionar un SGSI y así se afrontan en la metodología que se define.

Posteriormente se presenta concretamente una Metodología con el fin de alinearla con la serie ISO/IEC 27.000, fundamentalmente ISO/IEC 27.001 e ISO/IEC 27.005, con un enfoque sistémico, considerando las necesidades del negocio y la estructura empresarial planteada. La misma se desarrolla según las diferentes fases del ciclo PDCA, haciendo explícita la elección del enfoque y estrategia metodológica ante las alternativas presentadas.

Por otra parte, para la especificación de la misma, alineado con la guía de implementación presentada en ISO/IEC 27.003 ([8]), se definen los principales procesos detallando:
- *Entrada*: lo que se debe tener en cuenta para el mismo
- *Acción*: qué es lo que concretamente debe ser realizado
- *Quienes deberían participar*
- *Salida*: Que es lo que se debe obtener como resultado del mismo.

3.1 Motivación. Particularidades.

En esta sección se analizan aspectos relativos a la estructura empresarial relevantes para la gestión de la seguridad de la información, y se describen las necesidades y principales desafíos que deberían ser resueltos por una metodología con el propósito descrito en este documento.

3.1.1 Aspectos relacionados a la estructura jerárquica empresarial

Como se dijo en secciones anteriores, el objeto de análisis de este trabajo es un grupo multiempresarial de relacionamiento vertical o jerárquico. Relación jerárquica que se propaga o afecta a: las estrategias empresariales, infraestructura compartida, políticas, objetivos, recursos, etc. Esta relación (empresarial) no escapa a la Seguridad de la Información.

La empresa en cuestión - o subordinada -, debe considerar lineamientos básicos a seguir por parte 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 madre / principal.

Se pueden presentar entonces las siguientes problemáticas:

o Los riesgos detectados y las prioridades percibidas en la empresa en cuestión por parte de la empresa principal podrían no coincidir con las prioridades y riesgos detectados por parte de

[8] Under development

la empresa menor. Esto puede ocurrir debido a que la evaluación de prioridades localmente (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, globalmente a veces, no se consideran aspectos específicos o claves para la empresa cuando se baja el nivel de abstracción.

- Al existir infraestructuras compartidas, los servicios que involucran a ambas empresas pueden no estar explícita y globalmente valuados, y por ende las valoraciones de riesgos no estar adecuadamente calibradas o pueden inducir a decisiones locales no alineadas con la conveniencia global.
- Si los presupuestos de ambas empresas son independientes (o autónomos), y también los retornos (de inversión) puede ocurrir que los mismos no se adecuen a políticas que son aplicadas por parte de la empresa madre.
- Existen dependencias interempresariales tanto en la seguridad de los activos como en los riesgos que se afrontan. Esos riesgos que tienen una complejidad adicional, deben ser analizados y tratados en todo su alcance y de forma consistente y coordinada, con el fin de evitar un posible efecto cascada o incluso políticas de seguridad inconsistentes y por lo tanto, con cierto grado de ineficacia e ineficiencia.

Se hace necesario entonces, armonizar o alinear los objetivos y prioridades en lo que a Seguridad de la Información refiere, y por lo tanto a los SGSI de ambas empresas, de forma que por un lado, se atiendan los lineamientos del grupo y en particular los definidos por la empresa principal, sin ser percibidos como simples restricciones que deben cumplirse por mandato, sin un valor agregado. Si la política y SGSI de la empresa mayor no es vinculante (obligatoria) para la empresa menor, debe buscarse variar la relación costo beneficio y el sistema de valoración de activos y riesgos, para alinear percepciones e intereses, y por ende, líneas de acción, ya sea ampliando la visión y alcance del SGSI o buscando incentivar y revalorizando los servicios, activos y riesgos que afecten a ambas empresas o son prestados entre sí.
Por otra parte, se debe lograr la autonomía necesaria, la agilidad y 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.

Puede ser necesario 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, intentando alinear objetivos y prioridades de acuerdo a los intereses del grupo. Esta metodología debe lograr esa cooperación de forma eficaz y eficiente tanto en la búsqueda de recoger las directrices que vienen del SGSI de la empresa jerárquicamente mayor así como también trasladar el *feedback* y las necesidades de la empresa subordinada.

3.1.2 Nuestro posicionamiento frente al marco normativo y estándares.

La familia de estándares ISO/IEC 27.000 relativa a la gestión de la seguridad de la información y la gestión de riesgos, y en particular, la norma ISO/IEC 27.001, si bien define lineamientos genéricos y los requerimientos para un SGSI, no atacan este aspecto de la composición y relación jerárquica de un grupo multiempresarial. Tampoco se pronuncian en forma concreta

sobre algunos aspectos metodológicos que quedan abiertos, como por ejemplo en la elección de un método específico para la gestión de riesgos, sin perjuicio de lo especificado en la norma ISO/IEC 27.005.
La metodología a definir deberá por tanto, aproximar un enfoque más concreto al tema, a los efectos de guiar los procedimientos y actividades con mayor nivel de detalle.

Por otra parte, compartimos el enfoque pragmático y de costo-beneficio enfocado en el negocio que enfatiza ISM3, sin embargo, no compartimos lo que allí se afirma en cuanto a que la norma ISO/IEC 27.001 sea meramente una "*norma basada en controles*". En la propia ISO/IEC 27.001, se especifica literalmente que es una "norma basada en procesos", que se apoya en el ciclo PDCA (ciclo de Deming) para la retroalimentación y mejora del diseño e implementación del SGSI a partir de actividades de monitoreo, revisión, mediciones / métricas y auditorias. La Fase de Planificación, en el ciclo PDCA, concretamente la sección "*4.2.1 Establecimiento del SGSI* ", estipula concretamente la necesidad de definir el alcance y límite del SGSI así como la política del mismo en términos de" *las características del negocio, la organización, su ubicación, sus activos y tecnología*". Definiciones que guiarán las fases posteriores del SGSI y definiciones que deberán ser revisadas en el próximo ciclo de referencia (refinamiento sucesivo) en función de las mediciones, revisiones, auditorias y propuestas de mejora.

3.2 Planificación

En este capítulo, se plantean interrogantes, aspectos de enfoque y de definición de abordaje del tema, así como los lineamientos estratégicos a seguir. Se presentan diferentes alternativas a los efectos de generar la discusión y enriquecer el análisis, discernir y elegir, de forma crítica y con amplitud de criterio, la más adecuada teniendo presentes los *pros* y *contras* de cada una de ellas.

3.2.1 Definición de enfoque

La Gestión de la Seguridad de la Información, como casi cualquier proceso de gestión, tiene tres pilares que deben ser tenidos en cuenta dado que interactúan mutuamente: Personas, Procesos y Tecnología.

Por lo tanto, un SGSI deberá considerar el contexto de la industria y características culturales de la Organización. Deberá además, 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 su vinculación estructural.

Como se ilustra en la Figura 3.1 ([9]), a los efectos de establecer un SGSI, debe tenerse en cuenta: la estrategia de la empresa, principios y estándares de gestión, los recursos necesarios para todas sus fases del ciclo PDCA, en particular las personas involucradas (RR.HH.): tanto técnicos, gerentes y todo el personal alcanzado de una u otra forma por el SGSI.

[9] Adaptación propia de la imagen tomada de [78].

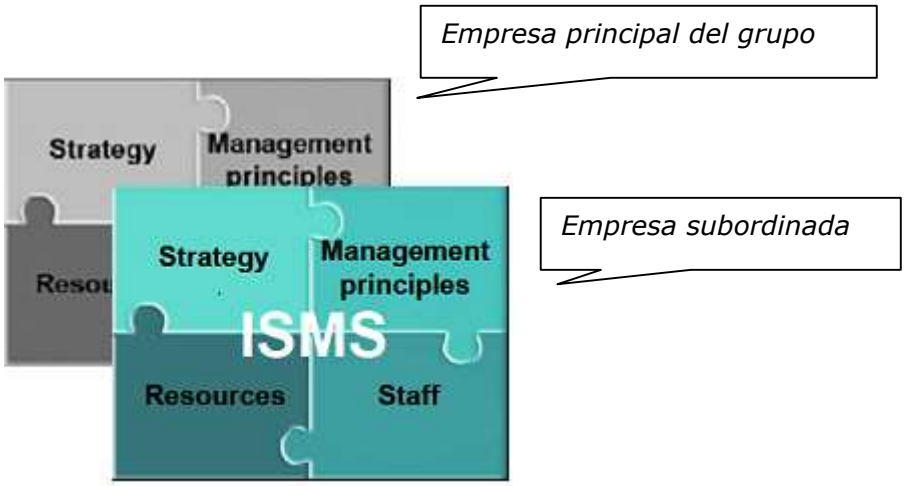


Figura 3.1 – Componentes de un SGSI (*ISMS*) [78] en un grupo empresarial (9)

En el caso de una empresa perteneciente a un grupo empresarial, objeto de este trabajo, y con las características generales de la metodología que se busca definir, se hace necesario coordinar y armonizar todos estos componentes para lograr efectividad en los objetivos de Seguridad, pero también eficiencia, haciendo un uso racional y conveniente de los recursos, de forma de adecuarse a la estrategia local - de la empresa en cuestión - y a su vez los lineamientos estratégicos corporativos, eventualmente compartiendo recursos y principios de gestión.

Elegimos por lo tanto un enfoque doblemente sistémico [77], por un lado en cuanto a las dimensiones o disciplinas que deben participar en la definición del SGSI, no sólo tecnológicos, en particular se pone énfasis en la necesidad de adecuación al negocio y la estrategia de la empresa, y por otro lado, debe tener consistencia global con las definiciones y políticas corporativas.

Será necesario para cada una de las fases del SGSI, planificar y gestionar los recursos disponibles bajo las mejores prácticas y principios de gestión, adecuándose a la idiosincrasia y políticas generales del grupo empresarial. Ello implica estimar, asignar, autorizar, administrar y racionalizar dichos recursos de un modo conveniente a los intereses y necesidades de la empresa respecto de la seguridad de la información.

Aquí pueden darse las siguientes alternativas que identificamos y definimos a continuación:

- ***Enfoque centralizado***: donde exista un único SGSI y la Seguridad de la Información sea gestionada en forma central a nivel más alto del grupo empresarial.
- ***Enfoque distribuido***: donde cada empresa tenga su propio SGSI y sean independientes.
- ***Enfoque mixto***: donde existan dos SGSI pero relacionados e integrados entre sí, respetándose la naturaleza jerárquica estructural (entre ambas empresas del grupo) pero también la autonomía operativa de cada una de ellas.

3.2.1.1 ¿ Enfoque Centralizado, Distribuido o Mixto ?

Un enfoque centralizado, si bien es más simple en su definición, se hace impracticable o al menos muy difícil 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 de la Información.

Para la estructura empresarial objeto de este trabajo, optaremos por 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 estrategias de forma global, pero con la flexibilidad de afrontar las definiciones e implementaciones de forma más local y acotada. De esta forma, se hace más manejable, se logra mayor flexibilidad y capacidad de gestión de la seguridad de la información, pudiendo atender las especificidades de sus ámbitos de aplicación, en términos del negocio, las tecnologías involucradas y los conocimientos requeridos.
Esta elección se basa fundamentalmente en la búsqueda de las ventajas correspondientes de ambos enfoques descritos en los párrafos anteriores, y a la propia naturaleza estructural del grupo.

3.2.2 Estrategia metodológica

Motivados en estas necesidades específicas, que responden a las particularidades de la estructura empresarial descrita, es necesario definir y especificar cómo afecta esta relación a la gestión de la seguridad de la información entre ambas empresas del grupo.

3.2.2.1 ¿ Cómo Gestionarlo ?

'Think big, Start small' + Enfoque Sistémico.

Una vez definido el enfoque, resta la tarea de definir una metodología para que esto que pretende tomar 'lo mejor de dos mundos' (jerárquico y distribuido) no se transforme en un perverso sistema que atente contra su propia intención integradora, volviéndose algo complejo que lejos de obtener las ventajas de un enfoque combinado, no obtenga las ventajas de ninguno de ellos e introduzca complejidad de forma no efectiva.

En otras palabras, el enfoque sistémico, y la visión global no implican que deba ser burocrático ni rígido. Sí deben estar bien definidas las responsabilidades, competencias y alcance de cada uno de los actores, áreas y empresas intervinientes.

Se requiere entonces, una metodología clara, que permita integrar la gestión de la seguridad de la información del grupo empresarial, eliminando o minimizando las ambigüedades así como la redundancia y la inconsistencia en las decisiones.
El objetivo es lograr un esquema eficaz y eficiente, en el sentido de la gestión de prioridades empresariales, riesgos a afrontar en cuanto a la seguridad de la información, y los recursos necesarios para lograrlo.

Deben evitarse complejas relaciones o innecesarias dependencias e interacciones entre ambas empresas del grupo, pero a su vez atender lo inherente a la estructura empresarial. En inglés hay un dicho que aplica bastante bien al criterio que debería primar: '*Think big, Start small*'. Es decir, ser ambicioso y atender la globalidad en la visión a los efectos de definir los lineamientos, pero permitir una implementación e implantación gradual. Haciendo extensivo el concepto, en esa línea, y llevándolo al plano de la Seguridad de la Información, la estrategia debe respetar la estructura y naturaleza empresarial del grupo y permitir la autonomía necesaria para su eficaz y eficiente implantación.

A tener en cuenta al momento de plantearse diseñar, implantar y adoptar un SGSI:

La Organización debe tener claro, qué tan importante es la Seguridad de la Información para su negocio (objetivos, prioridades y estrategia de negocios), considerando aspectos como: la calidad de servicio esperada y exigida por sus clientes, objetivos y recursos financieros, y aspectos legales, regulatorios y/o contractuales.

La Dirección y la Alta Gerencia debe mostrar su compromiso y aplicar su experiencia en la consecución de objetivos, gestión de prioridades, toma de decisiones, cumplimiento de cronogramas, etc. Este compromiso supone, liderar las actividades requeridas por la Alta Gerencia, aportar los recursos necesarios, y bregar por la concienciación y capacitación del personal, además de actividades de monitoreo y contralor.

Los procedimientos necesarios y requeridos por el SGSI deben ser integrados y embebidos en los procesos operativos de la empresa. Deben integrarse de la forma más natural y consistente posible a los efectos que no esté condenada a caer en desuso o los controles etiquetados de burocráticos. De lo contrario, será percibida como una imposición, una regulación sin un aporte que agregue valor al negocio y por lo tanto se corre el peligro que sea tratado como normas burocráticas ajenas al sector o al negocio concreto. La consecuencia de eso: ineficiencia operativa, ineficacia del SGSI y por lo tanto recursos mal utilizados.

Como se muestra en la Figura 3.2, la trilogía de: Confidencialidad, Integridad y Disponibilidad, principales atributos de seguridad de la información de cualquier sistema de seguridad de la información y/o método de gestión de riesgos [52] – y pilar de la propia norma ISO/IEC 27.001, debe enmarcarse entonces en el contexto del negocio, del marco legal y la estrategia empresarial.

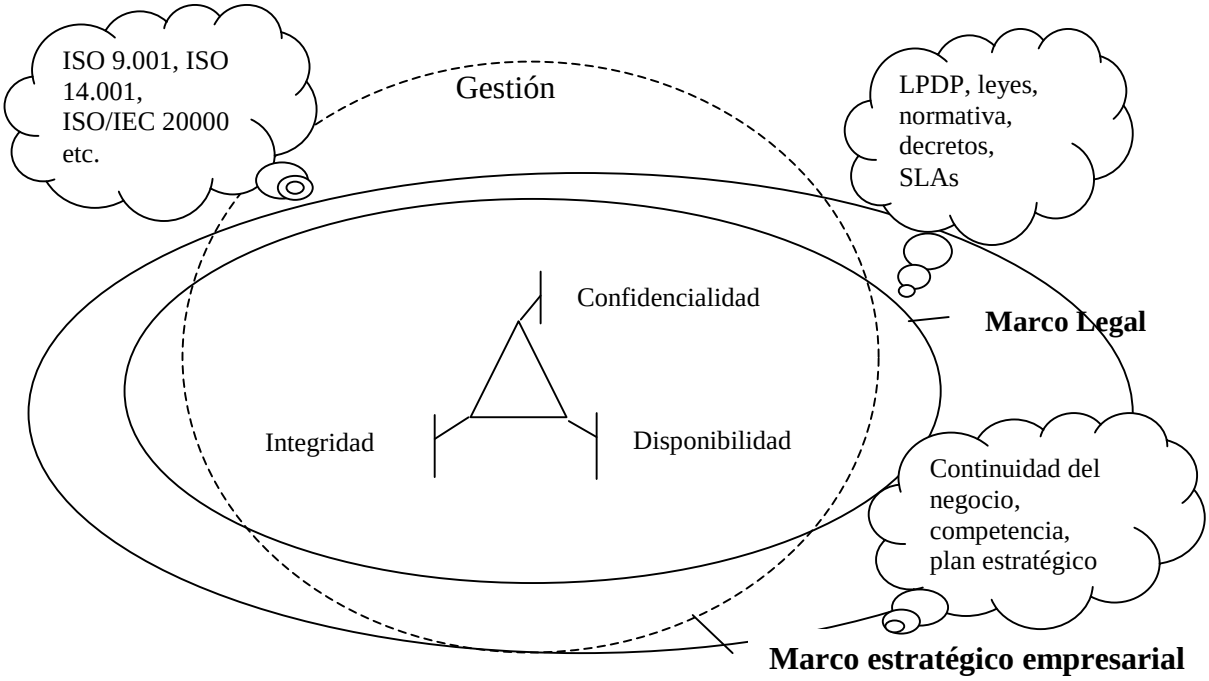


Figura 3.2 – Contexto de gestión de un SGSI

3.2.2.2 Claves de éxito

En general, para implantar y gestionar un SGSI de forma exitosa, es fundamental:

- Elegir criterios y herramientas adecuadas para la evaluación y tratamiento efectivo de riesgos. Adecuadas implica por ejemplo considerar la cultura organizacional, la costumbre con el uso de una metodología, y las prioridades estratégicas de la Organización. Es decir, la receptividad de una metodología como la que se persigue, en una empresa / organización que ya utilice alguna metodología para otros propósitos, o esté familiarizada por ejemplo con normas de calidad y procesos de gestión, puede ser mayor que en una que no posea metodologías formales. Esto puede condicionar el alcance y objetivos de la misma en cuanto a su ambición y evolución gradual.
- No hacer de la Seguridad de la Información un fin en sí mismo, buscando un ideal de seguridad que se aparte de los requerimientos del negocio o se concentre únicamente en posibilidades tecnológicas.
- La estrategia de seguridad, está relacionada con los planes estratégicos de negocios y planes operativos, y por supuesto con la misión y visión de la empresa. Los estándares y prácticas de seguridad deben contribuir en esa dirección y estar alineados tanto con los objetivos concretos de corto y mediano plazo como con el largo plazo.
- El éxito pasa también por hacer el compromiso sustentable y no sólo en el envión inicial en la fase de implantación. Es fundamental continuar en la fase de gestión, operación y monitoreo, a los efectos del mantenimiento y mejora del SGSI.
- Cuando se detecten apartamientos de lo especificado en el SGSI, o en su defecto, carencias de la definición del mismo para responder a las necesidades operativas o estratégicas del

negocio, es importante no hacer un tratamiento *ad hoc* ni dejar fuera del SGSI aspectos o procedimientos sino incorporarlos para corregir este apartamiento o salvar esta carencia de acuerdo a las necesidades y objetivos del negocio.

Con una estructura empresarial jerárquica, como la de nuestro caso de estudio se agrega:

- Visión global y sistémica pero con la autonomía y flexibilidad requerida para no perder la especificidad de cada empresa.
- Alinear las visiones globalmente, en un alto nivel y de largo plazo, de las empresas del grupo de acuerdo a sus planes de negocios y estrategias empresariales.
- Los SGSI de ambas empresas deberán cooperar y no competir.
- Especificar explícitamente y con claridad, el alcance y la relación jerárquica de ambos SGSI.
- La relación de ambos no puede ser demasiado compleja, pero a su vez debe no tener ambigüedades, deben ser consistentes.
- La metodología debe especificar de forma concreta, las actividades a realizar en cada etapa, sus entradas y resultados esperados, promoviendo la capacidad de reutilización de conocimiento entre las diferentes empresas del grupo, con el objetivo de optimizar recursos y beneficiarse de la sinergia sistémica entre las mismas, así como al grupo en su globalidad.
- La naturaleza de este tipo de empresas, eventualmente grandes corporaciones, hace que en general ya tengan implantados otros estándares de gestión, como por ejemplo, gestión de calidad (ISO 9001), o Cobit. El SGSI a implantar deberá tener en cuenta a los mismos para integrarse con ellos de forma conveniente, complementándose y retroalimentándose, no compitiendo ni generando conflictos de visiones o intereses.
- Es fundamental que las empresas del grupo compartan una cultura de seguridad de la información, que sentará los pilares y principios básicos sobre el que operará y contribuirá a su fortalecimiento el SGSI. Para ello es necesario dotar al mismo de un organigrama conveniente para gestionar la seguridad de la información, que atienda la naturaleza estructural del grupo, las necesidades de concientización y formación / capacitación.
- Además de los principios básicos de la seguridad de la información y por ende de un SGSI en general, y de los conceptos vertidos en la sección “3.2.2.1 ¿ Cómo gestionarlo ?”, deben atenderse aspectos concretos como se verá en la sección “3.2.2.4 El Desafío: Adecuación a la estructura y estrategia empresarial” y definir de forma conveniente aspectos estratégicos como se plantea en “ 3.2.2.5 ¿ Estrategia de implementación vertical o cooperativa e integrada ?”, entre otros.

3.2.2.3 Principios de la seguridad de la información

Se describen a continuación, algunos principios de seguridad de la información que aplican a este trabajo y al enfoque con el cual es realizado, agrupando algunos lineamientos básicos que si bien son conocidos, consideramos que deberían guiar una metodología para un SGSI.

La Seguridad es un proceso continuo, y como tal, se requiere de un sistema que lo soporte, que requiere además de su definición e implementación, ser mantenido y mejorado acorde a la evolución de las necesidades.
Involucra factores humanos, tecnológicos y procedimentales o de relacionamiento de los anteriores. Por ello, no es suficiente un enfoque meramente técnico, ni exclusivamente humano

o conductual. No bastan decisiones políticas ni reglas estrictas por sí solas, como tampoco es resuelto por la tecnología. Tampoco es suficiente atacar estos aspectos en forma disasociada o disjunta, sino que se requiere de una visión holística, integradora.

Debido al carácter dinámico y necesidad de revisión y mejora continua, se requiere de un enfoque metodológico, de apego a los estándares y a las mejores prácticas de la industria.
El uso de las mejores prácticas de la industria y estándares internacionales, así como las comparaciones con colegas / expertos contribuyen a alcanzar un estado de mayor madurez de la seguridad de la información y a su vez reafirma la insuficiencia en la búsqueda de la seguridad basándose únicamente en el carácter secreto de los procedimientos o los protocolos, ni reinventar estrategias *ad hoc* cuando hay estándares disponibles, convenientes y adecuados.

La Seguridad de la información, es un aspecto más del negocio, de carácter estratégico y como se dijo, no es un fin en sí mismo. Por lo tanto, debe primar un criterio de optimización de la relación Costo / Beneficio: minimizar los riesgos, maximizando el logro de los objetivos sin salirse de los parámetros de niveles de inversión (presupuesto) de acuerdo a las prioridades establecidas por la Organización / Empresa.

La eficiencia operativa, a veces requiere de soluciones más complejas en su diseño o fase de planificación y coordinación, así como una metodología más elaborada para una empresa en una relación jerárquica. Esto también es válido para la seguridad de la información.

Debe procurarse, en lo posible, la defensa en profundidad y seguridad por capas (múltiples líneas de defensa), como mecanismo de hacer más robusto el sistema de defensa (o de gestión de la información) y no ser vulnerable en un punto único de falla.

3.2.2.4 El Desafío: Adecuación a la estructura y estrategia empresarial

Una estrategia de Seguridad de la Información o un SGSI, de cualquier empresa u Organización, debe considerar la posibilidad de establecer referencias (cruzadas) entre los planes estratégicos, operativos y de seguridad. De lo contrario se corre el riesgo que los mismos no estén alineados y no proveer soluciones para los problemas y necesidades reales del negocio. Debe lograrse un balance a los efectos de no establecer controles más restrictivos o incurrir en costos mayores de los que amerita, ni asumir riesgos no convenientes ya sea por omisión o negligencia.

Debido además, a la estructura empresarial descrita, si bien ambas empresas son en cierta medida autónomas, existe una jerarquía tanto en sus políticas estratégicas como de la política de seguridad en particular que debe respetarse.
También cobra mayor importancia la necesidad de compatibilizar visiones multidisciplinarias y gestionar diferentes niveles de abstracción que, si bien son necesarios en todo SGSI, en un grupo empresarial o en una infraestructura compleja con múltiples tecnologías y dependencias interempresariales, se ve potenciado. Será necesario para comunicarse adecuadamente entre los modelos de negocios de ambas empresas, los servicios (internos y entre ambas), y la implementación técnica de estos servicios y procesos de negocios. Esta comunicación, que tiene su impacto en la seguridad de la información, debe modelarse adecuadamente, tanto interiormente en cada empresa, como en la relación entre ellas.

El desafío es, por lo tanto, lograr la definición de un SGSI que sea operativo y funcionalmente sustentable y sostenible a largo plazo, acorde con la misión, estrategia, objetivos y prioridades del negocio, así como con las políticas establecidas por la empresa principal del grupo, que comprenden en su alcance también a la empresa foco de este análisis (subordinada).
Decimos *sustentable* porque debe de poder argumentarse con razones convincentes el porqué y la conveniencia de los controles aplicables y los riesgos asumidos. Y decimos *sostenible* porque debe poder ser viable desde el punto de vista de los recursos necesarios y mantenido en el largo plazo.

En la Figura 3.3 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, promovidos por su misión y visión, respetando el marco legal vigente.
Por otro lado: en el plano horizontal, aunque reflejando la jerarquía propia de la vinculación entre las empresas, se refleja esta necesidad de armonizar y alinear las políticas corporativas, 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 mayor o principal.
Observar que se da una relación propia de subordinación a los lineamientos y políticas corporativas del grupo empresarial. Adicionalmente pueden identificarse también relaciones de confianza con otras empresas del grupo empresarial o eventualmente asociadas.

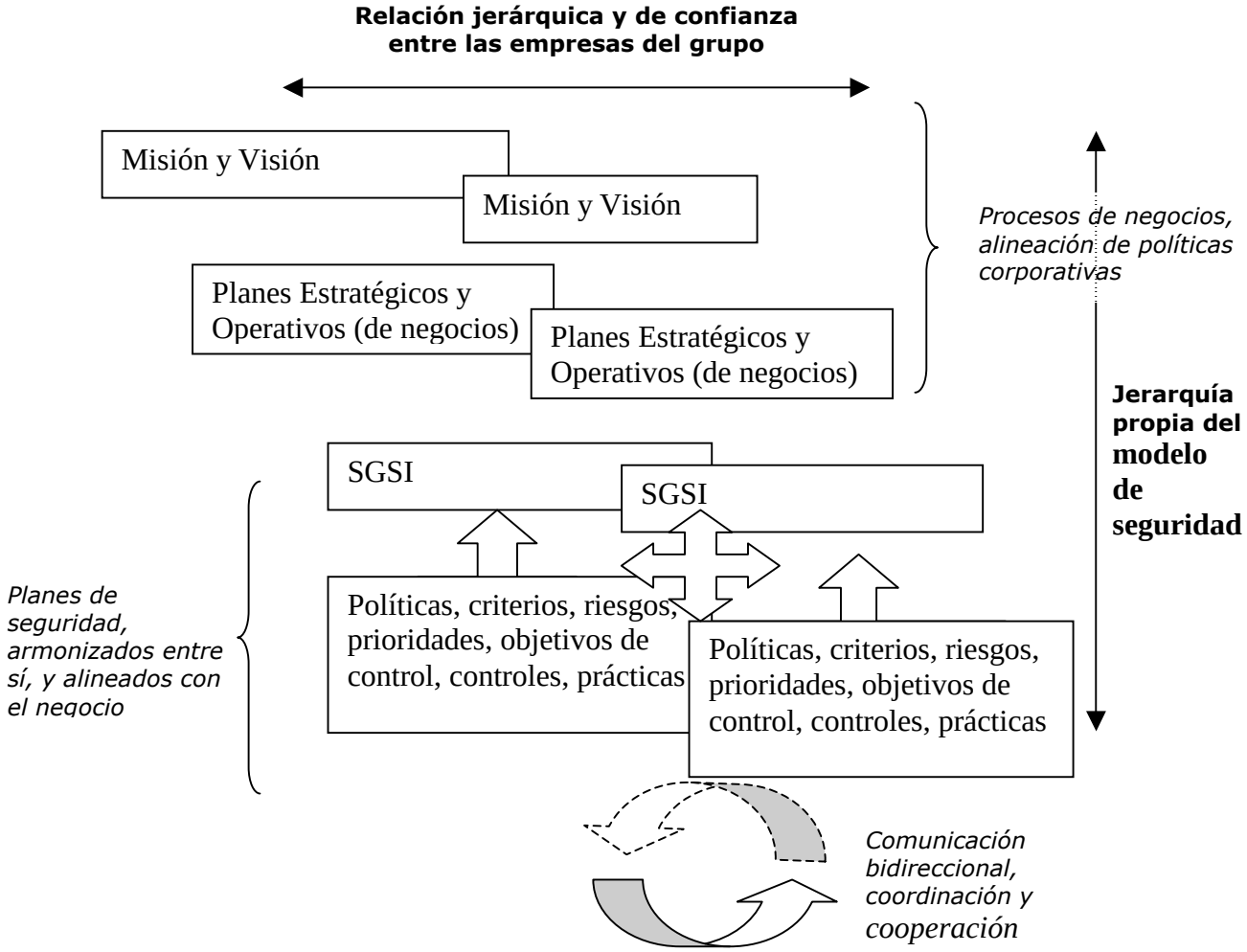


Figura 3.3 – Posicionamiento jerárquico relativo del SGSI en un grupo empresarial

3.2.2.5 ¿ Estrategia de implementación vertical o cooperativa e integrada ?

Cabe preguntarse si el rol que van a tener los responsables de Seguridad de una y otra empresa serán de control, en el sentido que estén cubiertos los lineamientos de seguridad globales o de la empresa principal del grupo, y que este control se haga de forma posterior, o si por el contrario, la gestión de la seguridad ya estará integrada en sus procedimientos y constitución de los grupos de trabajo por personas / profesionales de ambas empresas.
En este punto, la definición depende mucho de la estructura empresarial, considerando aspectos políticos, de dirección, constitutivos, así como la alineación de sus estrategias empresariales.

Deberá definirse por ejemplo, cómo se analizarán los riesgos, cómo se establecerán las prioridades cuando estos riesgos involucren activos que son comunes o afectan la seguridad de ambas empresas, eventualmente con percepciones de riesgos diferentes. Cómo pesarán y se

salvarán esas diferencias y con qué enfoque se gestionarán dichos riesgos. A qué nivel y sobre quién caerá la responsabilidad de definición de los controles, etc.

Deben identificarse todas las partes involucradas y asignarse los roles y responsabilidades. Cómo participa la empresa principal del grupo en las definiciones y políticas de la empresa subordinada. Debe estar claro si tiene un rol de contralor de las políticas globales del grupo, si tiene participación directa en las políticas de la empresa subordinada, o si sólo hace recomendaciones de carácter no vinculante u obligatorio.
A su vez, la empresa en cuestión – subordinada - tendrá su propia percepción y evaluación de riesgos, que muchas veces deberá elevar a la empresa madre del grupo.

Debe definirse formalmente el escalamiento para la toma de decisiones sobre Seguridad de la Información.
Deben especificarse los registros de las decisiones y mediciones necesarias.

Los recursos necesarios para esto, están previstos como uno de los componentes de la norma 27.001 para el SGSI.
Debe contar con aprobación Gerencial y de la Dirección, y debe mantenerse y mejorarse continuamente.

3.2.3 Síntesis de requerimientos para la metodología

Como surge de todo lo expuesto, una metodología para el propósito que se considera, como objetivo de este documento, debe considerar:

- Aspectos legales, contractuales y de regulación propios del sector industrial.
- Su alineación con la estrategia y aspectos propios del negocio (específicos) en un ámbito competitivo (Plan de negocios, metas, prioridades, etc.).
- Alineación y cumplimiento de las políticas corporativas.
- Promueva la consistencia corporativa y a su vez tenga capacidad de adaptación y adecuación a cada una de las empresas del grupo.
- Involucramiento y apoyo de la Dirección.
- El alcance del SGSI, a los efectos que la metodología sea aplicable y efectiva para una empresa de este tipo, con una infraestructura importante en cuanto a cantidad de activos de información y tecnología.
- Cumpla con el estándar ISO/IEC 27.001 para una eventual certificación.
- Se integre con otras metodologías y estándares de gestión y calidad.
- Adecuada y conveniente relación costo / beneficio.
- Permitir una adecuada gestión de la propia documentación del SGSI, en cuanto a su mantenibilidad y actualización para permanecer alineado y al día con los cambios en cualquiera de los componentes de: tecnología, recursos humanos y procedimientos de acuerdo a los requerimientos de los atributos de seguridad de la información para el negocio.

Afirmamos que dada la envergadura de un grupo empresarial como el considerado - objeto de este trabajo - a los efectos de lograr que la metodología sea aplicable y efectiva, y mantenga una relación conveniente costo / beneficio en cuanto a su eficiencia operativa y los niveles de

seguridad de la información requeridos, es fundamental concentrarse en los procesos críticos del negocio, los de mayor valor agregado y estratégicos para su continuidad, y dar soporte a los procesos que sustentan el desarrollo competitivo y exitoso de la empresa.

3.2.4 Síntesis gráfica de la metodología

En esta sección se presenta y se desarrolla en forma concreta, la metodología propuesta, bajo el enfoque y estrategia definidos en las secciones anteriores.

En la Figura 3.4 se ilustra la interacción y cooperación propuesta entre ambas empresas a los efectos de alinear el SGSI de la empresa en cuestión y la empresa principal del grupo.

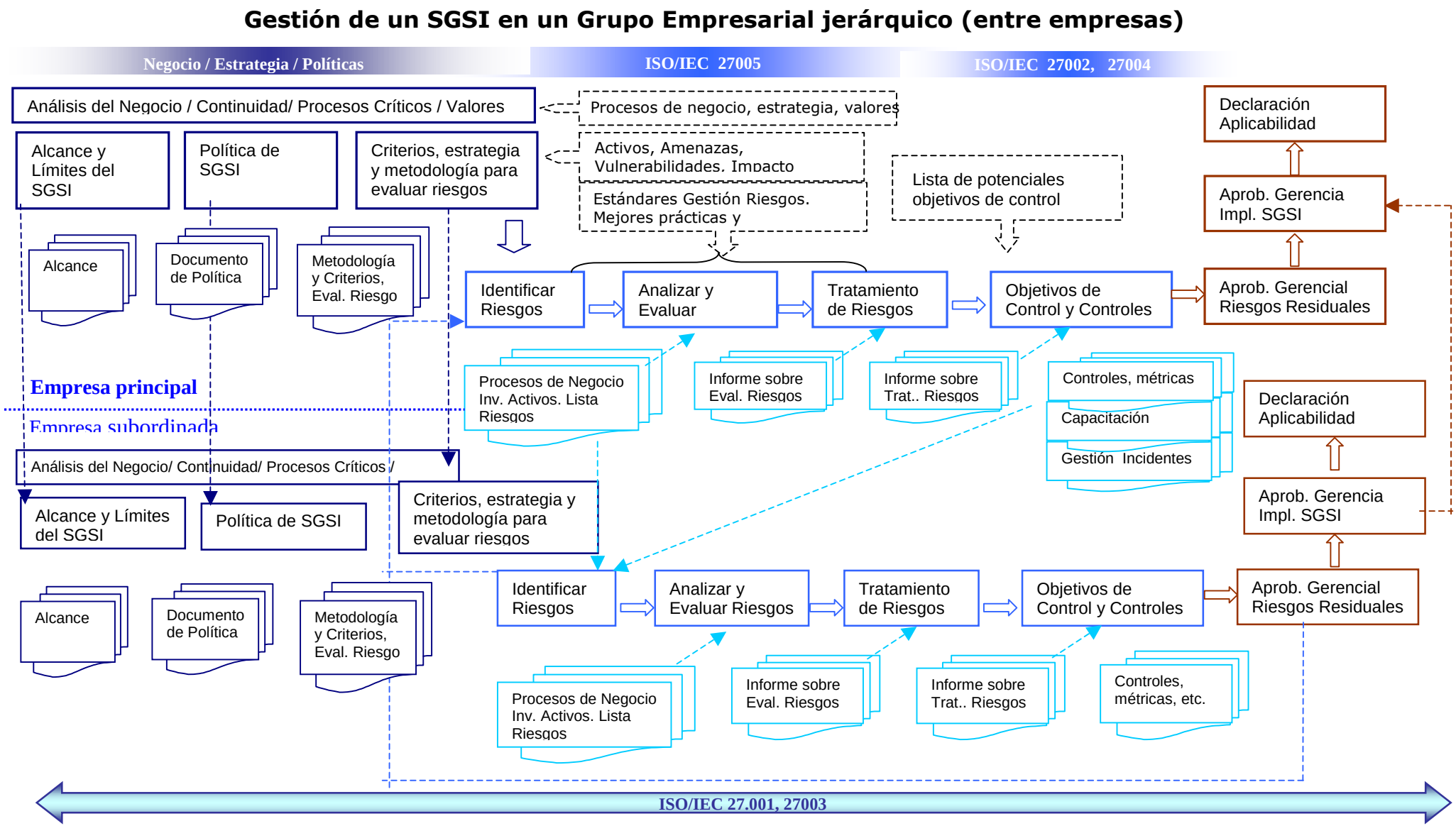


Figura 3.4 – Propuesta Metodológica

De lo ilustrado en el diagrama, vemos sintéticamente como se definirá la estrategia para alinear ambos SGSIs del grupo empresarial, que luego se describirá con mayor detalle en las secciones siguientes.
El objetivo es armonizar el SGSI de la empresa subordinada con el de la empresa principal del grupo empresarial, o más precisamente, con el SGSI del grupo empresarial en su globalidad.

El Alcance y Límites de la empresa principal, en general va a alcanzar a la empresa en cuestión (subordinada). 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.

La Política del SGSI de la empresa en cuestión o subordinada, deberá corresponderse o ser consistente con la Política del SGSI de la empresa principal o corporativa 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 qué autonomía y bajo qué lineamientos se relacionarán ambas empresas. Esto no escapa a a la seguridad de la información dado que tiene carácter institucional.

En cuanto a la estrategia, metodología y herramientas de evaluación de riesgos, si bien teóricamente las de ambas empresas pueden ser independientes si se establecen parámetros de correspondencia o fórmulas de conversión de uno a otro, a los efectos de favorecer la interoperabilidad y cooperación entre ambas, y por practicidad es conveniente que ambas empresas del grupo compartan la estrategia, criterios, metodologías y eventualmente herramientas de análisis y gestión de riesgos.
Así por ejemplo la calificación de activos y procesos realizada por la empresa principal del grupo en lo referente a los activos y procesos de la empresa subordinada pueden ser heredados para la clasificación por parte de esta última. No obstante, la empresa subordinada podrá ponderar cuánto pesa esa calificación heredada en sus propias valoraciones de riesgos.

Los riesgos percibidos por la empresa principal del grupo que afecten a activos y/o procesos que se encuentren dentro del alcance del SGSI de la empresa subordinada, serán considerados como insumo o dato de entrada para la identificación y valoración de riesgos. Como probablemente estos riesgos quizás fueron parcialmente tratados en los controles de la empresa principal, estamos en realidad haciendo referencia al riesgo residual, que podrá ser aceptable o no por la empresa subordinada y que podrá o no requerir de otros controles más específicos o con mayor efectividad.

De forma análoga, pero en sentido inverso, los riesgos residuales resultantes de la gestión de riesgos de la empresa subordinada, y una vez aprobados por la gerencia como riesgos aceptables, serán informados a la empresa principal a los efectos de tomar conocimiento e incorporarlo en su propia identificación y evaluación de riesgos.

Eventualmente pueden detectarse aquí riesgos que afectan a la empresa principal o al grupo empresarial como tal y que no habían sido previamente percibidos en su propia identificación de riesgos o eventualmente no fueron estimados en su real dimensión.

Una vez aprobado el SGSI por la Dirección y Gerencia de la empresa subordinada, será sometido en los lineamientos macro, como por ejemplo la Política del SGSI para la aprobación de la empresa principal y Dirección del grupo empresarial. La empresa principal intervendrá además, en etapas posteriores: en actividades de supervisión y/o auditoría, y en el tratamiento de riesgos compartidos o con dependencias interempresariales, con especial énfasis en los activos de información y procesos que impactan su propia operativa o aspectos estratégicos del grupo.

En los capítulos siguientes se profundizará en cada una de estas actividades que constituyen la metodología.

3.2.5 Organización, estructura y relacionamiento

Debe establecerse qué roles serán necesarios y cómo se vincularán entre sí en cada una de las etapas del SGSI, a lo largo del ciclo PHVA.

Como se establece en Magerit [3], deben especificarse los roles y las funciones necesarias para la metodología propuesta, que 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.

3.2.5.1 Quienes deben participar en la definición del SGSI. Organización

En ISM3 [66] 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, coordinación y aprobación de 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.

Creemos que 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.

En *IT Grundschutz* [78], 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, además, 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 (‘*IT Coordination Commitee’*), y un equipo responsable de gerenciar la seguridad de IT (‘*IT Security Management team’*).
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).
El Comité de Coordinación de IT, no es un comité permanente sino que puede ser convocado a demanda para definir decisiones generales en cuanto a la seguridad o responsabilidades y asignación de roles de seguridad por ejemplo.

Por otra parte, la norma ISO/IEC (FDIS) 27.003 – alineada también con la ISO/IEC 27.005 -, presenta las necesidades con respecto a la organización, roles requeridos y presenta también un ejemplo posible para una empresa.

Teniendo presente, estas recomendaciones, atendiendo a la estructura empresarial que se analiza y a las necesidades de coordinación expuestas hasta el momento entre las empresas, proponemos una estructura como la que se ilustra en la Figura 3.5.

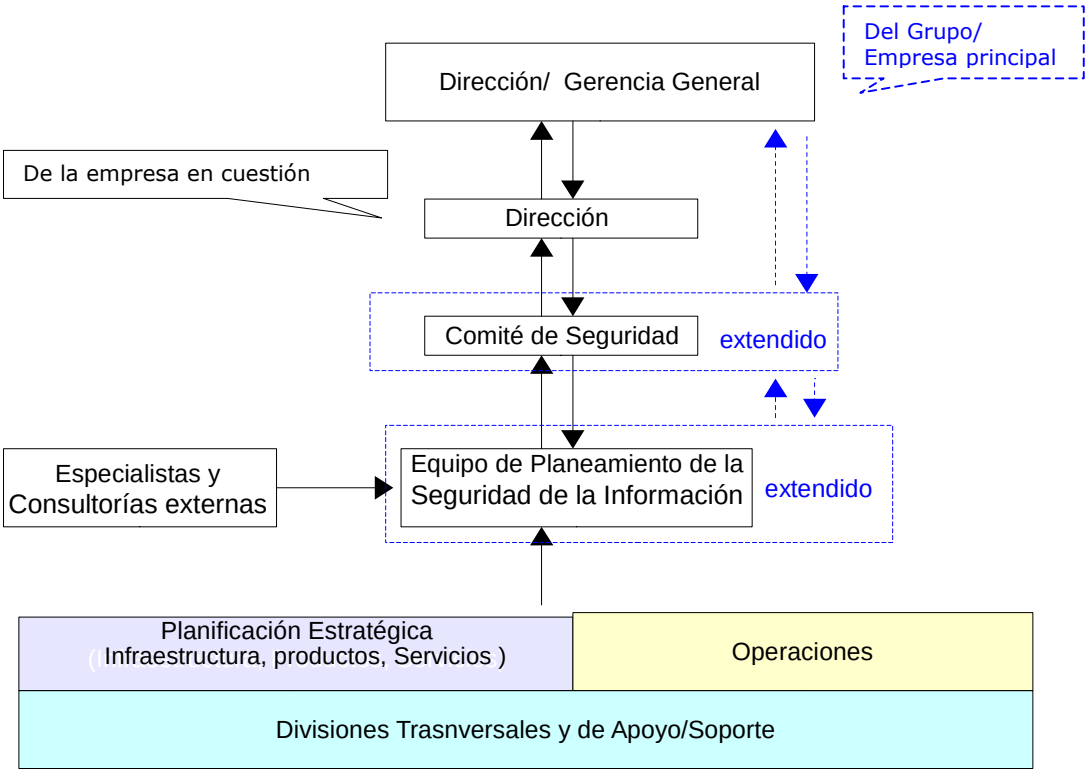


Figura 3.5 – Estructura de relacionamiento propuesta para el SGSI

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 con otras responsabilidades o áreas, ni comprometer estas decisiones de diferentes roles sobre la misma persona. Dependiendo de la empresa y su dimensión, éste será el Oficial de Seguridad, o la Gerencia de Seguridad en caso de existir para la empresa subordinada, que dependerá directamente de la Dirección de la misma para preservar independencia y apoyo directo de las máximas autoridades de la empresa.
Asimismo sería importante guardar una vinculación estrecha con la Gerencia de Seguridad de la empresa principal, en lo que refiere a la decantación de las propias políticas aplicables a la empresa subordinada y a la armonización entre ambos SGSI.

Se describen a continuación, los diferentes roles presentados en la Figura 3.5:

- Dirección y Gerencia General: La Dirección y Gerencia debe 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. En una primera instancia la Dirección y Gerencia de la empresa en cuestión (subordinada), y según el grado de dependencia de la estructura empresarial y sus políticas institucionales en general, podrá requerir de la aprobación o visto bueno de la empresa principal del grupo también.

- Comité de Seguridad (de la Información):
  Lleva un rol de liderazgo del SGSI, en sus lineamientos directrices y debe tener un rol ejecutivo para asegurarse que se cumplan las actividades y etapas requeridas.
  Planifica y gestiona los recursos y el 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 las diferentes Gerencias de línea y áreas de negocio, como por responsables máximos de la Seguridad de la Información de la empresa principal del grupo (por ejemplo, la Gerencia de Seguridad de la Información en caso de existir) y eventualmente de la Gerencia General si fuera necesario. 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 vez al año.

- Equipo de Planeamiento de la Seguridad de la Información: Especialistas 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 comprendidos 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 (mínimo) 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, pero que mantiene sobre sí, la responsabilidad de la seguridad de la información.

- Asesoramiento y Vínculos externos (Industria y Universidad): 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.

3.2.6 Análisis del Negocio

En la etapa de planificación de un SGSI o si se quiere, en una etapa previa, se hace necesario especificar y documentar claramente los aspectos relevantes del negocio para el cual se diseñará e implantará el mismo, lo que fijará los lineamientos y criterios de decisión que deberán tomarse en lo que respecta a la seguridad de la información.

En la actualidad, en cualquier sector de la industria, encontramos que los sistemas de información e informáticos de gestión son fundamentales como soporte a la actividad empresarial - cuando no son parte de la actividad sustantiva o el principal servicio -. Como se ilustra en la Figura 3.6, estos sistemas son diseñados e implementados a los efectos de servir a los procesos de negocio que a su vez responden a los planes operativos, alineados con los planes estratégicos de la empresa. Planes estratégicos que a su vez responden a las propias bases y finalidad de la empresa en función de su misión y visión.

En nuestro caso, debemos agregar además un nivel de lineamientos estratégicos y políticas corporativas, que serán generales a las empresas del grupo y serán por lo tanto heredadas más allá de tener las políticas y estrategias propias – las empresas subordinadas – que respeten este marco estratégico de políticas generales.

Este enfoque sistémico [77] u holístico como se lo denomina en [74] es fundamental para determinar criterios de prioridad y niveles de seguridad requeridos para los activos de información y hacer un uso racional de los recursos. El objetivo de un SGSI no debe ser lograr la mayor seguridad posible de acuerdo a las tecnologías y controles posibles, sino a la más adecuada y alineada con las necesidades del negocio y los planes empresariales.
Es con este enfoque que alinearemos la metodología propuesta en el resto de este trabajo.

Como podemos observar también en la Figura 3.6, existen relaciones múltiples N a N entre procesos de negocios y los sistemas de información, y entre los propios sistemas de información. También los hay obviamente entre los propios procesos de negocios. Estas relaciones deberán ser tenidas en cuenta en la metodología a los efectos de lograr efectivamente la seguridad requerida con una visión global.

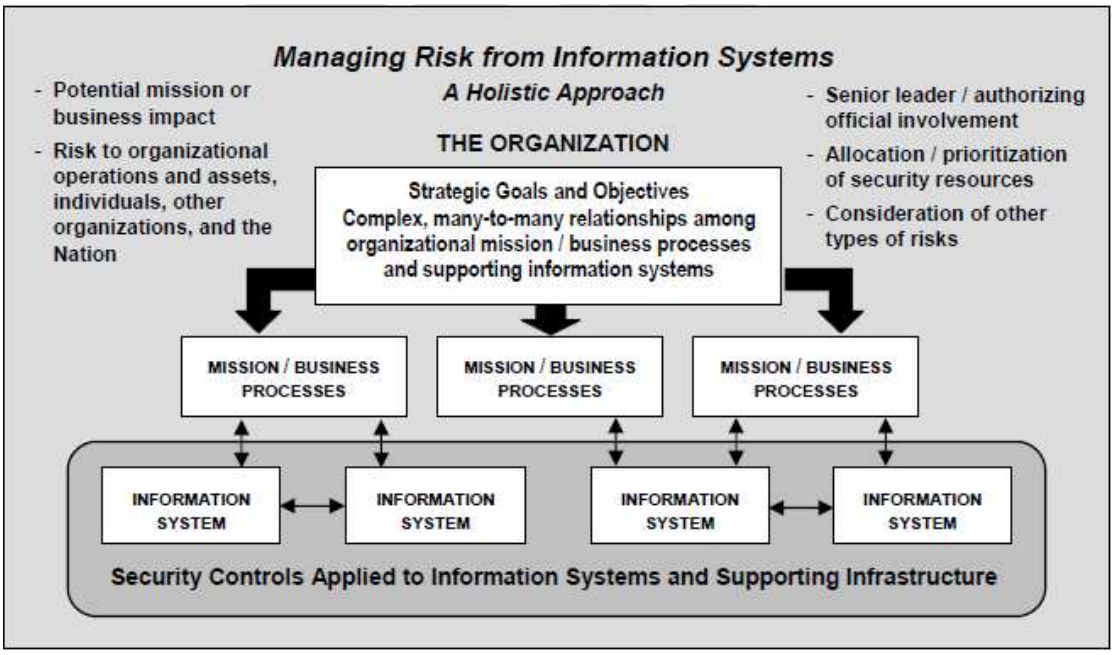


Figura 3.6 – Visión organizacional de la seguridad de la información [74]

Como se observa en la Figura 3.6 las dependencias se dan entre las diferentes capas de abstracción: es decir, entre los procesos de negocios y los sistemas de información que los soportan; pero también se dan en forma horizontal dentro de cada capa o nivel..

Por otra parte, este enfoque también está alineado con el ISM3 en el sentido que son los procedimientos del negocio y la estrategia empresarial los que guían el plan de seguridad de la información.
En la Figura 3.7, se establece cómo inciden los requerimientos del negocio en el alcance y los objetivos de seguridad, en conjunto con requerimientos legales y contractuales, limitaciones y necesidades técnicas, aspectos ambientales y de ciclo de vida de los sistemas y restricciones presupuestarias.

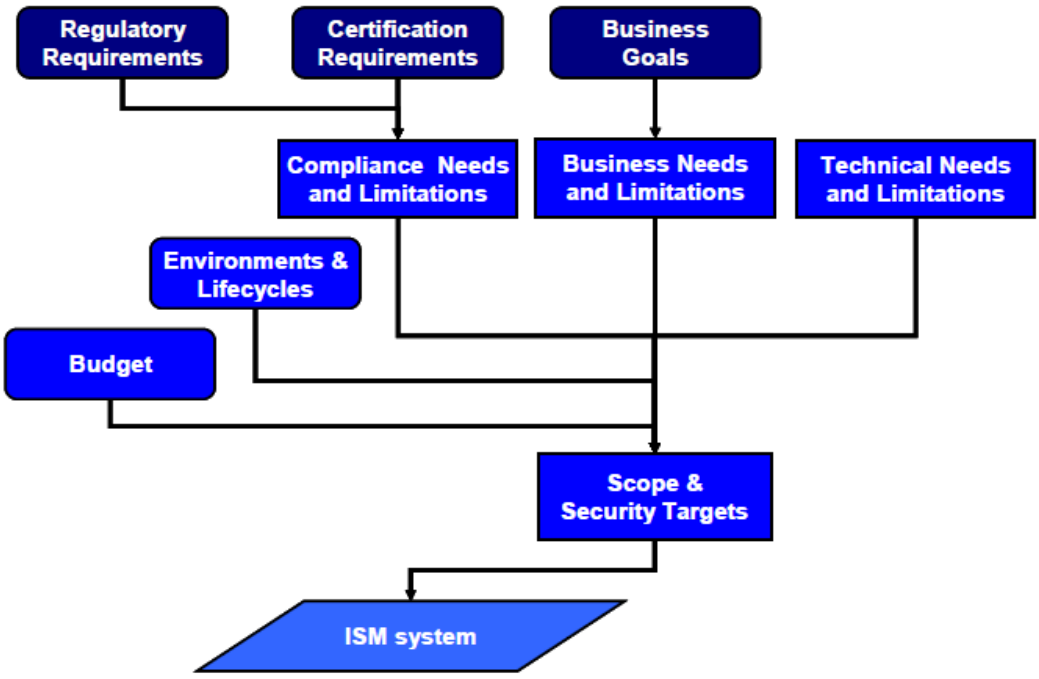


Figura 3.7 – Determinación del alcance y objetivos de seguridad [66]

El enfoque también está alineado con las norma ISO/IEC 27.001 e ISO/IEC 27.003, donde se establece que se deben realizar las siguientes actividades:

- Establecimiento del contexto
- Analizar los aspectos más relevantes del negocio desde un punto de vista estratégico-empresarial (objetivos, prioridades, planes estratégicos), a los efectos de determinar el alcance y límites del SGSI y la política del mismo.
- Especificar formalmente el alcance y límites del SGSI.
- Determinar la política del SGSI, alineada con la estrategia empresarial y a las decisiones tomadas por la Dirección y Gerencia en cuanto al mismo.

En esta etapa hay que contemplar, las actividades sustantivas de la empresa, pero también el marco funcional en el que se desempeña y la estructura del grupo empresarial al que pertenece. Deberán determinarse los grados de adecuación y cumplimiento a políticas y estrategias corporativas y los grados de autonomía. Estos aspectos trascienden a la órbita de la seguridad de la información, son aspectos institucionales que afectan diferentes áreas y diferentes disciplinas.

Dependencias y riesgos interempresariales:

Un caso particular, se da cuando además de una relación jerárquica entre las empresas del grupo, existe una relación de *proveedor – consumidor* en lo que a servicios se refiere; por ejemplo donde los servicios e infraestructura de una de las empresas, depende de los servicios prestados por la otra.

En [89] y [90] se describe un metamodelo conceptual denominado ISE por sus siglas en inglés *Implementation – Service – Effect* para infraestructuras complejas, donde además se presentan dependencias entre modelos eventualmente pertenecientes a un sistema o empresa externa. El mismo permite representar e integrar las diferentes perspectivas de un análisis que debe ser multidisciplinario, y facilita la abstracción de los aspectos relevantes del negocio y de los aspectos técnicos, y con ello la comunicación y alineamiento entre los expertos de diferentes disciplinas.

Como se observa en la Figura 3.8, se presentan tres capas de abstracción, una de *Efecto* o impacto, básicamente describe la incidencia en el negocio y las consecuencias en la calidad de sus servicios. Luego la capa de *Servicios* que soportan los procesos de negocios, y una capa de menor nivel de abstracción es la de *Implementación*, que comprende los detalles técnicos de la implementación de esos servicios.

Se establecen las dependencias jerárquicas entre las capas mencionadas, pero además las eventuales dependencias transversales que existan entre los diferentes submodelos, en particular, en nuestro caso los servicios de ambas empresas y cómo eventualmente el impacto en una de ellas puede afectar a la otra, y tener además efectos globales.

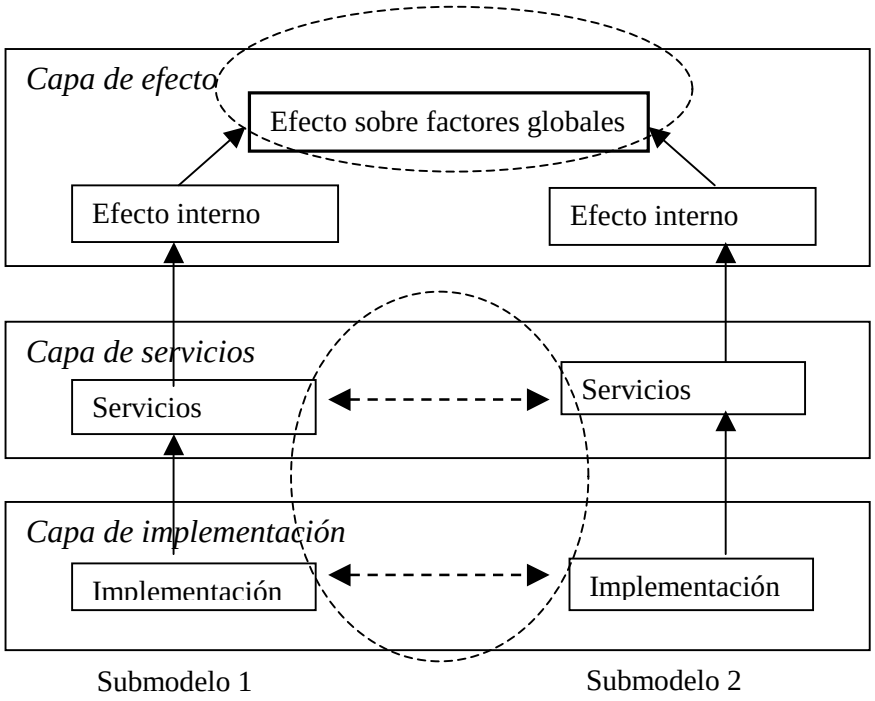


Figura 3.8 –Metamodelo ISE. Adaptación propia de [89]

3.2.6.1 Establecimiento del contexto

Deben considerarse: la misión de la organización, los valores o principales activos del negocio, los estratégicos, los factores de éxito. Debe analizarse además el sector en el que se desarrolla la Organización y características propias de la misma. Objetivos y prioridades respecto al desarrollo del negocio, planes de continuidad del mismo.
Debe considerarse aquí, la relación con las políticas globales del grupo; cómo inciden y en qué grado son vinculantes y obligatorias las políticas generales sobre las particulares de la empresa subordinada y como se relacionan o corresponden.

En la Figura 3.9 se explicita la relación entre las diferentes empresas y organizaciones y la referencia de estándares y marcos normativos y metodológicos, a los efectos de inferir los requerimientos extendidos de la seguridad de la información, provenientes de estándares, políticas y buenas prácticas generales.

Allí vemos en un primer nivel: las normas y estándares internacionales ISO/IEC, y por otro lado estándares, recomendaciones y buenas prácticas de la industria, que podrán ser normas de la ISO/IEC o Recomendaciones de otros organismos especializados en el sector de la industria correspondiente. Estos estándares son, en general, avalados y homologados a nivel nacional por la Unit [83], con su aporte correspondiente. En un nivel inferior encontramos las políticas generales de estado y las políticas corporativas, que en su justos términos recaerán sobre la empresa en cuestión al momento de considerar los requerimientos iniciales que son heredados como base de partida para su consideración.

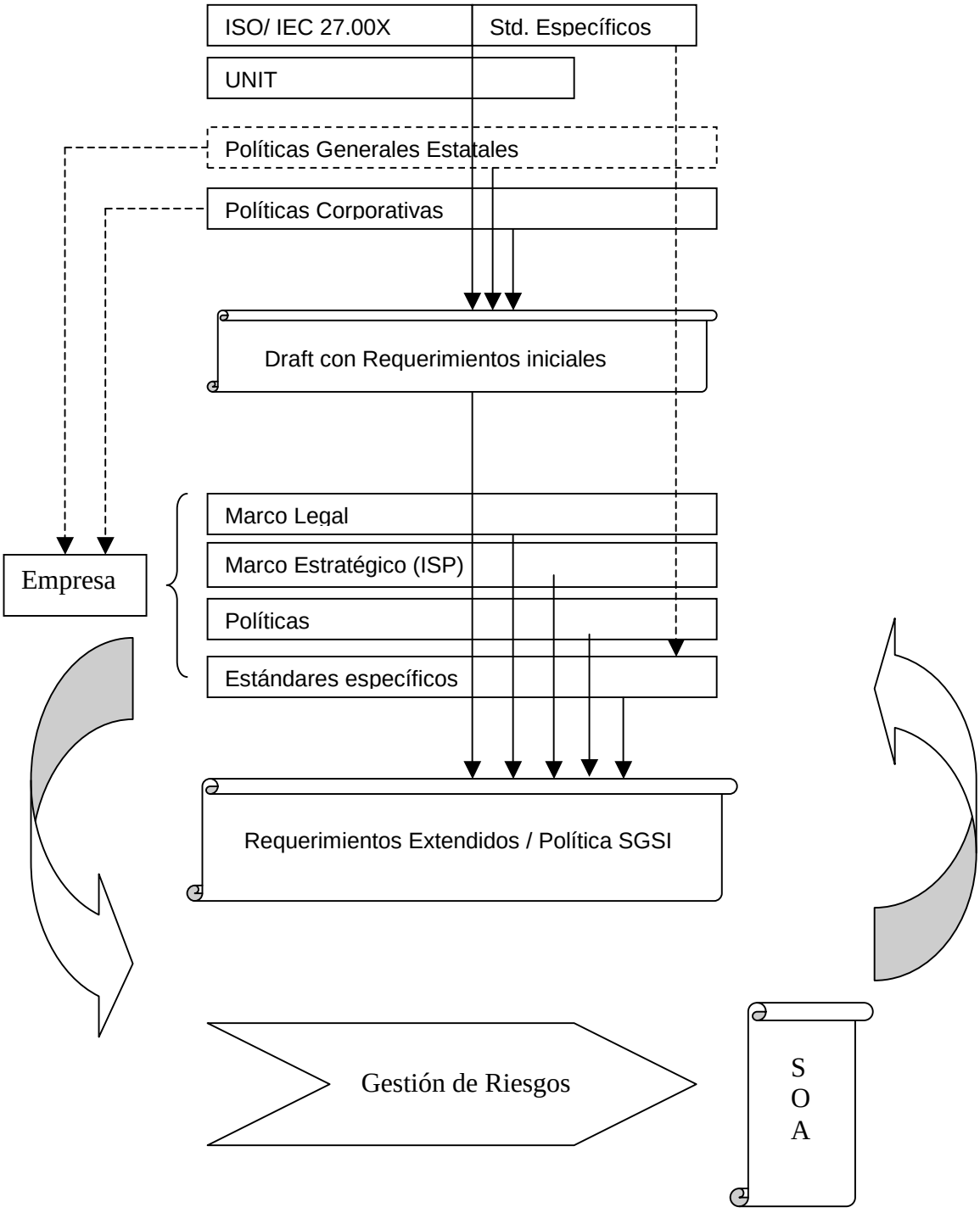


Figura 3.9 – Determinación de los Requerimientos extendidos del SGSI

3.2.6.2 Definición de los Requerimientos de Seguridad del Negocio

Se definen los requerimientos de seguridad del negocio adecuados para el negocio y el sector industrial en el que se desempeña.

Entrada:

Debe tenerse en cuenta, entre otras cosas:

a. Estrategia del Negocio en un ámbito de competencia. Misión, Visión, Planes Estratégicos, etc.
b. Requerimientos operativos críticos.
c. Políticas Corporativas.
d. Marco Jurídico y contractual.

Acción:

Algunas herramientas que son aplicables en las primeras fases de análisis del negocio, con foco en la Seguridad de la Información son:

a. *Focus Groups*, seleccionando un número acotado de participantes representativos y en torno a un área o proceso que los vincula (foco). Esta actividad puede ser guiada y/o complementada por modelos de operación y/o de gestión del negocio así como estándares para la industria en este sentido. Se busca que la integración del grupo enriquezca con puntos de vista diferentes pero conservando la especificidad del tema concreto o foco del grupo. Es conveniente que los mismos sean conducidos y moderados por un especialista en el área de Seguridad con buen entendimiento del negocio si es posible.
b. Técnica *Delphi* ([10])
c. *Workshops* específicos, eventualmente dirigidos por un experto en el área de seguridad y de SGSI.
d. Consultorías.

Quienes deberían participar:

a. Gerencia / Dirección de la empresa.
b. Comité de Seguridad
c. Gerentes de línea y de las diferentes unidades de negocio.
d. Responsables de los procesos sustantivos (críticos y prioritarios) de la empresa.
e. Profesionales y especialistas con buen entendimiento del negocio así como los requerimientos y aspectos relevantes de la Seguridad de la Información.

La participación de Personal especializado en el área con experiencia en la implantación de SGSI en la industria puede ser un valor considerable.

Salida:

[10] Referirse al Glosario.

Un documento con la definición en un nivel macro, de los requerimientos de seguridad del negocio y de la seguridad de la información.

3.2.6.3 Alcance y limites

Debe especificarse con claridad, el alcance del SGSI, qué cosas están incluidas y cuales no. El alcance puede ser la empresa en su totalidad, algunas áreas específicas, algunos productos y/o servicios específicos.

Entrada:

Deben considerarse objetivos y planes estratégicos, planes de negocios, la estructura y funciones de la organización, marcos legales, contractuales y regulatorios, condiciones geográficas, aspectos socio-culturales, expectativas de los clientes, restricciones, etc.

Desde una perspectiva de sistemas, entre otros deben considerarse:

Planes Estratégicos.
Planes Operativos.
Planes de Continuidad del Negocio.
Soporte tecnológico de hardware, infraestructura, etc.
Soporte lógico.
Software de Gestión: Aplicaciones ([11]) / ERPs, Scripts, Herramientas / Case
Datos: Bases de datos, repositorios de información.
Documentación: Políticas, procedimientos, mejores prácticas.
Información Comercial. Información Técnica. Proyectos. Finanzas, etc.
Marco Legal / Jurídico, Contratos.
Relaciones con sus pares (competencia, empresas comparables, referentes del sector, etc.).
Relaciones con Proveedores.
Relaciones y Calidad de Servicio al Cliente. SLAs ([12]).

Acción:

Debe analizarse toda la información descrita en la entrada, y considerar aspectos como la cultura organizacional, a los efectos de plantearse un alcance adecuado para los objetivos y prioridades de la empresa y posibles de lograr con los recursos con que se contará. Deben analizarse aquí posibles intersecciones con el alcance del SGSI de la empresa principal, a los efectos de contemplarlo en las diferentes fases del mismo.

Quienes deberían participar:

a. Gerencia / Dirección.
b. Comité de Seguridad.

[11] Comerciales o a medida
[12] Service Level Agreement

Salida:

Una especificación concreta y concisa del alcance, que determine en lo posible sin ambigüedades, qué activos de información estarán comprendidos en el SGSI y cuales no.
A modo de ejemplo, podría ser tan sólo desde un proceso de negocio crítico, una parte de la organización (una División, un Departamento, etc.), o la gestión de la información de la empresa en su totalidad, en su alcance más ambicioso.

3.2.6.4 Política del SGSI

La Política del SGSI especificará como deberá definirse, mantenerse y actualizarse el SGSI.

Entrada:

a. Contexto
b. Alcance y Límites

Acción:

Deben definirse al menos:
a. Los criterios, principios y lineamientos fundamentales con respecto a la seguridad de la información.
b. Criterios, contexto y mecanismos por el cual se gestionarán los riesgos.
c. Requerimientos del negocio en cuanto a la seguridad de la información.
d. Normativa / Legislación vigente.
e. Aspectos contractuales en lo referente a la seguridad de la información.

Cuando la política del SGSI de la empresa principal del grupo empresarial alcanza también la de la empresa considerada, puede esperarse en general que los principios y lineamientos directrices de la seguridad de la información sean muy similares o coincidan, sin embargo la estructura normativa y requerimientos contractuales pueden ser diferentes.

Quienes deberían participar:

a. Gerencia / Dirección.
b. Comité de Seguridad.

Salida:

Un documento con la Política del SGSI.

3.2.7 Análisis de Gap

A los efectos de planificar la implementación de un SGSI, como en todo proyecto, es deseable conocer el estado o situación en la que se encuentra la empresa en cuanto a los objetivos a trazarse y el alcance del mismo, y poder planificar así sobre estimaciones más certeras el plan, diseño e implementación del SGSI (*roadmap*).
Los objetivos y alcance deberán estar alineados con la realidad de la empresa y sus prioridades, así como salvar las condicionantes y prever recursos acorde a la dimensión de la tarea a realizar considerando el escenario de partida y el escenario planteado como meta.

Entrada:

a. Análisis del negocio.
b. Normas, Estándares y Buenas prácticas. (internacionales, nacionales, generales y específicas de la industria y así como recomendaciones propias para el sector.)
c. Marco jurídico normativo y contractual.
d. SGSI de la empresa 'madre' (o principal del grupo) y políticas corporativas.

Acción:

Seleccionar en una primera instancia los procesos más relevantes del negocio y analizar los requerimientos en términos de confidencialidad, integridad y disponibilidad.
Comparar con los requerimientos de los estándares de referencia (familia ISO/IEC 27.000), las buenas prácticas y los requerimientos del negocio.

Quienes deberían participar:

a. Equipo de Planeamiento de la Seguridad de la Información.
b. Gerentes de línea y de las diferentes unidades de negocio.
c. Responsables de los procesos sustantivos (críticos y prioritarios) de la empresa.
d. Profesionales y especialistas con buen entendimiento del negocio así como los requerimientos y aspectos relevantes de la Seguridad de la Información.
e. La participación de Personal especializado en el área con experiencia en la implantación de SGSI en la industria puede ser un valor considerable.
f. Esta etapa puede ser guiada por un consultor o especialista en Seguridad de la Información, que podría ser interno o externo.

Salida:

Un informe de situación respecto de el estado de la empresa en cuanto a la Seguridad de la Información y la distancia o los aspectos pendientes de resolver para llegar al nivel deseado.

3.2.8 Gestión de Riesgos

En esta sección se analiza la necesidad de definir *criterios básicos para la gestión de riesgos,* se presenta una *introducción, la base normativa* y el *enfoque* que debe guiar este proceso. Se especifica sintéticamente el proceso de análisis y evaluación de riesgos, y se da lugar a los *cuestionamientos* que se presentan para la *definición de una estrategia* para la gestión de riesgos en un grupo empresarial como se pretende a los efectos de fundamentar la elección de la estrategia adoptada. Para ello además, se especifican las diferentes actividades necesarias para la Gestión de Riesgos presentadas en el Cuadro 2.2 de la sección "2.16 Norma ISO/IEC 27.005 y el Ciclo de Deming" en el capítulo anterior.
Complementariamente se conceptualiza el problema de la *estimación de riesgos* y *valoración de activos* en términos de *grafos* y se presenta la posibilidad de aplicación de técnicas de grafos para este cometido.

3.2.8.1 Definición de Criterios Básicos

Deben definirse los criterios básicos de seguridad de la información que son relevantes para el negocio. Estos criterios, guiarán las sucesivas etapas de análisis y gestión de riesgos y sustentarán las decisiones en este sentido. Sobre estos criterios, se basarán respuestas a las interrogantes de hasta dónde es conveniente invertir en seguridad, si son tolerables o no los riesgos que se afrontan, así como la elección de la alternativa más conveniente y adecuada para la empresa.

Deben definirse:

- Criterios para evaluación de Riesgos
- Criterio para análisis de Impactos
- Criterio para aceptación de Riesgos

A modo de ejemplo, un mercado y sector de la industria donde se compite por productos similares o que pueden ser percibidos como equivalentes, la confidencialidad y oportunidad de la información, como puede ser la liberación de un nuevo producto o servicio, tiene eventualmente un impacto positivo en la diferenciación del servicio como un valor agregado, oportunidad y valor que se pierde si no se llega primero al mercado.

3.2.8.2 Introducción y base normativa

Definir y adoptar un sistema de gestión de riesgos, entendiendo *"sistema"* por los criterios elegidos para identificar, evaluar, y tratar riesgos hasta su punto de aceptación es algo obligatorio para dar cumplimiento a la norma, pero más allá de eso es un elemento muy valioso para analizar de forma racional que tan importante y hasta que punto se debe llegar con la seguridad de la información. Cuál es el valor agregado al negocio, o que cosas son imprescindibles ya sea por el marco legal o su nivel de criticidad y estratégico para el negocio.

Un Plan de Tratamiento de Riesgos, implica entre otras cosas: establecer el contexto de alcance y aplicabilidad, identificación y evaluación de activos y de riesgos, tratamiento de los mismos, aceptación del riesgo (residual), comunicación de los riesgos, monitoreo y revisión (de los riesgos y del plan).
Implica además, como todo plan, establecer objetivos y prioridades y asignar recursos, responsables.

Deben detectarse los diferentes activos de la organización, en particular, los activos de información. Asimismo, detectar las vulnerabilidades de los mismos y amenazas a las que están expuestos, y el impacto o los daños que le ocasionaría a la Empresa u Organización que las mismas se concreten.

Dado que la Seguridad no es un fin en sí mismo, debe definirse antes que nada, cual va a ser el criterio para identificar, evaluar y tratar esos riesgos.
A los efectos de establecer objetivos y prioridades es necesario saber hasta donde llegar, hasta donde evitar riesgos y donde conviene asumirlos. Para ello es necesario estimar el riesgo (impacto y probabilidad) y los recursos necesarios. También se requiere de criterios de aceptación bien definidos. A los efectos del monitoreo y ajustes sucesivos en la estimación así como en la medición de efectividad del plan y los controles implementados, se requiere el uso de métricas.

Este contexto, los criterios de aceptación, las prioridades e incluso quizás las métricas a utilizar, dependerán en gran medida del perfil de la organización y el área de negocios en que se desarrolla.

En función de dichos criterios, y un análisis Costo – Beneficio se obtiene una lista de riesgos priorizada.

Estos riesgos, deben ser tratados, es decir, se debe optar si los mismos deben:

- mitigarse (implementando controles)
- aceptarse
- evitarse
- transferirse (por ejemplo a terceros por contrato o una compañía aseguradora).

El proceso de gestión de riesgos, y la evaluación en si misma, es un proceso iterativo, en el cual además de ir cambiando el contexto, permite llegar a diferentes grados de profundidad en el análisis pero sin demorar las detecciones más inmediatas y mejoras que se pueden incorporar rápidamente, que quizás son las que tienen una mejor relación costo / beneficio.

Si los riesgos residuales no son aceptados, se requiere el tratamiento de los mismos, incorporando nuevos controles, eliminando o mitigando los mismos o de lo contrario transfiriéndolos a terceros.
Aquí es necesario otro ciclo de evaluación para ver si el nuevo nivel de riesgos es aceptable.

Es crítico para la efectividad del Plan y el fin perseguido que es la Seguridad de la Información, a los efectos de la continuidad del negocio, que los riesgos que no se traten (por ejemplo por

motivos económico-financieros, por considerarse de costo excesivo), sean expresamente asumidos por la Dirección y nivel gerencial.

En la Figura 3.10, tomada de la norma ISO/IEC 27.005 [30], se ilustra el proceso de Gestión de Riesgos anteriormente descrito:

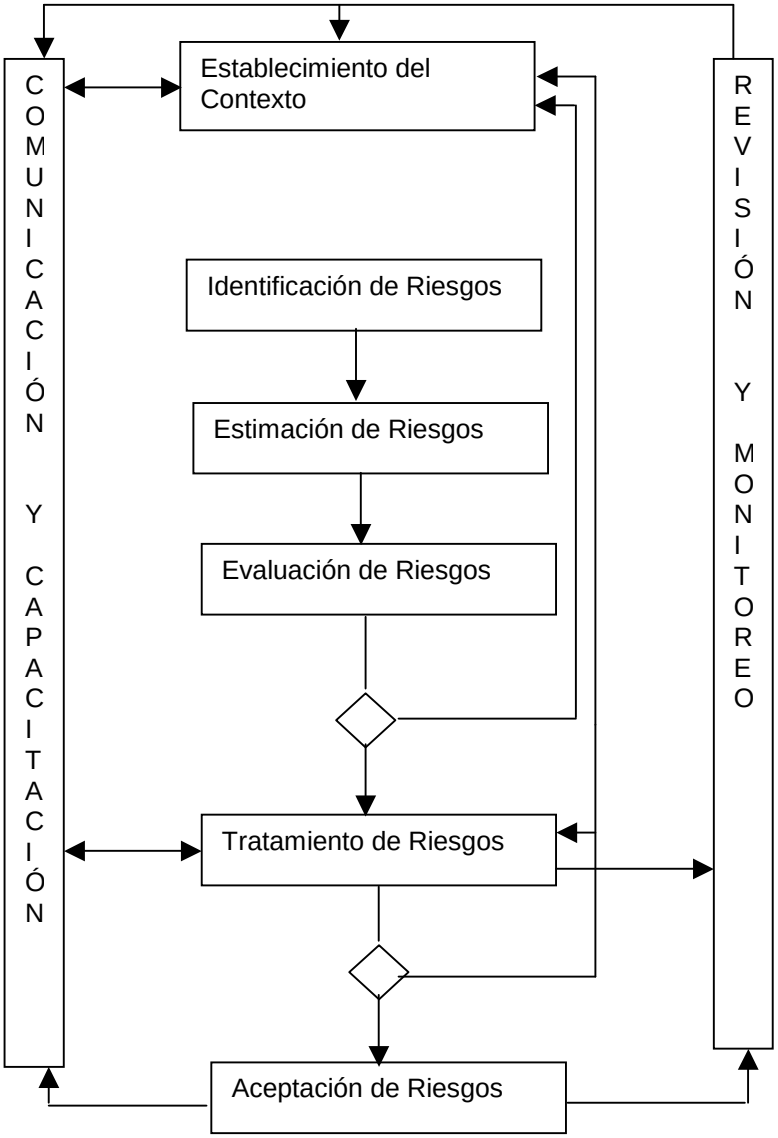


Figura 3.10 – Gestión de Riesgos. [30]

Cuando esto es analizado en el contexto de un grupo empresarial con una estructura jerárquica, este proceso debe coordinarse.
Por ejemplo, pueden existir activos de información compartidos (más allá de quien es el dueño de la misma), recursos o controles que requieran la coordinación de esfuerzos para lograr eficacia y ser eficientes.

A modo de ejemplo, una de las empresas puede ser "*dueña*" (responsable) de determinado recurso de información (porque la genera o la gestiona), pero que el acceso o la disponibilidad de la misma sea prioritario para la otra (o requerida para prestar sus servicios).
Podrían incluso percibirse los riesgos de forma diferente o priorizarse de forma diferente.
Desde un punto de vista sistémico, y considerando al grupo empresarial en forma global, lo ideal sería que ese riesgo sea tratado evitando controles redundantes es decir de forma eficiente y con la prioridad requerida. Pero por otra parte, considerando cada empresa, es esperable que cada una de ellas trate el riesgo de acuerdo a como lo percibe, a su estrategia de negocios, sus objetivos y su relación costo beneficio.
Si las estrategias no están alineadas, tampoco lo estarán en este aspecto.

Se requiere por tanto, de una definición metodológica concreta y un marco de trabajo para gestionar y operar estas circunstancias.

Por otra parte, según la ISO 27.001, todos los controles que se implementen para un SGSI deben estar basados en un proceso de Gestión de Riesgos. Esto tiende a hacer eficiente la definición e implementación de los controles, con una metodología que los justifique con criterios bien definidos.

3.2.8.3 Enfoque

La Evaluación de Riesgos es el eje central de la norma ISO/IEC 27.001 y por tanto de un SGSI, pero además participa y muchas veces es el *Core* de varias actividades y de otros planes de gestión como se ilustra en la Figura 3.11.

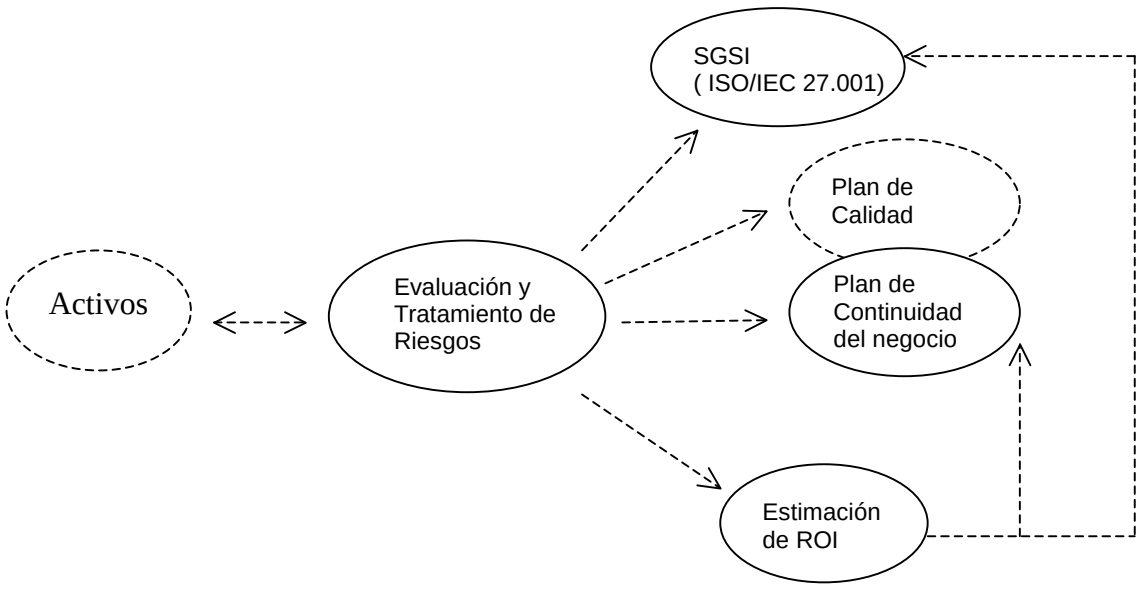


Figura 3.11 – Gestión de Riesgos I

O más precisamente, atendiendo a las composición y alcance de la ISO/IEC 27.001, como se reformula en la Figura 3.12:

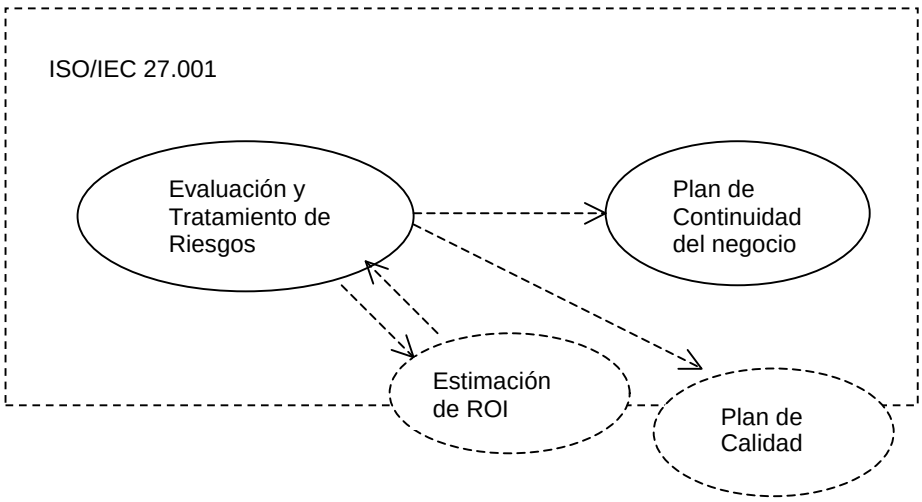


Figura 3.12 – Gestión de Riesgos II

Algunos ejemplos para esta relación o participación de la evaluación de riesgos en múltiples análisis y planes (de continuidad del negocio, de seguridad, de calidad, etc.) que pueden resultar muy gráficos son:

- En función de la criticidad de determinado proceso, de los requerimientos de seguridad (atributos y niveles necesarios de seguridad), y de los riesgos percibidos, puede decidirse que un proceso sea realizado internamente por funcionarios técnicos propios de la empresa o de lo contrario se puede optar por la conveniencia de tercerizarlo.

- Por otra parte, sería un gasto de recursos excesivo e inconducente, establecer un plan de tratamiento de riesgos a bajo nivel, con detalles operativos de un proceso o asegurar completamente una aplicación que la empresa luego decide tercerizar. No debe confundirse aquí los detalles de implantación de controles con las necesidades de especificar la seguridad requerida, lo cual hasta cierto nivel es necesario y conveniente, a los efectos de incluir en las cláusulas contractuales con terceros.
  Es decir, deben coordinarse los esfuerzos con las necesidades concretas en el área de Seguridad de la Información y alineada con otros planes estratégicos, de gestión, de calidad, etc.

3.2.8.4 Análisis y Evaluación de Riesgos

La norma ISO/IEC 27.001, está basada en procesos. Con ese enfoque, el Análisis y Evaluación de riesgos es un proceso. El mismo se especifica a continuación:

Entrada:

a. Criterios básicos, el alcance y limites, y las características de la propia organización.
b. Riesgos percibidos por la empresa principal para el ámbito de el SGSI que se está analizando. Los mismos estarán clasificados según la percepción Corporativa de la empresa principal y bajo su propio SGSI.

Acción:

Se debe considerar la clasificación de los riesgos de forma cualitativa y cuantitativa. Luego se deben priorizar según un criterio definido y los objetivos de la organización.

Los riesgos, como puede sintetizarse de [25], son la combinación de la ocurrencia de uno o más eventos que tienen una determinada probabilidad de ocurrir, provocando un impacto no deseado. Puede ser visto como la materialización de una amenaza que explota una o más vulnerabilidades a la cual están expuestos los activos / bienes de la Organización.
La evaluación cuantitativa y cualitativa de riesgos, permite a la gerencia priorizar los riesgos a minimizar y tomar las decisiones con mayor certeza.

Salida:

Una lista de riesgos priorizados según una lista de criterios de evaluación.

Sin embargo en la norma no se presenta ni se especifica un método ni un algoritmo concreto para realizar este análisis y evaluación de riesgos. Por lo tanto cada Organización deberá elegir la estrategia que mejor se adapte a sus necesidades, características y le dé mejores resultados teniendo presente las disposiciones legales y los requerimientos del negocio. En una organización multiempresa con estructura jerárquica se hace necesario definir una estrategia para el análisis y evaluación de riesgos eficaz y eficiente.

3.2.8.4.1 Estrategia: ¿ Top Down o Bottom up ?

Entendemos que lo más adecuado, para este tipo de organizaciones, considerando todas las apreciaciones de las secciones anteriores así como las normas referidas, es un enfoque de alto nivel, que guíe la estrategia de identificación, evaluación y priorización de riesgos. Cuanto más global es el enfoque en una primer etapa, donde se establecen los lineamientos y políticas generales, es mayor la probabilidad de su adecuación a la estrategia y políticas generales del negocio y a su vez con una relación costo – beneficio conveniente en lo global.

En este enfoque global, no se debería entrar en detalles tecnológicos concretos ni particularidades del dominio concreto 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 know how específico, deberán hacerse las evaluaciones locales así como la definición de controles y la estrategia de implementación.

Por otra parte sin embargo, atendiendo a la especificidad y complejidades de cada área o dominio de aplicación, y al *know how* de los profesionales de cada área, 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.
En este caso, puede ser necesario eventualmente, elevar determinada percepción de riesgos si es necesaria su consideración a un nivel superior (de la Gerencia General o Dirección del Grupo Empresarial por ejemplo).
En este caso, tendríamos una implementación de controles y aporte (como retorno) del riesgo percibido *Bottom-Up*.

Por lo tanto, es claro según lo anterior que lo conveniente es una estrategia 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.

Esto intenta sumar 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 ejemplo).

Como se afirma en [12] un sistema de Gestión de Riesgos de un SGSI, a los efectos de dar cumplimiento a los requisitos de las norma ISO/IEC 27.001, debería cumplir con los siguientes requerimientos:

- Enfoque *Top – Down*, desde un inicio, debería estar guiada por una visión de alto nivel de la Organización y los procesos de negocio, refinada sucesivamente pero siempre alineada a las necesidades del negocio.
- Identificación de los procesos de negocios, los activos de información y su criticidad y niveles de seguridad requeridos.
- Identificación de amenazas, vulnerabilidades, y niveles de riesgos referentes a cada activo. Activos que aportan valor en los procesos de negocio.
- Enfoque proactivo, es decir que considere medidas preventivas y de contingencia, además de las acciones correctivas**,** con la posibilidad de seleccionar controles y medidas que permitan instrumentar un Plan de Tratamiento de Riesgos, con un criterio racional y conveniente en cuanto a la relación costo / beneficio.
- Integración o posibilidad de reutilización de esta estrategia para la gestión de riesgos necesaria en un Plan de Continuidad del Negocio y complementaria con eventuales Planes de Calidad de la empresa.

A. Bialas y K Lisek [12] presentan una estrategia de evaluación de riesgos “de dos etapas”, como se muestra en la Figura 3.13, 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.

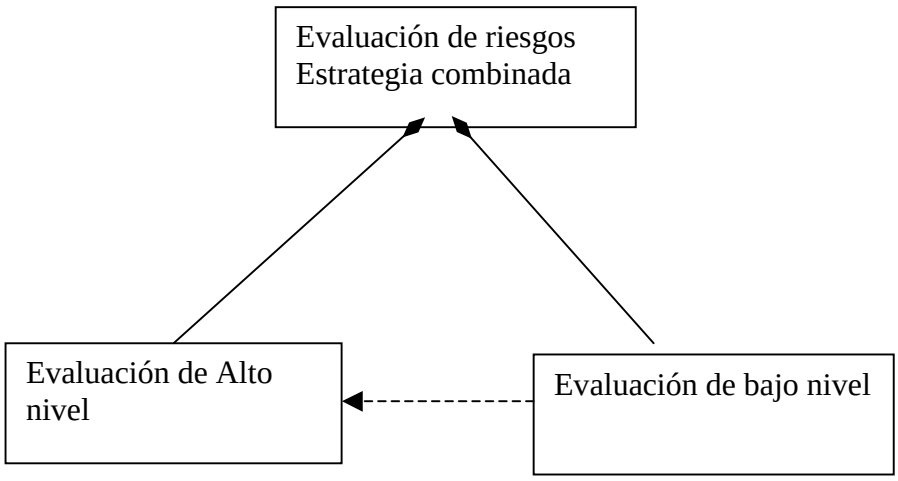


Figura 3.13 Evaluación de riesgo en dos fases. [12]

Es decir, se plantea una evaluación de riesgo combinada, bi-fase:

- Una fase de alto nivel: de un mayor nivel de abstracción, que establece las directivas y lineamientos y define un mapa rápido de riesgos corporativos.

- Una fase de un nivel más bajo, más detallado y técnico o especializado por dominio de aplicación y donde amerite, de acuerdo al análisis de alto nivel.

Este enfoque permite, determinar los dominios y procesos más críticos, de mayor valor agregado para el negocio y donde la inversión en seguridad tiene el mayor retorno, o dicho con otras palabras lo amerita ampliamente, para evitar impactos importantes en el negocio. De esta forma se logra un buen nivel de efectividad en cuanto que permite alinear el SGSI a las necesidades del negocio.
A su vez, este enfoque tiene la virtud que se puede profundizar de forma selectiva en las áreas / dominios de información y procesos que se consideren más críticos y no en todos los procesos y activos uniformemente. Es decir, prestar mayor atención y asignar más recursos (tiempo y técnicos) a aquellos procesos claves y relevantes, y dotar de una línea base de protección definida para el resto no tan importantes.

Esta estrategia logra una adecuada relación costo / beneficio, evitando la sobreasignación y superposición de recursos o complejos análisis para procesos o activos que no lo ameritan.
Sin embargo, como bien lo reconocen sus autores, este enfoque no es totalmente compatible con la norma ISO/IEC 27.001, que requiere en su Anexo A - el cual tiene carácter normativo – que: “todos los activos deben ser claramente identificados”.

En el presente trabajo de tesis, se propone una variante para subsanar este aspecto, además de generalizar este enfoque al SGSI en su globalidad.

3.2.8.4.2 Definición de la Estrategia

Atendiendo a la estructura empresarial que se analiza, y a lo expuesto en las secciones anteriores, proponemos visualizar el análisis y evaluación de riesgos como la combinación consistente de ciclos de análisis de diferente jerarquía, nivel de abstracción y frecuencia cíclica. Decimos combinación consistente en el sentido que el o los ciclos de mayor nivel de abstracción guían el/los ciclo/s sucesivo/s con mayor nivel de detalle que a su vez varían con una frecuencia mayor.

Es decir, un análisis de alto nivel que fija las pautas, establece criterios y los pilares para la gestión de riesgos así como las prioridades, que varía relativamente con menor frecuencia que el análisis y tratamiento de los riesgos que debe realizarse a un nivel más bajo, con especificaciones y controles de menor granularidad.

Esto vale tanto para el enfoque del Grupo Empresarial (o empresa principal) con sus empresas subordinadas, así como también, internamente, en cada una de las empresas - de dimensión considerable – la relación entre sus diferentes dominios de actividad, es decir: las principales áreas de su organigrama y relevantes para la seguridad de la información. No obstante, la clasificación de estos dominios o áreas en las que se organiza la gestión de riesgos, no debe necesariamente ser la del organigrama; podría ser otra la clasificación más conveniente, en función por ejemplo de aspectos técnicos, conceptuales o políticos.

Otra forma de visualizarlo, en términos de ciclos de frecuencia y granularidad, se ilustra en la Figura 3.14.

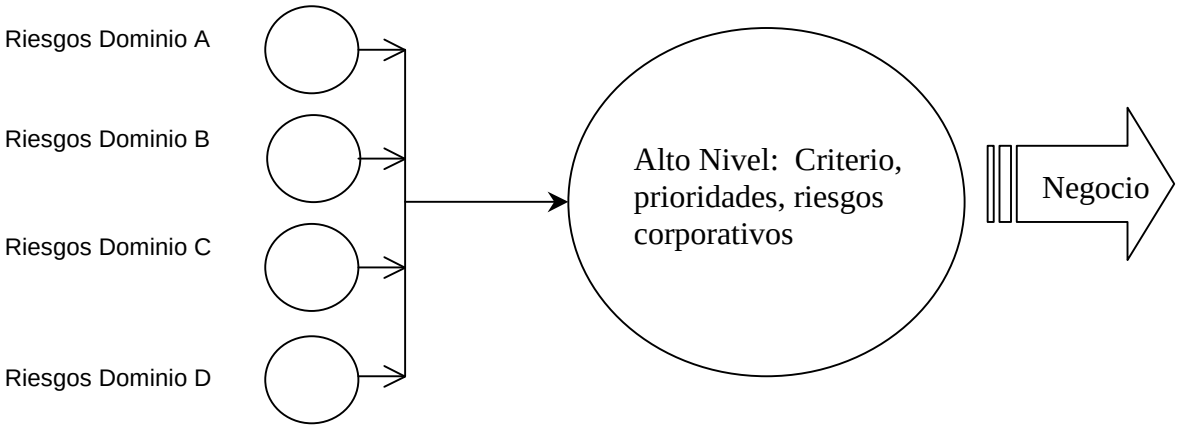


Figura 3.14 – Enfoque de riesgos jerárquico y multifase

Es decir, el análisis de riesgos es guiado por los principales procesos, activos y prioridades del negocio, alineado con la estrategia corporativa, y guiando a su vez a los otros dominios de análisis de riesgos. En el alto nivel (corporativo), los cambios son más lentos o varía con menos frecuencia. En los niveles más bajos en cambio, se establecen y revisan controles con mayor frecuencia y tiene un mayor nivel de detalle, políticas específicas y procedimientos técnicos y operativos.

Análisis de Riesgos de alto nivel:

En esta instancia se realiza un análisis de riesgos focalizando el aspecto funcional y de los requerimientos del negocio, intentando abstraerse de aspectos específicos de una tecnología, equipamiento (hardware) o software en particular.

Un análisis de riesgos de alto nivel permite:

- Obtener un rápido y grueso mapa de riesgos, detectando dónde debe ponerse el foco y priorizarse la utilización de los recursos disponibles.

- Ese "mapa" actúa como un croquis o esqueleto, que da los lineamientos y ayudará a prototipar los sucesivos análisis de riesgos de más bajo nivel. También permite comunicar de forma más rápida, concisa y clara, hacia donde se dirigirá la estrategia de tratamiento de riesgos, y facilita las correcciones oportunamente o ajustes que correspondan al nivel de la Dirección.

- Abstraerse de los aspectos tecnológicos o detalles específicos del dominio de aplicación, y permite focalizarse en los aspectos del negocio y el contexto operacional. De esta forma es más probable que la atención se ponga sobre las necesidades reales del negocio y no sobre aspectos tecnológicos o incluso controles sobredimensionados o que exceden las amenazas reales y las necesidades de seguridad.

- Por otra parte, este análisis de alto nivel, por su enfoque mismo, naturalmente se concentrará en escenarios de incidentes que así lo ameriten, y no se convertirá en un análisis sistemático de cada recurso (activo o proceso) en forma aislada. Permite entonces detectar más rápidamente qué es relevante y qué no (eficacia del análisis) y evita distraer recursos analizando en detalle activos o procesos no sustantivos o poco relevantes.

- Se detectan grupos más limitados de vulnerabilidades, amenazas y activos relacionados y no extensas listas que por su tamaño y diversidad / heterogeneidad de su composición se vuelven difíciles de analizar y gestionar.

- Es más fácil detectar riesgos vinculados, sobre un mismo dominio, y de esa forma permite adoptar una estrategia de riesgos que abarque varios de esos riesgos relacionados en forma conjunta, lo cual contribuye a la eficiencia y racionalización de los controles. Por otra parte, visualizar en forma temprana esas vinculaciones y dependencias permite lograr también la eficacia requerida para los objetivos y prioridades de seguridad establecidos.

3.2.8.4.3 Identificación del Contexto

El Contexto será básicamente el establecido para el SGSI pero debe especificarse de forma concreta cuales serán los criterios para la gestión de riesgos y toma de decisiones respecto al tratamiento de los mismos.

Entrada:

Debe considerarse el Contexto del SGSI: Normativo e Institucional, la Política del SGSI, los requerimientos de seguridad del negocio – producto del análisis del mismo -, y las consideraciones y resultados del Análisis de GAP.

Acción:

Analizar de forma amplia y concisa, cuál debe ser el marco contextual del proceso de gestión de riesgos, determinar el alcance y limites del mismo.

Quienes deberían participar:

El Contexto debería establecerse con una visión amplia, del negocio y de los requerimientos de seguridad del mismo, por ello si bien son estos últimos los que deberían primar sobre el análisis de riesgos, es deseable que la Dirección y Gerencias tengan el asesoramiento técnico de especialistas en materia de seguridad de la información. Deberían participar al menos:

a. Gerencia / Dirección de la empresa.
b. Comité de Seguridad / Gerencia de Seguridad de la Información.
c. Gerentes de línea y de las diferentes unidades de negocio.
d. Equipo de Planeamiento y Seguridad de la Información.
e. Asesoramiento del área Jurídica.

Salida:

Criterios básicos y lineamientos claros para la gestión de riesgos y toma de decisiones de forma que estén alineadas con los planes estratégicos del negocio.

3.2.8.4.4 Identificación de Riesgos

A los efectos de identificar los riesgos, deben cumplirse las siguientes actividades:

a) Identificación de los procesos de negocios más relevantes.
b) Identificación de Activos
c) Identificación de Amenazas
d) Identificación de Controles (existentes)
e) Identificación de Vulnerabilidades

A continuación, se describe *quienes deben participar* de los procesos de identificación de riesgos en forma general, teniendo presente que no todas las actividades se dan en el mismo

nivel de la jerarquía y que requiere la complementación entre las directrices gerenciales y una visión técnica detallada donde corresponda.
Posteriormente, en la especificación de cada una de estas actividades se especificará: la *entrada*, *acciones* a ser realizadas y la *salida* que se espera.

Quienes deberían participar:

La identificación de riesgos debe darse en todos los niveles jerárquicos, pero podemos distinguir un nivel macro, donde hay una participación más activa de las gerencias de línea, la Dirección y Gerencia General, particularmente la identificación de los procesos / activos críticos. Son ellos quienes conocen cuales son los procesos críticos del negocio, los fundamentales para su continuidad y los que aportan mayor valor, que en definitiva serán los estratégicos y donde la Dirección tiene un rol fundamental. Es en ese ámbito que se tiene la visión global y estratégica del posicionamiento de la empresa y hacia donde pretende dirigirse.

Por supuesto que la misma se apoyará en sus áreas técnicas y asesorías especializadas, donde necesariamente se detectarán vulnerabilidades, amenazas, controles y riesgos a un nivel más detallado y también activos a un nivel más desagregado.

Deben participar profesionales con fuerte conocimiento del negocio, los objetivos y estrategia de la organización, y además con conocimiento de los aspectos relevantes de la seguridad y como puede afectar los intereses y objetivos empresariales.

Algunos de ellos:

a. Alta Gerencia / Dirección de la empresa objetivo: en el alto nivel brindando las pautas directivas, políticas y estratégicas de negocios.
b. Gerentes de línea o a cargo de unidades de negocio: con una participación directa sobre su área, gestionando los recursos humanos especializados para realizar esta tarea. Responsable de identificar los riesgos de su dominio.
c. Responsables de procesos de negocios importantes: Análisis directo y puntual sobre los mismos, brindando la información necesaria para su gerencia responsable de forma proactiva con respecto a la seguridad de los mismos.
d. Otras personas con las características descritas.

Resulta conveniente además, para guiar el proceso y brindar asesoramiento, la participación de:

e. Comité de Seguridad de la Información, en forma de supervisión, dando lo grandes lineamientos y coordinando el proceso de análisis de alto nivel con la Dirección. Además apoya al Equipo de Planeamiento de Seguridad de la Información en cuanto éste lo requiera.
f. Equipo de Planeamiento de la Seguridad de la Información: colaborando en la identificación de riesgos desde su visión técnica.
g. Analista en riesgos.

Es importante el trabajo cooperativo entre los especialistas del negocio con especialistas en Gestión de Riesgos y Seguridad de la Información.

3.2.8.4.4.1 Identificación de los Procesos de negocios más relevantes (críticos).

Es vital, que la política del SGSI y la de la Seguridad de la Información, estén alineadas con la estrategia corporativa y planes de negocio de la empresa. En ese sentido, un análisis de la información y los procesos críticos y más relevantes de la empresa, permite concentrar y enfocar los esfuerzos en los procesos y activos de mayor valor agregado, logrando un rápido 'mapa' que permita visualizar dónde están los activos críticos de información y dónde tendrá mayor retorno la inversión realizada (ROI con criterio amplio, en lo que refiere a mantener la competitividad, evitar pérdidas y apoyar la estrategia y favorecer los planes de negocio).

Entrada:

a. Identificación de los procesos críticos y prioritarios desde la percepción de la empresa principal del grupo, procesos que estén dentro del alcance del SGSI en cuestión.
b. Know – How del negocio.
c. Planes existentes de continuidad del negocio.
d. Plan Estratégicos y Operativos.
e. Análisis de Organización & Métodos.

Acción:

Una fuente importante para relevar los procesos críticos, además de los planes estratégicos y operativos en general, es el análisis de la Gestión de la Continuidad del Negocio. Sobre la base que el negocio debería siempre poder funcionando, de este análisis pueden surgir los procesos críticos si es que no fueron detectados en estudios previos y son ampliamente conocidos por la Gerencia y Dirección de la empresa.

Tanto en la norma ISO/IEC 27.002 y el CobIT [74] de la ISACA (*Information Systems Audit and Control Association*), la Continuidad del Negocio ocupa un lugar importante.

De las once (11) Cláusulas de Control de la seguridad que define la norma ISO/IEC 27.002 como se mencionó en "2.1.1 Serie ISO/IEC 27.000", la décima es la " *Gestión de la Continuidad del Negocio* ", la cual comprende:

- Desarrollar y mantener un Proceso de Continuidad de Negocio en la organización y los requisitos de Seguridad de la Información necesarios para el mismo.
- Evaluación de Riesgos en términos de probabilidad e impacto / consecuencias para el negocio. Fundamentalmente, análisis de impacto en sentido amplio con visión en el negocio como tal: enfoque operativo y estratégico.
- Planes de Contingencia y Restauración de las operaciones y asegurar la disponibilidad de la información en el grado y tiempo requeridos (tolerancia).
- Pruebas, mantenimiento y reevaluación de estos planes de continuidad del negocio.

En el CobIT [74] por ejemplo, se tienen cuatro (4) dominios, que a su vez tienen procesos. En el dominio de "Entrega y Soporte" se tienen trece (13) procesos, y en particular el "*DS4 – Aseguramiento de Continuidad del Servicio / Operaciones*". Este proceso a su vez,

especifica trece (13) Objetivos de Control que van desde la especificación de un marco de referencia, una estrategia y una filosofía para la continuidad, hasta las indicaciones de contenido, implementación, pruebas y distribución del mismo.

Si bien ambos estándares tienen enfoques diferentes, en el caso de la ISO/IEC 27.002 es un conjunto buenas prácticas y controles para la gestión de la seguridad de la información, y en el caso de CobIT es el control de la información y el gobierno de IT, ambos enfoques coinciden en la necesidad de identificar los procesos críticos del negocio y de elaborar una estrategia corporativa en ese sentido, alineada con la estrategia, objetivos y planes del negocio.

Salida:

Los procesos críticos y prioritarios que aportan mayor valor agregado al negocio y son estratégicos para la misión y objetivos de la empresa.

3.2.8.4.4.2 Identificación de Activos

Es necesario identificar o inventariar los activos para luego analizar su valor y sus riesgos. Además de identificarse los activos debe especificarse y documentarse quien es su dueño o responsable de la seguridad del mismo, tal como se expresa en [26]: A.7.1 y A.7.2 y sus correspondientes secciones de [27] de donde son tomadas.
Debe además establecerse una política de uso de dichos activos como se establece en [26]: A.7.1.3.

Sin embargo puede ser muy costoso realizar esta tarea sin categorizar o agrupar los mismos con algún criterio. De acuerdo a la norma ISO/IEC 27.001 ([13]), Activo es "*aquello que tenga valor para la organización*", lo cual en principio admite una interpretación amplia y eventualmente con cierto grado de subjetividad.

En el método Magerit [3] se distinguen diferentes tipos de activos a los efectos de su categorización, ellos son:

- Servicios (externos al cliente e internos)
- Datos / Información
- Aplicaciones
- Equipos informáticos / Hardware
- Redes de comunicaciones: propias y contratadas
- Soportes de Información: dispositivos físicos de almacenamiento permanente.
- Instalaciones: físicas / locativas
- Personal
- Equipamiento Auxiliar: acondicionamiento eléctrico, térmico, mobiliario, *UPS*, cableado, etc.

Si bien los Servicios incluyen un amplio espectro, tanto de servicios prestados al cliente como servicios internos, no se distingue en principio, entre procesos auxiliares o de apoyo a las actividades sustantivas y los procesos y servicios que son realmente "un activo" como parte

[13] Tomado a su vez de ISO/IEC 13335-1: 2004.

medular del negocio. Es decir, un proceso puede llegar a ser crítico por la forma en que se hacen las cosas. En un futuro, si las cosas se hacen de una forma diferente o se redefinen los procesos, el valor de este activo cambia radicalmente.

De forma análoga en la norma ISO/IEC 27.005, en su Anexo B que tiene carácter informativo, se sugiere la distinción entre activos primarios: procesos y actividades de negocio, información y activos de soporte: hardware, software, redes, personal, infraestructura física y organizacional, etc.
Una distinción análoga se hace también en otras metodologías como por ejemplo Mehari [48].

Además de identificar y clasificar los activos según sus requerimientos de seguridad (y su criticidad para el negocio), debe identificarse quién es el propietario (o dueño) de ese activo. El mismo será el responsable por su seguridad, pudiendo delegar actividades o poder sobre la gestión de controles sobre el mismo, pero no podrá transferir (ni delegar) la responsabilidad.

Entre los activos primarios tenemos los procesos de negocios, actividades sustantivas y la información (estratégica, personal protegida jurídicamente, propiedad intelectual, crítica, etc.), que podemos ponerlos en un plano diferente a aquellos activos que sustentan actividades de soporte para el funcionamiento de la organización, incluyendo eventualmente software (no crítico), hardware, infraestructura logística y técnica, etc.

Sin embargo, la división no es tan simple, es sólo un enfoque desde dónde comenzar a priorizar los activos. El software por ejemplo, en lo que refiere a un sistema de información, suele ser menos crítico que la información en si misma, sin embargo puede tener igual importancia si es la única vía de acceso a la información, en ese caso, la indisponibilidad del software provoca que la información tampoco sea accesible o no esté disponible.
Por otro lado, para continuar con otro ejemplo de software, podemos tener software crítico en el sentido que es la base del negocio o implementa conocimiento propio del área del dominio de aplicación, eventualmente con tecnología propietaria de la propia empresa (desarrollo interno), y por otra parte, software ERP de terceros para tareas no sustantivas de la organización (por ejemplo: control de gastos, gestión de stock, RR.HH., etc.).

En la metodología que proponemos, diferenciamos de forma explícita los procesos de los (*"otros"*) activos, dada su naturaleza y a su carácter de ser: o bien inherentemente crítico atendiendo a la estrategia del negocio, o circunstancialmente crítico en función del flujo de trabajo y procedimientos establecidos.
A continuación, definimos el proceso de identificación de activos, y en particular, de activos críticos:

Entrada:

a. Know – How del negocio.
b. Relevamiento de los Procesos del negocio.
c. Planes estratégicos.
d. Calificación de los Activos realizados por la empresa principal que estén comprendidos dentro del alcance del SGSI que se analiza.

Acción:

Una vez definidos los "Procesos Críticos" o de mayor valor para el negocio, es posible obtener los activos críticos, que serán todos aquellos que intervengan y den sustento a los primeros o eventualmente sean resultado de los mismos.

Por otra parte, es una herramienta para determinar activos críticos o prioritarios en cuanto a los sistemas de información y la información en sí misma, determinando por ejemplo:
- ¿ Qué sistemas de información sustentan dichos procesos ?
- ¿ Qué información es requerida por los mismos ?
- ¿ Qué información es relevante y particularmente importante en cuanto a su confidencialidad, disponibilidad e integridad ?
- ¿ Qué factores o incidentes podrían afectar de forma grave o relevante estos procesos ?
- ¿ Cómo afecta esto a los procesos más relevantes del negocio ?

A los efectos de modelar esta realidad, y en la búsqueda de respuestas a estas interrogantes, definimos las relaciones R1, R2, R3 y R4 tal como se muestra en la Figura 3.15:

R1 (Activos x Activos)
R2 (Procesos x Activos)
R3 (Activos x Procesos)
R4 (Procesos x Procesos)

Todas ellas pueden leerse como "Depende de la seguridad de", es decir, el nivel de los atributos de seguridad requeridos para un proceso / activo requiere de determinados niveles de seguridad en los procesos / activos de los cuales depende.

Al igual que en Magerit [3], las relaciones denotan como se dijo, "dependencia de la seguridad", no dependencia funcional para su ejecución u obtención. En otras palabras, dos entidades (proceso o activo) estarán relacionadas si la seguridad de uno está comprometida por la seguridad del otro, es decir, si un incidente de seguridad en uno afecta la seguridad del otro.

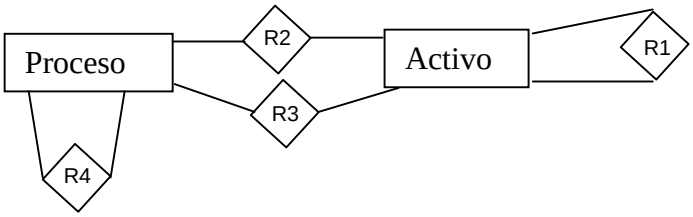


Figura 3.15 – Modelo Entidad relación entre Activos y Procesos

Generalizando podemos considerar **Activos*** = Procesos U Activos
Y así R: Activos* x Activos* = R1 U R2 U R3 U R4
Mediante proceso de clausura transitiva de las dependencias funcionales (R) podemos así identificar los activos de valor estratégico para la organización.

Una metodología eficaz y eficiente es:

Procesos Críticos y
*Dependencia entre Activos** $\Longrightarrow$ *Activos Críticos*

Donde $\Longrightarrow$ denota "determina".

Observar que si bien, generalizamos la relación de dependencia (R) a los procesos y activos, podemos diferenciar igualmente, el conjunto de activos que se consideran inherentemente críticos.

Sin embargo, como se mencionó en la sección: "*3.2.8.4.1 Estrategia: ¿ Top Down o Bottom up ?*" la norma ISO/IEC 27.001, en su Anexo A que tiene carácter normativo, requiere que "todos los activos deben ser claramente identificados". Esto es: todos los activos – todo aquello que tenga valor para la organización - comprendidos en el alcance del SGSI.
Es decir, que si nos interesa cumplir fielmente la norma, a los efectos de una certificación pero a su vez, concentrarnos en los procesos (y activos) críticos o de mayor valor para el negocio, una estrategia es ser más precisos en la declaración del Alcance del SGSI y eventualmente redefinirlo, como se muestra en la Figura 3.16.

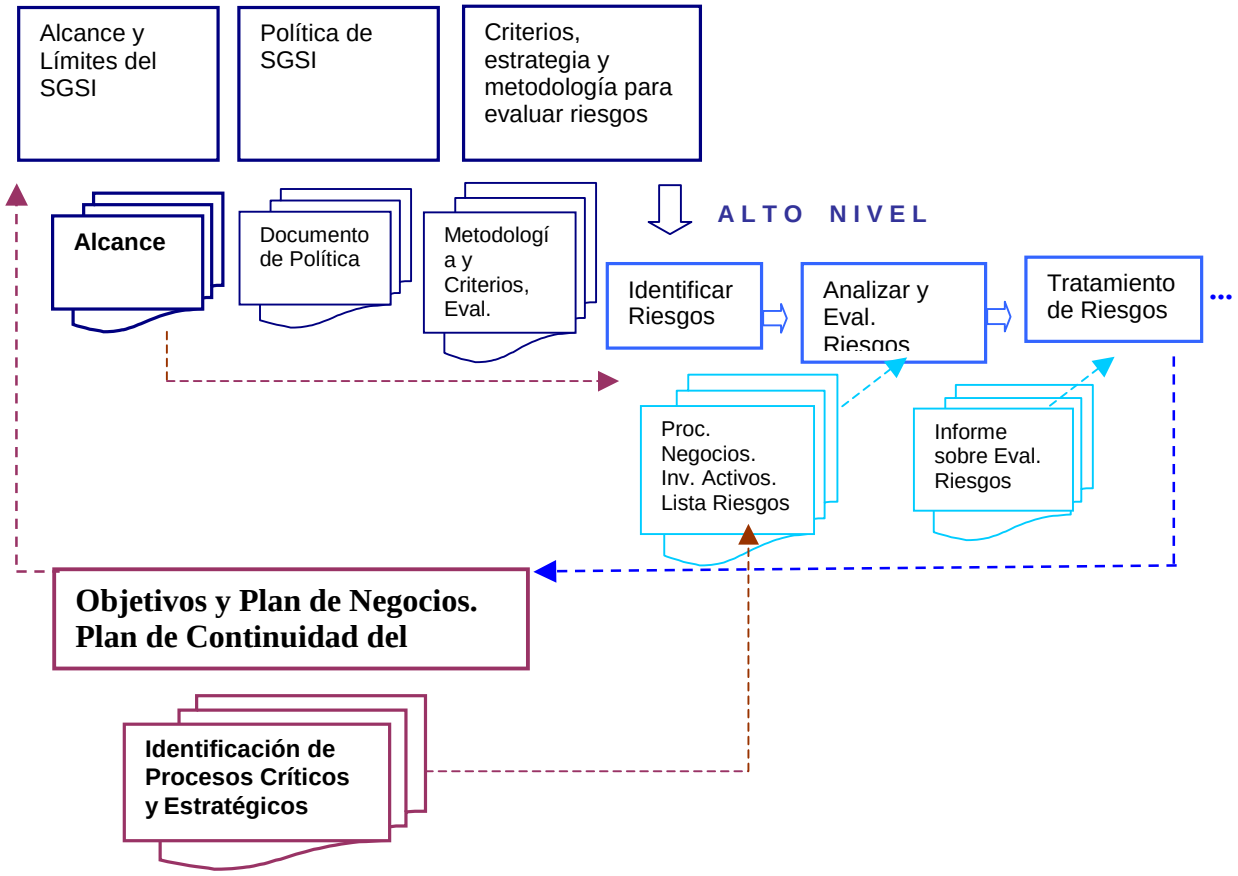


Figura 3.16 – Redefinición del Alcance del SGSI en función del Plan de Continuidad del negocio

Si además consideramos que el grado de dependencia entre activos puede variar con el tratamiento de riesgos (controles, contingencias, redundancias) y por ende la criticidad de los mismos, tendremos:

Procesos Críticos/ Alcance y
Dependencia entre Activos/ Contingencias* ⟹ *Activos Críticos*

Notación: " / " denota " dado "

En la Figura 3.17, representamos los procesos con elipses y los activos como rectángulos, y la relación P depende de A como P → A.
Para la dependencia entre activos, debe considerarse el grado de dependencia o criticidad de esa dependencia. El cual representamos con una flecha punteada y con el porcentaje de dependencia como atributo. La Figura 3.17 muestra además que el activo A depende parcialmente (de la seguridad) de otros dos activos B o C, los cuales podrían ser por ejemplo activos sustitutos o equivalentes en un grafo donde el atributo de dependencia considerado es la disponibilidad.

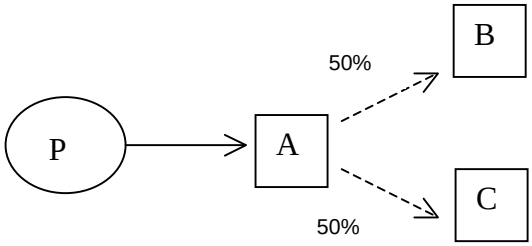


Figura 3.17 – Notación y Semántica de Grafo de Dependencias

En las secciones "3.2.8.4.5.4. Grafo Valuado de Dependencias" y "3.2.8.4.5.5 Cualidades del Grafo Valuado de Dependencias" se formalizan y generalizan estos conceptos aquí introducidos y se profundiza en las posibilidades de esta herramienta gráfica que proponemos para el análisis y estimación de riesgos.

Salida:

Un relevamiento de los activos de la Organización comprendidos en el alcance del SGSI. Cada uno con su correspondiente dueño / responsable.

3.2.8.4.4.3 Identificación de Amenazas

Entrada:

a. Incidentes reportados, estadísticas locales (CSIRT / CERT).
b. Reportes específicos, de organizaciones reconocidas, de amenazas para el sector / industria.
c. Estadísticas de amenazas globales.
d. Informes y aportes de los "dueños de los activos" (de información).

e. Especialistas y técnicos del dominio de aplicación.
f. Especialistas en Seguridad de la Información.

Acción:

Debe tenerse un mapa o catálogo de amenazas bien identificado y lo más completo posible, considerando, tanto amenazas internas como externas, factores humanos y acciones deliberadas como accidentales, ambientales, etc.

Es muy importante referirse a catálogos conocidos y estadísticas globales propias del dominio de aplicación, así como aquellas que afectan y se detectaron en otras empresas comparables y por supuesto estadísticas propias y detectadas a nivel nacional.
Otra fuente de detección de amenazas para la empresa subordinada, puede ser las identificadas por la empresa principal o amenazas relacionadas que potencialmente también lo sean para la empresa en cuestión.

Deben clasificarse las amenazas según su tipo (acciones no autorizadas, daño físico, fallas técnicas, etc.).
Es importante mantener actualizado este escenario de amenazas debido a que las mismas muchas veces son variantes de otras anteriores y surgen nuevas.

También es importante conocer la motivación en el caso de las amenazas deliberadas llevadas a cabo por acciones humanas.
Otro elemento a tener en cuenta que puede resultar de gran ayuda para la comprensión de ese mapa de amenazas son los vectores o vías por las que finalmente se llevan a cabo.

Tanto la motivación y las vías de concreción de las mismas (vectores) pueden ser el foco para las acciones preventivas y establecimiento de controles (o sanciones) que combatan o mitiguen el impacto no deseado o la concreción de la amenaza.

A los efectos de detectar amenazas y riesgos en los servicios y activos de información, puede resultar de importancia contar con árboles de ataque que a partir de vulnerabilidades y amenazas sobre un activo, permitan inferir y descubrir amenazas sobre los servicios y activos que dependen del primero.

Salida:

Una lista de amenazas reales, clasificadas según su tipo y origen.

3.2.8.4.4.4 Identificación de Controles

Entrada:

a. Documentación de los controles existentes.
b. Documentación de la Implementación del Plan de Tratamiento de Riesgos.

Acción:

A los efectos de no caer en costos e inversiones de tiempo y trabajo en controles que se superpongan con otros existentes (ineficiencia operativa), es importante conocer el grado de cobertura actual de los mismos. Para esto pueden ser útiles tanto los informes de implementación de controles de planes de tratamiento de riesgos anteriores así como informes de auditoría. Deben considerarse tanto los controles existentes como aquellos incluidos en el Plan de Tratamiento de Riesgos.

También es importante armonizar los planes de tratamiento de riesgos de la empresa subordinada con los de la empresa principal relacionada, en aquellos riesgos que así lo permitan, o corresponda. Esto permite tener todos los elementos para una mejor evaluación de los riesgos reales y una utilización más racional de las inversiones en seguridad estableciendo prioridades con mayor certeza.

El campo de acción de los controles, es potencialmente el escenario de riesgo constituido por las vulnerabilidades existentes, las amenazas detectadas y el impacto que tendrían sobre los activos en caso de efectivizarse.
Por lo tanto, pueden y deben establecerse controles tendientes a:

- Minimizar las vulnerabilidades
- Eliminar o reducir / inhibir las amenazas
- Eliminar, mitigar o transferir el impacto sobre los activos.

Algunos recursos a tener en cuenta para esta actividad son:

- Informes y recomendaciones del Departamento de Jurídica, respecto a la legislación vigente aplicable.
- Informes de Auditoría de la propia empresa.
- Informes o la percepción de los propios usuarios involucrados y el "dueño" de la información (especialistas del dominio). (Grado de uso y efectividad de los controles). Observaciones *on-site* de los controles físicos por ejemplo.
- Informes de especialistas en seguridad de la información. (Grado de uso y efectividad de los controles). Estadísticas.
- Análisis de vulnerabilidades y amenazas y su grado de impacto en los activos.
- Informes de Auditorías previas de la empresa principal.
- Plan de Tratamiento de Riesgos de la empresa subordinada y de la empresa principal.
- Informe de Controles implementados (en ambas empresas)

Salida:

Un escenario claro de los controles existentes y los planificados, su grado de implementación, uso y efectividad.

Aspectos Humanos, Comerciales y de manejo de la información confidencial:

A continuación mencionamos algunos aspectos no tecnológicos que también deben ser atendidos al momento de identificar y establecer controles:

- Información del lanzamiento de nuevos productos.
- Gestión de permisos y manejo de las claves de acceso a información privilegiada (infraestructura, futuros proyectos, información técnica, información confidencial de interés para la competencia), considerando aún los funcionarios que eventualmente dejan de pertenecer a la empresa.
- Gestión de la información confidencial o privada / reservada.
- Datos privados, de la empresa y de clientes.
- Acceso Físico.
- Relaciones contractuales, comerciales y laborales.

3.2.8.4.4.5 Identificación de Vulnerabilidades

Entrada:

a. Informes internos de vulnerabilidades.
b. Reportes y repositorios de vulnerabilidades de sitios y organizaciones especializadas (Internet).
c. Listas de vulnerabilidades conocidas (ej. NIST I-CAT)
d. Reportes de incidentes (locales o de otras empresas). CSIRT / CERT.
e. Informes de auditorías previas.
f. Informe de vulnerabilidades de la empresa principal en lo que corresponda (por ej. infraestructura).
g. Informes y noticias de seguridad de fabricantes y firmas especializadas.
h. Listas de distribución y Foros de seguridad
i. *Checklists* de requerimientos de seguridad
j. Evaluaciones previas y *tests* (prediseñados) de seguridad
k. Análisis de riesgos realizados previamente

Acción:

Las vulnerabilidades tienen su importancia relativa en función de la existencia de amenazas reales (factibles), que puedan explotarla, y el impacto que eso pueda generar para la organización.
Así mismo deben considerarse los controles existentes (y planificados) que pueden mitigar o eliminar dicha vulnerabilidad.
Si se detectan vulnerabilidades que no tienen una amenaza conocida factible, deben igualmente documentarse, porque el escenario (y las amenazas) podrían cambiar.

Deben identificarse las vulnerabilidades no sólo referentes a la tecnología, dispositivos y protocolos de comunicaciones utilizados, sino que la cobertura debe ser de todas las áreas:

- Organización
- Procesos y Procedimientos (Organización & Métodos, operaciones)
- Recursos Humanos
- Condiciones ambientales y físicas.
- Aspectos técnicos (configuración, infraestructura: hardware, software, comunicaciones, etc.)
- Relaciones y dependencias de terceros.

Algunas herramientas útiles para la detección de vulnerabilidades son:

- Herramientas automáticas de *scanning* y detección de vulnerabilidades (en general conocidas).
- Test de penetración (*Hacking* ético)
- Auditorías de Evaluación de Seguridad.
- Revisión de código.
- Encuestas y observaciones en el lugar (inspecciones físicas).
- Reportes de incidentes.
- Grafos o árboles de vulnerabilidades [90], incluyendo como son afectados los servicios y/o activos de información, aún para las dependencias entre la empresa principal y la subordinada. Esto puede ser de utilidad tanto para detectar vulnerabilidades en los servicios que surgen de analizar los activos que lo soportan e incluso pueden alertar de una vulnerabilidad que surge de un factor que no está dentro del dominio de la empresa subordinada.

Salida:

Una lista de vulnerabilidades de los activos, considerando las amenazas y controles existentes. Deben incluirse las vulnerabilidades para las que no se identifique en principio una amenaza real, indicando esta condición.

3.2.8.4.4.6 Identificación de Consecuencias

Entrada:

La identificación de los procesos de negocio (clasificados según criticidad), los activos relacionados, las amenazas y vulnerabilidades asociadas a los activos y en lo posible con su grado de relevancia asociado.

Acción:

Identificar el impacto sobre los activos que supondría la concreción de esas amenazas, en términos de pérdida de confidencialidad, integridad y/o disponibilidad.
La concreción de alguna de esas amenazas explotando una o más vulnerabilidades se identificará como un potencial incidente (escenario de incidente).

Salida:

Una lista de potenciales incidentes (o escenarios) con sus impactos asociados.

3.2.8.4.5 Estimación de Riesgos

En esta sección, se aplica el enfoque estratégico y metodológico definido para la estimación de riesgos que como se vio consta de dos niveles.

Posteriormente se definen una serie de herramientas metodológicas que son de utilidad para la Estimación y Evaluación de Riesgos, ellas son:

- Valoración de Activos
- Dependencias entre Activos
- Grafo Valuado de Dependencias
- Subgrafos de Valuación.
- Estimación del impacto de los riesgos
- Estimación de la probabilidad de ocurrencia
- Estimación del nivel de los riesgos

Finalmente se completa la sección con la estimación de Impacto, Ocurrencia y Nivel de Riesgo respectivamente.

Al igual que en la sección de "Identificación de Riesgos", indicaremos en forma general, quienes deben participar en estas actividades de "Estimación de Riesgos", a los efectos de no ser reiterativos, y luego donde corresponda, se formalizará la *Entrada, Acción* y *Salida* de cada actividad o proceso.

Quienes deberían participar:

a. Gerencias de línea
b. Equipo de Planeamiento de Seguridad de la Información
c. Comité de Seguridad de la Información (estimación de alto nivel).
d. Analista de Riesgos.
e. Dirección y Gerencia General (en caso de ser necesario)

3.2.8.4.5.1 Estrategia de Estimación

Se presentan a continuación los dos niveles definidos para el análisis y evaluación de riesgos. Es decir, un alto nivel para las definiciones y detecciones "macro" y un bajo nivel cuando se requiera mayor detalle.

Estimación de Alto Nivel:

Para el alto nivel de la estimación de riesgos, dada su naturaleza, se recomienda una estrategia de estimación cualitativa basado en que:

- En general la empresa conoce cuales son sus procesos críticos, y por lo pronto, ellos serán el foco de atención en cuanto a las vulnerabilidades y amenazas de los cuales la empresa se debe proteger. Ellos son los de mayor valor para el negocio y por lo tanto si son afectados o se los deja no disponibles, el impacto sería (muy) alto.
- La estimación precisa saber que tan alto es el impacto y el riesgo, puede ser irrelavante en el sentido que las medidas de protección, seguramente estén justificadas y el costo muy probablemente será inferior (en ordenes de magnitud).
- Muy probablemente sea muy dificil y costoso obtener una estimación certera o precisa en términos cuantitativos, sin bajar de nivel, lo que supone una mayor dedicación de tiempo y recursos.

Cuando se requiera, y se considere conveniente, para la evaluación detallada o específica, a niveles más técnicos, pueden aplicarse estrategias de valoración combinadas, cuantitativas y cualitativas, según lo amerite y sea posible y útil realizarlo. Por ejemplo para justificar o decidir una inversión en medidas preventivas.

Análisis detallado:

Este análisis, más profundo, involucra un mayor nivel de detalle de las amenazas, los activos involucrados y sus vulnerabilidades. Por este motivo es más exigente en cuanto a los recursos que insume, por ejemplo el tiempo y los profesionales involucrados.

Una vez detectados los dominios y aplicaciones o procesos de mayor valor para la empresa, incluyendo aquellos críticos, es en ellos que conviene profundizar y donde la relación costo / beneficio arroja mejores resultados.

En el Anexo E de la norma "*ISO/IEC 27005:2008 - Information technology - Security techniques -Information security risk management*", el cual tiene carácter informativo se presentan diferentes técnicas y matrices para la evaluación de niveles de riesgo.

Por otra parte en [52] se presentan una serie de métodos y herramientas para la evaluación y estimación de riesgos (*RM/RA Methods y RM/RA Tools*). Entre ellas destacamos Magerit [3], Mehari [48] y CRAMM [65].

Como referencia principal para este trabajo, se consideró especialmente la norma ISO/IEC 27.005, justamente por estar estrechamente alineado con la norma ISO/IEC 27.001 y ser parte de la serie ISO/IEC 27.000.

No obstante, las diferentes metodologías se complementan, y es posible combinar enfoques e incorporar beneficios y aportes de otras sin salirse de la línea elegida, que justamente no especifica detalles de implementación porque no es su propósito.

Mehari [48] y CRAMM [65] soportan esta estrategia combinada de análisis y evaluación de riesgos [52]. En Mehari [48] en particular, se especifica un "Módulo de Evaluación Rápida" y un "Módulo de Evaluación detallada". El primero justamente es para tener una revisión rápida del estado de la seguridad y descubrir las carencias y debilidades más importantes, y el segundo, más detallado y preciso para analizar con mayores datos en forma concreta los riesgos más importantes y su valoración.

Creemos que este último enfoque es muy adecuado y está alineado con la estrategia elegida de análisis y evaluación progresiva de riesgos de la metodología, en el nivel de detalle y en el alcance, desde el nivel estratégico primero, al nivel operativo luego.

En [3] se presenta un Modelo Cuantitativo, que, debido al esfuerzo que requiere, y su costo asociado, entendemos es conveniente utilizarlo para activos y riesgos específicos que así lo ameriten.

3.2.8.4.5.2 Valoración o valuación de activos

La valoración de activos, es fundamental para cualquier plan de seguridad de la información. Como plan que es, requerirá de recursos, y cuanto más fundamentado esté la importancia de los activos que se esté protegiendo, será más fácil justificar las inversiones requeridas en seguridad y también las decisiones tendrán más elementos para basarse en una relación costo / beneficio. No obstante, no es sencillo obtener un retorno de la inversión (ROI) para la seguridad de la información, ya que debe considerar estimaciones sobre el riesgo evitable que no siempre son fáciles de realizar (al menos a priori), además de aspectos financieros de y valor actual neto (VAN) del retorno de una inversión a largo plazo propios de un proyecto de inversión.
La valuación de activos puede ser muy simple o compleja dependiendo del tipo de activo.
Por ejemplo, para algunos activos puede considerarse simplemente el valor de reposición como valor del mismo. En otros casos deben considerarse otros costos, indirectos como por ejemplo "costo de oportunidad", "lucro cesante", etc. Para otros puede tener que asignarse un valor subjetivo o abstracto difícil de cuantificar como por ejemplo la pérdida de imagen institucional. También pueden intervenir aspectos financieros que hagan más compleja aún la valuación. Por ejemplo el valor de la pérdida de confidencialidad del lanzamiento de un nuevo producto / proyecto o de datos privados de clientes.

Por este motivo, no siempre es viable ni conveniente, intentar una valuación cuantitativa de los activos (ni siquiera los críticos), sino que a veces es más viable y conveniente utilizar una valoración cualitativa.
Una clasificación probable y valoración cualitativa típica, tal como lo establece la norma ISO/IEC 27.005 es:
Irrelevante, Muy Bajo, Bajo, Medio, Alto, Muy Alto y Crítico.

En [3] se establece un mapeo entre una escala de niveles cualitativos de riesgo como la anterior y un ranking de 1 a 10 a los efectos de tener mayor granularidad al momento de calificar y eventualmente comparar numéricamente los riesgos. Una correspondencia análoga puede aplicarse a la escala anterior.

Sin embargo, atendiendo al tipo de Organización, puede ser más adecuado una primer clasificación, de alto nivel, en Bajo, Medio, Alto y Crítico, para eventualmente hacer la escala más fina en etapas posteriores.

Para la valuación o valoración de activos y (sub)procesos, al igual que en la evaluación de riesgos (para la estimación del impacto) una estrategia puede ser planteárselo en términos de cuánto pierde la organización por no poder cumplir con los objetivos de control (ISO/IEC 27.002). Deben considerarse en sentido amplio aspectos tangibles y no tangibles, y por lo tanto deben considerarse los impactos en los siguientes valores / atributos relativos a la seguridad de la información:

- Correctitud / Precisión y Confiabilidad de la información (Integridad).
- Disponibilidad y Oportunidad de la información.
- Confidencialidad de la información.
- Continuidad del negocio.
- Seguridad, detección y prevención de fraudes.

- Cumplir con dictámenes, reglamentaciones, contratos y niveles de servicio comprometidos (SLAs).
- Manejo de operaciones (AAA, cobros, pagos, compras, servicios, inventarios, etc.)
- Impacto económico-financiero y estratégico-empresarial,
- Flujo de fondos. Rentabilidad.
- Eficiencia operativa.
- Pérdida de competitividad.
- Imagen y prestigio empresarial.
- Costos legales.
- Costos de recuperación del incidente.
- Costos indirectos (de oportunidad, lucro cesante, etc.).
- Otros.

Debe tenerse presente, que los valores asignados pueden cambiar con el tiempo dada su naturaleza, por ejemplo información que es reservada hasta que se decide hacerse pública. Otro ejemplo es el valor de los *logs* con el transcurso del tiempo.
En ese caso, debe revisarse periódicamente esta valoración ya que no es estática, y de no hacerse se estaría incurriendo en un gasto debido a esta sobrevaloración no justificada.

Otro aspecto a tener en cuenta es el grado de dependencia de los procesos de negocio de los activos y de otros (sub)procesos.

3.2.8.4.5.3 Dependencias entre activos

Nos interesará representar la dependencia de seguridad de los activos de información entre sí.

Se define: *A depende directamente de B* y se denota: $A \rightarrow B$, cuando la seguridad requerida del activo A, requiere a su vez de ciertos niveles en los atributos ([14]) de seguridad del activo B.
Observar que la dependencia es sobre las condiciones de seguridad y no únicamente sobre aspectos funcionales. Si un activo se necesita para elaborar o ejecutar otro activo pero la seguridad del primero no afecta en nada ni pone en riesgo los niveles de seguridad requeridos para el segundo, esa dependencia es sólo funcional y no será tal en la relación de dependencia que estamos considerando (de compromiso de seguridad).

La relación de dependencia es transitiva, y definimos su clausura transitiva (denotada por '$\Rightarrow$') como:

$$A \Rightarrow C \ \textit{sii} \begin{cases} A \rightarrow C, \text{ o bien} \\ \exists\, B/\ (A \Rightarrow B) \wedge (B \rightarrow C) \end{cases}$$

A depende de C sí y sólo si: o bien depende directamente o bien existe algún activo B tal que A depende (eventualmente por transitividad) de B y a su vez B depende directamente de C.

[14] Confidencialidad, Integridad, Disponibilidad, Autenticación, etc.

Conceptualmente, a los efectos de valorar los activos y cómo inciden sus dependencias de seguridad, nos interesará identificar dos aspectos:

- Los activos de los cuales en mayor o menor medida depende (parcial o totalmente) la seguridad de un número significativo de activos.
- Los activos de cuya seguridad dependen otros activos aún indirectamente a través de una cadena de dependencias (en forma transitiva).

En [3] se presentan conceptos similares de dependencias entre activos. Se presenta allí, un modelo cualitativo y uno cuantitativo, y en cuanto a la valuación de activos, se presenta el concepto de valor acumulado y se define con una fórmula en cada uno de los modelos respectivamente.
Sin embargo, en el modelo cualitativo para el cálculo de valor acumulado no se considera el grado de dependencia de un activo, es decir, la posibilidad de establecer dependencias parciales donde la violación de seguridad de un activo compromete la seguridad del otro pero no es determinante (en cuyo caso la dependencia sería total).
Se considera en cambio, la dependencia a los efectos de propagar el valor o calificación del activo que depende del que se está considerando como si la misma fuera siempre total, es decir, se establece un máximo entre el valor de ambos. Esto de hecho, no siempre es así, y por lo tanto este criterio puede sobredimensionar la valoración asignada a la dependencia y por ende al activo del cual se depende (quizás de forma parcial).
El modelo cuantitativo, si bien considera un grado de dependencia, es decir la posibilidad de asignar una dependencia parcial y no total, no es siempre el modelo más adecuado para ser aplicado. Esto se debe a las dificultades que puede presentar una estimación cuantitativa con algunos activos y el esfuerzo para realizarlo con un nivel de certeza adecuado, atendiendo a factores de diversa índole como ser: aspectos financieros como la actualización de un valor futuro, la propia incertidumbre sobre valores intangibles sobre los que quizás no se tienen referencias válidas, etc.

Buscamos definir para nuestra metodología, un mecanismo de ajuste de valuación de activos, que nos permita en forma conjunta:

- La utilización de valuación cualitativa, además de la cuantitativa según sea más adecuado para el activo y análisis en consideración.
- Considerar el grado de dependencia de la seguridad de un activo respecto de la de otros de los cuales depende.
- Establecer un algoritmo de ajuste de la valuación, en función de las estimaciones realizadas y que considere las cadenas de dependencias entre activos, que sirva además como referencia primaria de análisis para una posterior revisión y ajuste, donde intervengan otros factores subjetivos y humanos, eventualmente no automatizados.

3.2.8.4.5.4 Grafo Valuado de Dependencias

Motivados en los conceptos presentados en la sección " *3.2.8.4.4.2 Identificación de Activos"* y "3.2.8.4.5.3 Dependencias entre activos" definiremos en esta sección el Grafo Valuado de Dependencias, que utilizaremos para establecer el valor (cuantitativo o cualitativo) de los activos (incluyendo procesos) teniendo en cuenta a su vez, el grado de dependencia entre los mismos.

Los Nodos: Representarán los procesos y (sub)procesos de negocios, y los activos en general. Para una mejor visualización se notarán los procesos con forma de elipse y los activos en forma de rectángulo.
Los nodos tendrán un valor asignado en lo que refiere a confidencialidad , integridad y disponibilidad: VC, VI y VD respectivamente.

Los Arcos: denotarán la relación de dependencia de la seguridad. Si el activo A_1 depende del activo A_2, entonces existirá un arco en la dirección A_1A_2 (entrante en A_2). Estos arcos estarán además etiquetados por el grado de dependencia entre sus nodos extremos.

Formalmente definimos G (V,R,g) de la siguiente manera:

Sea ***V***: el conjunto de Activos de la Organización. Activos en su acepción más amplia, es decir, todo aquello que tenga valor para la misma, como se define en la norma ISO/IEC 13335-1: 2004. En particular, destacamos que incluye también a los procesos.

Cada nodo, tendrá un *valor, más específicamente un atributo multivalorado* representativo de que tan relevante es para el proceso de negocio, o en general, para el negocio, en términos de Confidencialidad (C), Integridad (I) y Disponibilidad (D): VC, VI y VD respectivamente. En la Figura 3.18 se ilustra el concepto con un ejemplo.

Sea ***R: VxV*** que definimos de la siguiente manera:

i) R es irreflexiva, es decir dados i, j/ $(V_i,V_j) \in R$ entonces $i \neq j$.
ii) R es transitiva, es decir, dados i, j, h/ $(V_i,V_j) \in R$ y $(V_j,V_h) \in R$ entonces $(V_i,V_h) \in R$.
iii) $(V_i,V_j) \in R$ si la seguridad requerida para V_i depende de la seguridad requerida de V_j. Dicho de otra manera, si un incidente que vulnere la seguridad de V_j vulnera también la seguridad de V_i.

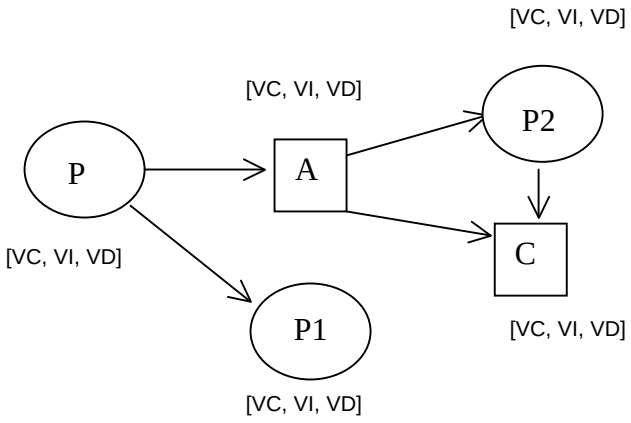


Figura 3.18 –Grafo Valuado de Dependencias (C, I, D)

Para simplificar la notación, y teniendo presente la terna [VC, VI, VD], en adelante, se generalizará como Val(V_i) el valor del nodo V_i, sabiendo que es una terna, y asumiendo el valor del componente que corresponda si el contexto refiere particularmente a uno de los tres atributos: Confidencialidad, Integridad o Disponibilidad. Tal como se mencionó en la sección "*3.2.8.4.5.2 Valoración o Valuación de activos*" esta valoración puede ser cuantitativa o cualitativa.

Resta por ver, como representa, a nivel de la semántica del Grafo de Dependencias, cuando un recurso, llámese (sub)proceso o activo ([15]), depende parcialmente de otro/s.
En ese caso, representaremos gráficamente la dependencia con un arco punteado indicando el ***grado de dependencia (g)*** con una etiqueta sobre el arco (con un coeficiente representativo del porcentaje). Tendremos entonces un Grafo que además de tener un valor asociado en cada uno de sus nodos, es ponderado en sus arcos.

El grado de dependencia debe determinarse en función de cuanto compromete la seguridad del activo dado que se viole la seguridad del activo del cual depende. Por lo tanto el grado de dependencia será una terna (g_c, g_i, g_d) correspondientes al grado de dependencia relevante para alguno de los siguientes atributos de seguridad: Confidencialidad (C), Integridad (I) y Disponibilidad (D) respectivamente.

Definimos el **<u>grado de dependencia (g)</u>** como:

$$grado_{<atributo>}(A \rightarrow B) = \begin{cases} 0 \text{ si la seguridad } (^*) \text{ de A no depende, ni siquiera parcialmente, de la seguridad de B.} \\ 1 \text{ si la seguridad de A depende totalmente de la seguridad de B y la violación de seguridad de B implica la violación de la seguridad de A (respecto del <atributo>).} \\ x \ / \ 0 < x < 1, \text{ es decir, un valor intermedio entre 0 y 1 si la dependencia es parcial. Cuanto mayor sea el grado de dependencia respecto del <atributo>, mayor es la dependencia del activo en cuestión, o dicho de otra manera, el activo es más sensible a la seguridad (según <atributo>) del activo del cual depende.} \end{cases}$$

NOTA(*): En todos los casos donde dice 'seguridad' se refiere a la seguridad respecto del <*atributo*>, es decir C, I, o D, siendo sus grados g_c, g_i, o g_d respectivamente.

Al grafo **G = (V, R, g)** lo llamaremos **<u>Grafo Valuado de Dependencias</u>**, el cual además de tener el atributo multivalorado de seguridad asociado a cada uno de sus nodos [VC, VI, VD], tiene sus arcos ponderados (o etiquetados) con el grado de dependencia correspondiente (g_c, g_i, g_d).

Por claridad en la notación, en adelante, notaremos genéricamente como g el vector (g_c, g_i, g_d), teniendo presente que se trata de una terna con sus respectivos coeficientes. Adicionalmente se usarán los subíndices de cada activo en el grado como se muestra en la Figura 3.19.

[15] Se generaliza a los efectos de sintetizar, si es un proceso se representará como una elipse y si es un activo como un rectángulo, tal como se vio en la Figura 3.17.

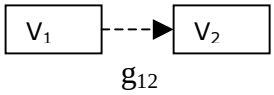


Figura 3.19 –Dependencia parcial

Si bien puede ser más claro visualizar el concepto de grado de dependencia para el atributo: Disponibilidad, por ejemplo ante la presencia de alternativas en situaciones contingentes, sin embargo la Confidencialidad e Integridad son valores a preservar en términos absolutos, debe considerarse que el grado de dependencia en estos dos atributos, puede referirse a la mayor vulnerabilidad de un activo - en ese atributo de seguridad - dado que se ha vulnerado la del activo del cual depende. Si consideramos un escenario donde se aplica seguridad en profundidad y por lo tanto controles parcialmente redundantes, también tendremos una dependencia parcial en términos de Confidencialidad e Integridad.

Un caso particular de dependencia parcial, para el caso de Disponibilidad, es la de un proceso / activo que depende de otros (n) indistintamente. Para ejemplificar, sea el recurso A que depende de la preservación de la seguridad (en este caso disponibilidad) de uno de estos dos: B o C. Representamos el "OR" como se ilustra en la Figura 3.20. En la medida que se cuente con ambos activos B y C podemos considerarlo como una alternativa de contingencia y en ese caso la criticidad de cualquiera de ellos es menor para el proceso / activo A. (50% en el caso que sean dos sustitutos equivalentes, o generalizando 100/n % si se trata de n sustitutos)

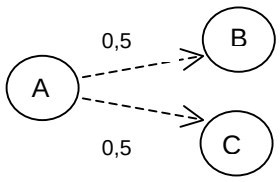


Figura 3.20 – Dependencia con dos alternativas

Es de interés considerar y detectar tres tipos de situaciones para su análisis:

a) Aquellos activos de información que concentran dependencias de un número importante de activos.
b) Las cadenas de dependencias de seguridad de los activos, que pueden afectar el valor de la seguridad de un activo, más que por el valor que tiene en sí mismo, por el valor que tienen aquellos activos que dependen del primero.
c) Considerar las dependencias interempresariales, las cuales pueden condicionar la valoración de activos, y también de riesgos.

Estas consideraciones, que son ilustradas en la Figura 3.21, deberían ser tenidas en cuenta por una herramienta de software que se utilice para la valoración de activos y estimación de riesgos. Una funcionalidad útil para esta actividad, es visualizar o generar (con la asistencia de software) un grafo de dependencias y valoración de activos que permita además de una ayuda

visual, aplicar algoritmos sobre grafos, atendiendo a las particularidades y cualidades del Grafo de referencia. (ver Anexo G)
La misma debería asistir en la identificación o detección de estos casos, y proponer un ajuste para la valoración de activos que pueda servir de <*entrada*> para una eventual revisión y/o ajuste por los profesionales analistas / especialistas en valoración (de activos y de riesgos si corresponde).

Si bien los *ítems a)* y *b)* no refieren a situaciones particulares propias de la naturaleza estructural del grupo empresarial jerárquico, lo explicitamos aquí como situaciones de interés para el análisis, que además en el caso de la consideración de las cadenas de dependencias (*ítem b*) se ven potenciadas en el caso que involucre activos de la empresa principal y la subordinada, es decir dependencias interempresariales (‘*ítem c*’).

Para el *ítem a)* podemos utilizar el semigrado exterior (o grado saliente) y semigrado interior (o grado entrante) de un nodo, conceptos de Teoría de Grafos que recordamos a continuación. [102][104]

El semigrado exterior de un nodo: *semigdoext(V_i)* se define como el número de arcos salientes del mismo es decir el número de arcos (V_i, V_j) en R $\forall$ $V_j \in V$. Análogamente, el semigrado interior: *semigdoint(V_i)* es el número de arcos entrantes o incidentes al mismo, es decir el número de arcos (V_h, V_i) en R $\forall$ $V_h \in V$.
En la Figura 3.18, *semigdoint* (A) = 1, *semigdoext* (A) = 2.

Cuanto mayor es el semigrado interior de un nodo, es mayor la cantidad de los (sub)procesos y/o activos cuya seguridad depende de la seguridad del nodo en cuestión. Esa debería ser una propiedad a considerar junto con el valor intrínseco o aporte directo al negocio de cada activo.

Por otra parte, cuanto mayor es su semigrado exterior, mayor es el número de activos y subprocesos de los cuales su seguridad depende. Este dato puede ser útil al momento de analizar eficiencia operativa, riesgos y planes de continuidad del negocio, así como en la fase de tratamiento de riesgos. En la medida que no se cuente con uno de los activos requeridos, es relativo el beneficio de los controles o salvaguardas / contingencias que se hayan definido sobre los otros activos, ya que el proceso / activo requiere (depende) de todos ellos para preservar su valor (de seguridad). Dicho de otra manera, no se obtiene el nivel de seguridad (beneficio) esperado con respecto a la inversión (costo) realizada en los otros controles, al menos en lo que refiere al proceso o activo en cuestión.

Para el caso de las cadenas de seguridad (‘*ítem b*’), o cómo condiciona el valor de la seguridad de un activo a otros es necesario formalizar algunos conceptos, lo cual es realizado en la siguiente sección: *“3.2.8.4.5.5 Cualidades del Grafo Valuado de Dependencias”*

Por otra parte, el Grafo o un subgrafo inducido por un conjunto de activos* puede recibir una calificación / valoración heredada por parte de la empresa madre del grupo empresarial, como resultado de su propio SGSI, y en particular: la valoración de activos y riesgos. En ese sentido, estos valores, pueden funcionar como mínimo aceptable, o podrán ser ponderados por la empresa que nos compete, esto previamente establecido en función de sus políticas y relaciones institucionales.

Es decir, como se muestra en la Figura 3.21, pueden darse dependencias interempresariales de seguridad (‘*ítem c*’) entre un proceso / activo de la empresa principal y un proceso / activo de la empresa subordinada y viceversa (en cualquiera de los sentidos).

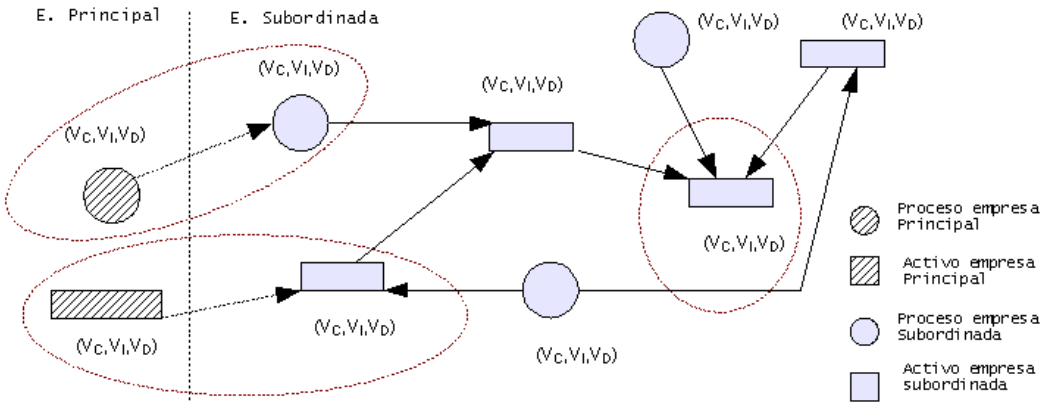


Figura 3.21 – Grafo valuado de dependencias multiempresa

Una dependencia identificada desde la empresa principal hacia la subordinada, como se observa en la Figura 3.21 puede establecer una cota inferior en la valoración del activo de la segunda, más allá de la valoración para su propio negocio.

Una vez asignado un valor primario de los procesos y activos, es necesario una revisión de los mismos para ajustar posibles subestimaciones de activos o procesos así como posibles sobrevaloraciones. Observar que esta revisión es parte del método y es diferente a la revisión periódica por eventuales cambios de escenario o del valor asignado. En este caso se debe a ajustes debido a la dependencia y valor asignados a otros activos.

Sobre el grafo de dependencias se pueden identificar las vulnerabilidades y construir así, a partir de un servicio o activo, un grafo de vulnerabilidades, a los efectos de propagar las mismas de un activo de información hacia otros (activos y servicios) que dependen del primero.

3.2.8.4.5.5 Cualidades del Grafo Valuado de Dependencias

Se explicitan a continuación, una serie de características del Grafo Valuado de Dependencias que se demuestran en el Anexo G.

- R define un orden parcial estricto sobre V, es decir, R es irreflexiva y transitiva.
- Como consecuencia, G es un grafo dirigido acíclico (DAG).
- Es un DAG pero no necesariamente un árbol, es decir, de la seguridad de un activo puede depender la seguridad de varios activos ([16]).
- Afirmamos, y demostramos en el Anexo G, que es posible definir un algoritmo de ajuste de la valuación de activos, que considere la relación de dependencia en los atributos de seguridad.

[16] No unicidad de ‘padre’.

Algoritmo de ajuste de valuación de activos

Sea G (V,R,g) un grafo valuado de dependencias, donde g representa el grado de dependencia, es decir, atributo multivaluado de la relación que asigna un valores entre 0 y 1 a terna (g_c, g_i, g_d) de acuerdo a su definición en *"3.2.8.4.5.4 Grafo Valuado de Dependencias*".
Para fijar ideas podemos pensar en términos escalares o de una dimensión ya sea Confidencialidad, Integridad o Disponibilidad. En términos vectoriales es análogo pero debe operarse en dicho sentido.

Afirmamos:

1 - Existe S = [V_0,...,V_i,....V_j...,V_n], un orden topológico de G (V,R,g), es decir si (V_i,V_j) ∈ R entonces i < j. (V_i precede a V_j en el orden topológico)

2 – Es posible definir el siguiente algoritmo de ajuste de la valuación de activos:

∀i desde 0 a n, en S (orden topológico de G (V,R,g)):
∀ V_j ∈ Ady(V_i) con grado de dependencia g_{ij}, o sea *grado*($V_i \rightarrow V_j$) = g_{ij}
Si Val(V_j) < g_{ij} * Val(V_i) ⇒ *Recalcular(Val(V_j), Val(V_i)).*

Cuadro 3.1 – Algoritmo de ajuste de valuación de activos

NOTAS:

i) Un ejemplo del *Recalcular* podría ser redefinir Val(V_j) = gij * Val(V_i) y/o ser reconsiderado por un profesional especialista en valoraciones para el dominio.

ii) Si se utiliza valoración cualitativa, sean por ejemplo sus valores: Val_1, Val_2,..., Val_h,...Val_n, a los efectos de poder operar con los mismos, definimos la siguiente aritmética para el operador '*':

Sea Val_h un valor cualitativo cualquiera, por ejemplo el de Ai, esto es: Val(Ai)=Val_h, definimos:

$$gij * Val_h = \begin{cases} Val_{(trunc\ (h\ x\ gij)\ +\ 1)}, & \text{si } h\ x\ g_{ij} > trunc(h\ x\ g_{ij}) \ (^{17}), \\ Val_{(trunc\ (h\ x\ gij))}, & \text{sino.} \end{cases}$$

Es decir, informalmente y en lenguaje natural, se establece la correspondencia (mapeo) de la secuencia de valores con un rango de naturales, se opera, y luego se hace la correspondencia inversa para obtener el nuevo valor cualitativo.

A los efectos de ilustrar con un ejemplo la motivación del algoritmo definido, analizaremos el caso particular donde la dependencia de la seguridad es total, es decir el 100% (g_{ij} = 1).
Sean V_1 y V_2 dos nodos de G, por claridad y sin pérdida de generalidad supongamos que son dos activos y, como se muestra en la Figura 3.22, A2 es adyacente a A1 según la relación de

[17] trunc: *R* -> N, es la parte entera de *R*.

dependencia, esto es: la seguridad de A1 depende de A2. Supongamos además que depende de forma crítica.

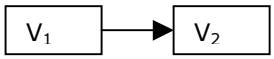


Figura 3.22 – Relación de Dependencia

Si el valor asignado a V_2 es inferior al valor asignado a V_1, la valoración de V_2 debería reverse, ya que probablemente esté subestimado, dado que hay un recurso (proceso o activo) de mayor valor que depende de forma significativa de él.

El algoritmo surge, a partir de esta motivación, generalizando para dependencias parciales e introduciendo por tanto el concepto de grado de dependencia.

Como se muestra en el Anexo G, por ser G = (V, R, g) un grafo dirigido acíclico, existe un orden topológico S.
Esto nos da un orden para hacer una revisión de los activos prioritarios, y analizar que los activos y procesos en los que basa su seguridad no están siendo subestimados.

Es decir:

Sea S = [V_0,...,V_i,....V_j...,V_n] ([18]) un orden topológico de G (V,R,g), esto implica que si (V_i,V_j) $\in$ R entonces i < j. (V_i precede a V_j en el orden topológico).

Podemos recorrer S revisando que Val(Vj) >= g_{ij} * Val(V_i), $\forall$ (V_i,V_j) $\in$ R con i < j.

De no ser así, redefinimos Val(V_j) = g_{ij} * Val(V_i)

Observar que estamos definiendo un mecanismo de revisión y ajuste de las estimaciones, en relación a las estimaciones de los activos superiores o que dependen del activo en consideración, que no sólo nos da un orden en el cual recorrer los activos de información, sino que además una cota inferior del valor de un activo en función de su valor propio y las dependencias.

Un ajuste más fino podría ser:
$Val(V_j) = Max \{ Val(V_j), \Sigma_i^{j-1} \{ Val(V_i) \times gij \}, \forall V_i / V_i \rightarrow V_j \}$

En este caso, se está considerando el hecho de que un activo no sólo es al menos tan relevante como otro activo que depende de él (en función del grado de dependencia), sino que además, cuanto más activos requieran o dependan del activo en consideración, la valoración del mismo será mayor.
Observar que se itera hasta (j-1) en el orden topológico del Grafo, es decir, sólo existen arcos "hacia adelante".

En el caso que se tenga que representar que A depende de (B o C) y de (D o E), para que no sea ambigua la notación, deben introducirse nodos intermedios como se muestra en la Figura 3.23.

[18] 0..n es una reenumeración de los índices en forma creciente, según el orden topológico elegido.

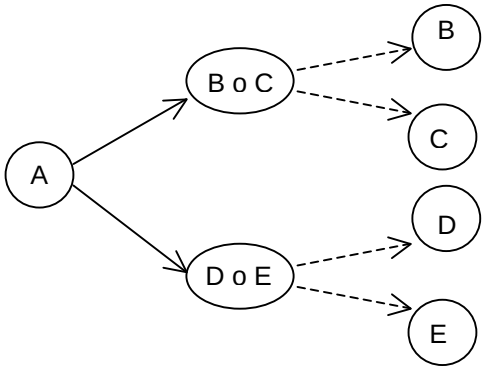


Figura 3.23 – Representación de la conjunción (AND) de disyunciones (OR)

3.2.8.4.5.6 Subgrafos de valuación

Es posible generar un (sub)grafo valuado de dependencias considerando únicamente un aspecto de la seguridad como por ejemplo uno de los siguientes: la confidencialidad, la integridad o la disponibilidad.

Esto es útil para el análisis de riesgos y escenarios, donde se quiera priorizar uno de los aspectos de la seguridad o analizar escenarios hipotéticos (del tipo *"Que pasa si..."*) y así poder analizar los activos críticos desde ese punto de vista y evaluar diferentes alternativas en el caso que haya que optar o comprometer los niveles de seguridad en algún aspecto (debido a los recursos disponibles / costos), priorizando lo que corresponda.

En este caso los nodos tendrán únicamente el valor del atributo elegido (VC, VI o VD respectivamente).

Todo lo expuesto en las secciones anteriores, aplica en este caso pero referido a valores escalares (valor, grado, etc.) y ya no vectoriales.

Para este tipo de análisis sería importante contar con un software que permita generar tales subgrafos o dicho de otra manera, tener diferentes vistas (*o layers*) del Grafo de Valuado de Dependencias.

En la sección *"3.7 Características deseables de Software de Apoyo al SGSI de un grupo empresarial"* se profundiza en este aspecto.

En la Figura 3.24 se ilustra con un ejemplo sencillo, un grafo valuado de dependencias, donde se destaca la dependencia de activos no informáticos como puede ser una impresión, o las personas. Por otro lado se destaca la dependencia de un proceso participando como nodo en un grafo, en el ejemplo: el proceso de respaldos.

3.2.8.4.5.7 Ejemplo Grafo de dependencias

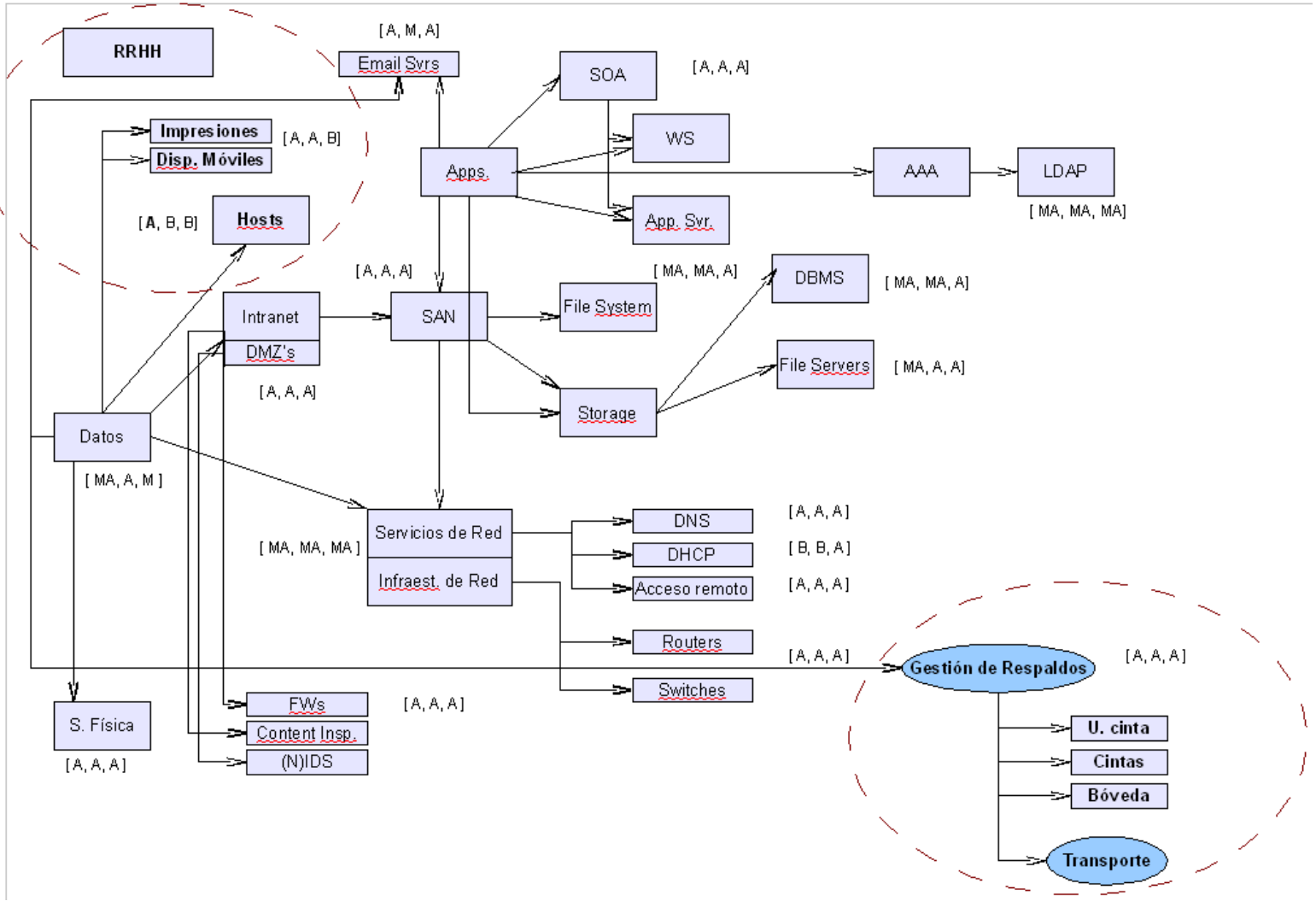


Figura 3.24 – Ejemplo Grafo Valuado de Dependencias (C, I, D)

3.2.8.4.5.8 Estimación del impacto

Para la evaluación de impacto y Tasa de Ocurrencia (Frecuencia) pueden utilizarse Métricas: de la propia Organización, de estudios anteriores (externos o internos), del sector de la industria u organizaciones comparables (rubro, ingresos anuales, clientes) pero en general esto no es de dominio público (suele ser confidencial), a veces consultoras especializadas pueden proveer información específica del área de actividad.

Entrada:

a. Identificación de Vulnerabilidades.
b. Identificación de Controles existentes.
c. Identificación de Amenazas.
d. Valoración de Activos.
e. Grafos y Subgrafos de dependencias.
f. Valoraciones de la Industria, Seguros, etc.
g. Valoraciones de Organizaciones comparables, que sean conocidas.
h. Informes de Consultoras especializadas.
i. Informe de Análisis de Riesgos, incluyendo valoraciones y estimación de impacto, realizada por parte de la empresa principal sobre activos de información y/o procesos que están bajo el dominio de la empresa que se considera en este análisis (la empresa subordinada).

Acción:

Deben considerarse las amenazas en sentido amplio, por ejemplo un ataque que degrade parcialmente los servicios, o el tráfico en la red, se traduce en pérdida de eficiencia operacional y eventualmente de calidad de servicio. También deben tenerse en cuenta otros aspectos no tangibles (pérdida de imagen) y costos indirectos (lucro cesante, de oportunidad, etc.)

Una herramienta útil para la evaluación de riesgos, y en particular la estimación del impacto, es el planteo de escenarios hipotéticos de análisis de impacto del tipo: "*Que pasa si...*". Y como vimos en la sección anterior, para ello también son útiles los subgrafos de valoración vistos en la sección anterior.

En [3] se plantea un Modelo Cuantitativo y uno Cualitativo de estimación del riesgo.
Proponemos utilizar principalmente un Modelo Cualitativo, en particular, para las estimaciones primarias, luego, si se requiere una estimación más precisa para los riesgos considerados críticos podría utilizarse el Modelo Cuantitativo.
En el modelo cualitativo, cada calificación se corresponderá, siempre que sea posible y el tipo de activo e impacto lo admita, con un rango según la cuantificación que pueda estimarse.

Algunos ejemplos y preguntas que pueden ayudar:

- ¿ Que ocurre si el plan estratégico es revelado a la competencia ?

- ¿ Qué valor tiene salir antes que la competencia con un servicio diferenciador de valor agregado original ?
- ¿ Cuánto vale la información estadística y registral o los contratos de mis clientes ? ¿ De mis clientes potenciales ?
- ¿ Como podría ser penalizado legal y comercialmente si es violada la información personal (p. físicas o jurídicas) de mis clientes ?
- ¿ Cuanto me cuesta en pérdida de clientes actuales un incidente importante que se haga público de seguridad que afecte la confiabilidad del servicio a la vista o en la percepción del mercado ? ¿ Y cuánto me cuesta en la pérdida de clientes potenciales (lucro cesante) ?

Además de los costos económicos directos y financieros en lo que puede ser la reparación o restitución del servicio deben considerarse costos indirectos.
Algunos de los indicadores a tener en cuenta pueden ser:

- Número de horas de inactividad o indisponibilidad de los servicios y costo asociado.
- Porcentaje de actividades paralizadas debido al evento
- Como afecta el negocio (esta indisponibilidad).
- Costo de recuperación de los servicios (horas del personal afectado y servicios contratados)
- Tiempo estimado de recuperación
- Transacciones perdidas por hora
- Multas por no lograr lo comprometido en SLAs con clientes.

Otros menos tangibles:

- Pérdida de la imagen y de la calidad del servicio percibido por los clientes
- Eventual pérdida de potenciales clientes
- Pérdida real de clientes actuales
- Daño ocasionados a terceros atribuible a una falla de seguridad de la compañía de la cual no se esté libre de responsabilidad legal ni contractual.
- Costo de oportunidad de realizar la inversión utilizada con otro propósito.

Salida:

Una estimación / valoración para cada uno de los riesgos en caso de concretarse cualquiera de las amenazas identificadas, de acuerdo al criterio y calificaciones de estimación establecidas. Esta valoración puede presentarse en forma tabular, asociando una calificación que puede ser cualitativa para cada amenaza o bien puede agrupar amenazas que generan un riesgo común, y en ese caso se calificará el riesgo como tal.

3.2.8.4.5.9 Estimación de la probabilidad de ocurrencia

Además del impacto de los riesgos, debe analizarse qué tan frecuente ocurren las amenazas y que tan fácil es explotar las vulnerabilidades.

Entrada:

Algunos datos a tener en cuenta para la estimación de probabilidad de ocurrencia:

- Registros Históricos propios.
- Datos estadísticos de Organizaciones similares (Sector de la Industria)
- Datos estadísticos globales.
- Consultoras / Sitios especializados. Asesoramiento y recomendaciones de profesionales de Seguridad de la Información.
- Estadísticas relacionadas, y la experiencia de organizaciones especializadas ya sea de CSIRTs locales o CERTs.
- Informes de análisis resultado de investigación de patrones de comportamiento hostil, por ejemplo resultado de las *Honeynets / Honeypots.*
- Controles existentes (y los planificados) y cómo pueden y/o logran efectivamente mitigar los riesgos / vulnerabilidades o reducir y eliminar amenazas.
- Informes de especialistas y técnicos del dominio de aplicación o dueños de los activos.
- Las vulnerabilidades por separado de cada activo o del conjunto y la configuración de la infraestructura como tal.
- Factores accidentales o ambientales. Estadísticas y previsiones.

Acción:

Es necesario realizar proyecciones o estimaciones de la probabilidad de ocurrencia de los riesgos de forma consistente con los datos históricos, ya sea propios o de otras organizaciones, a nivel nacional y a nivel internacional, y tomar en cuenta la realidad actual. Es decir, proyectar esos datos a la realidad nacional, la específica del sector y en función de las tendencias de las amenazas existentes y potenciales.

También resulta importante conocer otros aspectos no sólo cuantitativos (o estadísticos) sino también cualitativos:

- Para las amenazas deliberadas (humanas): entender su motivación y capacidades, factores dinámicos que requieren revisión crítica periódica, así como los recursos disponibles para los atacantes.
- La percepción de atractivos y vulnerabilidad de determinados activos u organizaciones a los atacantes (*hackers*).
- Observatorios, *Honeynets*, *Honeypots*. Informes especializados, específicos para el sector y/o por región. Justamente, estas técnicas sirven para analizar comportamientos y capacidades de los atacantes a los efectos de mejorar los mecanismos de defensa.

En [3] se propone una posible evaluación de la frecuencia como se muestra en el Cuadro 3.2:

100	muy frecuente a diario
10	frecuente mensualmente
1	Una vez al año
1/10	Poco frecuente, cada varios años

Cuadro 3.2 – Ejemplo de escala para la frecuencia de riesgos

Es decir, a los efectos de establecer la calificación, debe establecerse un criterio que determine la misma en función de datos objetivos, verificables siempre que sea posible, basado en datos históricos y en tendencias sólidas en función de la situación actual y la proyectada.

Salida:

Una tabla con la frecuencia (o calificación de la frecuencia de acuerdo al criterio establecido) estimada de para cada uno de los riesgos identificados, atendiendo a las amenazas identificadas, las vulnerabilidades y los controles existentes.

3.2.8.4.5.10 Estimación del nivel de riesgo

Como se vio en secciones anteriores, un intento de estimación de riesgos cuantitativa, con márgenes estrechos de incertidumbre, puede ser una tarea bastante costosa y no se justifica (salvo raras excepciones). Para el establecimiento del ranking de riesgos y una priorización en la asignación de recursos para su tratamiento, resulta más efectivo y eficiente adoptar estrategias de evaluación cualitativas. Este es el caso que aplica a empresas medianas o grandes donde además intervienen diversas tecnologías, numerosos activos tangibles y no tangibles en términos de infraestructura, procesos, activos lógicos, valor comercial y estratégico, etc.

Entrada:

- Estimación del impacto de los riesgos identificados.
- Estimación de la probabilidad de ocurrencia de los riesgos.

Acción:

Algunos principios básicos que deben tenerse en cuenta y guiar la estimación de niveles de riesgo son:

- ✓ Los requerimientos reales de seguridad de cada activo y proceso. Si un criterio de seguridad es irrelevante para un activo o proceso, no debería ocurrir que por sobreasegurar ese activo / proceso de forma no justificada se le quiten recursos o posibilidades de implementar otros controles más necesarios, ya sea sobre ese activo o sobre otros. Un ejemplo de lo que no se debe hacer sería buscar dotar de confidencialidad a información que de acuerdo a su clasificación puede ser pública. Aquí, algunos controles de encriptación ya sea de almacenamiento como del canal de comunicaciones, podrían resultar excesivos y quizás tener un costo en performance y calidad de servicio no justificado.

- ✓ La relevancia o importancia que tiene para el proceso de negocio o el/los activos afectados (el grado de dependencia). En el nivel de riesgo se deberá ver reflejado, que los riesgos que afectan a activos o procesos críticos tiendan a posicionarse en niveles superiores (de mayor riesgo) frente a aquellos que afectan activos o procesos secundarios.

- ✓ La probabilidad real de ocurrencia. Que como se dijo debe de considerar: amenazas, vulnerabilidades y la factibilidad del escenario de incidente donde una o más

vulnerabilidades puedan ser explotadas por algunas de las amenazas. Una vulnerabilidad que no tiene a priori una amenaza latente para ser explotada o por el contrario, una amenaza para las cuales ya se adoptaron los controles pertinentes o simplemente no aplique a la realidad existente, deben documentarse pero no deberían recibir tratamiento prioritario sobre otros riesgos actuales y reales.
A modo de ejemplo, si no tengo la infraestructura necesaria para realizar comercio electrónico, esto debe documentarse, pero no es una prioridad ni una necesidad dotar a la empresa de esta infraestructura si no está previsto en los planes empresariales (estratégicos y operativos) ofrecerlo.

Herramientas y metodologías:

El concepto tradicional de nivel de riesgo, está dado por el impacto ponderado por la probabilidad de ocurrencia, es decir: *Impacto x Probabilidad de Ocurrencia*.

Sin embargo, aparecen otros factores que deben tenerse en cuenta, como el "riesgo residual", "riesgo acumulado" y también factores financieros, que a veces con importante incertidumbre deben estimarse. Por ejemplo: ¿ Cual es el valor o impacto de perder la confidencialidad de los datos de potenciales clientes ?
Muchas veces también los riesgos tienen efectos residuales y a su vez el impacto de diferentes riesgos perdura por diferentes periodos, por lo cual habría que aplicar técnicas financieras de evaluación de proyectos como valor actualizado neto (VAN) y tasa interna de retorno (TIR), a los efectos que estos riesgos evaluados cuantitativamente sean comparables.

Sin embargo el costo de optar por un Modelo Cuantitativo, como por ejemplo el que se presenta en [3], para la totalidad de los riesgos, puede ser muy alto y no ser oportuno, se estaría invirtiendo tiempo y recursos más allá de lo conveniente. Por otra parte, muchos riesgos son muy difíciles de estimar cuantitativamente con una certeza razonable.
En esos casos, análisis Costo – Beneficio y teniendo en cuenta datos estadísticos, *Focus Groups* y eventualmente técnicas de encuestas y formularios (*Delphi*) pueden hacer converger estas estimaciones.

Tal como se analizó en: "*3.2.8.4.1 Estrategia: ¿ Top Down o Bottom up ?*" lo más adecuado es una estrategia combinada: un análisis en dos niveles o dos pasadas, un Alto Nivel, y un Bajo Nivel, pero además con posibilidad de escalar riesgos *bottom up* en caso de ser necesario porque no fue detectado en el alto nivel.

Salida:

Una tabla con el ranking de riesgos, calificados con su nivel correspondiente en función del criterio establecido atendiendo a su impacto estimado en el negocio y a su probabilidad de ocurrencia, a los efectos que puedan priorizarse los mismos para su tratamiento.

3.2.8.4.6 Evaluación de Riesgos

El objetivo principal de la evaluación de riesgos es priorizar los mismos y racionalizar los recursos disponibles para la implantación de controles. Incluso establecer el cronograma de acciones en función de estas prioridades, en ese caso, el recurso tiempo es un recurso más a racionalizar, que también es escaso si se consideran las ventanas de oportunidad que se abren para las amenazas latentes, vulnerabilidades presentes y el tiempo disponible para mitigar estos riesgos.

Por otra parte, por un tema de eficiencia operativa y de la relación costo / beneficio, como en cualquier proyecto, es necesario priorizar las actividades relevantes.
Evaluar todos los riesgos posibles, a nivel detallado, sobre todos los activos indiscriminadamente, supondría una inversión en recursos (técnicos y profesionales) y tiempo difícil de justificar. Por otro lado, los riesgos más graves que podrían suponer impactos nefastos para el negocio o pérdidas financieras importantes, se verían postergados debido a una aplicación sistemática de evaluación de todas las vulnerabilidades, amenazas, controles y activos, cosa que claramente no es deseable.

No obstante, justamente por esa virtud de concentrarse en los aspectos más gruesos, es que puede ocurrir que algunos activos o procesos críticos / importantes o quizás más relacionados al dominio específico de la aplicación y a aspectos técnicos o tecnológicos, sean subestimados o no sean detectados. Por ello se hace necesario una instancia que permita elevar los riesgos detectados a más bajo nivel. Esto es, no sólo el refinamiento del análisis de alto nivel sino además, permitir escalar los riesgos en sentido inverso (*bottom up*) si es que se omitieron o corresponde ajustar.

<u>Evaluación de Alto Nivel</u>:

Entrada:

Algunos aspectos que pueden ser una ayuda importante en este análisis de alto nivel son:

a. El Grafo Valuado de Dependencias
b. La inversión que realiza la organización en cada activo / proceso (inicial, mantenimiento, control, gestión, etc.).
c. Especificación de los procesos y activos de mayor valor agregado para el negocio.
d. Las consecuencias de incidentes conocidos y comparables, ya sea propios o de otras empresas similares.
e. Especificación de los criterios de evaluación de riesgos establecidos.

Acción:

Debe realizarse, en función de toda la información relevada y analizada, la evaluación de los riesgos (residuales) en función de los criterios establecidos previamente para ello. Además debe establecerse una lista prioritaria a nivel macro, de los riesgos a atender con prioridad, que resultará de los procesos y activos críticos y los riesgos que pueden ocasionarle mayor daño a la empresa y/o tengan una probabilidad alta de ocurrencia.

Quienes deberían participar:

f. Gerencias de línea
g. Equipo de Planeamiento de Seguridad de la Información
h. Comité de Seguridad de la Información, eventualmente con el asesoramiento de un Analista de Riesgos.
i. Dirección y Gerencia General (en caso de ser necesario)

Salida:

a. Un documento general con los grandes lineamientos de gestión de riesgos, y principales riesgos priorizados de acuerdo al criterio de evaluación previamente establecido.
b. Un documento con los requerimientos para profundizar en un análisis detallado en las áreas críticas y de alta prioridad (en función de objetivos estratégicos, operativos, marco legal, etc.).

Evaluación Detallada:

Entrada:

a. Un documento general con los grandes lineamientos de gestión de riesgos, y principales riesgos priorizados (alto nivel).
b. Un documento con los requerimientos para profundizar en un análisis detallado en áreas críticas y de alta prioridad.

Acción:

En función del análisis de riesgos de alto nivel, debe refinarse el análisis con conocimiento específico del dominio y a un nivel más detallado para asegurarse que los controles sean definidos para lograr el nivel de seguridad requerido.
Elevar eventualmente nuevos riesgos detectados en el dominio específico o áreas técnicas, que no están cubiertos en el análisis de alto nivel y requieren de la intervención de los órganos gerenciales y/o corporativos para su consideración.

Quienes deberían participar:

a. Gerencias de línea
b. Técnicos / especialistas del área
c. Equipo de Planeamiento de Seguridad de la Información
d. Comité de Seguridad de la Información (consultas puntuales y sólo si es necesario).

Salida:

a. Un documento que consolide la evaluación detallada de riesgos en las áreas críticas y de alta prioridad.
b. Una lista de riesgos eventualmente inadvertidos a alto nivel o subestimados a consideración de especialistas de un dominio específico (dueños de la información), que amerita su escalamiento para reconsideración.

3.2.8.5 Tratamiento de Riesgos

El tratamiento de riesgos debería ser guiado por algunos principios de gestión básicos, atendiendo a que no se busca una protección absoluta, con todos los controles posibles, sino una seguridad conveniente, atendiendo a: los aspectos legales, estratégicos y a la disponibilidad de los recursos.

Debe perseguirse la eficacia de los controles para lograr los requerimientos de seguridad del negocio, fundamentalmente sobre cada activo y proceso importante.

Por otra parte, debe procurarse la eficiencia operativa, intentando racionalizar los recursos acorde a las prioridades y no sobreproteger ni subproteger los activos por error u omisión. No debe confundirse aquí, la sobreprotección por falta de planificación o disciplina de diseño con la seguridad por capas, principio básico de seguridad. Debe primar el principio de costo / beneficio en su acepción más amplia, considerando no sólo aspectos de costos y retornos de la inversión en términos financieros, sino aspectos estratégicos y valores menos tangibles como la imagen, prestigio, etc.

Entrada:

a. Una lista de riesgos priorizados, de acuerdo al criterio de evaluación de riesgos y acorde a los escenarios de riesgos identificados.
b. Restricciones (de tiempo / oportunidad, financieras, técnicas, ambientales, legales / regulatorias, contractuales, culturales, de interoperabilidad, adecuación etc.).
c. Lista de amenazas sobre los activos de información, atendiendo factores humanos, técnicos y procedimentales.
d. Lista de vulnerabilidades de los activos, con el mismo alcance que el ítem anterior.

Acción:

Debe decidirse cómo se enfrentará cada uno de los riesgos, los cuales pueden:

- mitigarse: implementando controles y obteniendo así un riesgo residual.
- aceptarse, según los criterios y umbrales de aceptación inicialmente especificados.
- evitarse: haciendo el riesgo residual 'despreciable' o nulo.
- transferirse: a terceros, por ejemplo a otra empresa mediante contrato o una compañía aseguradora.

Los controles pueden operar sobre el impacto (mitigando el mismo), sobre las amenazas (disminuyendo su probabilidad de ocurrencia) o sobre las vulnerabilidades (fortaleciendo esos aspectos).

Es posible combinar más de una estrategia para un riesgo, por ejemplo, aplicar controles para mitigar un riesgo y el riesgo residual transferirlo mediante la contratación de un seguro.
En sentido complementario, también es esperable y deseable, que un mismo control sirva como medida para contener o mitigar más de un riesgo y funcione como salvaguarda para varios activos.

A veces, pueden detectarse controles redundantes, pero puede ocurrir que quitar el control sea más costoso que mantenerlo, ya sea por la oportunidad del cambio y el impacto que tiene en la revisión y evaluación de nuevos escenarios de posibles incidentes, así como el impacto en si mismo que puede requerir el cambio por tareas que deban realizarse (en las aplicaciones por ejemplo). En este caso, también debe aplicarse el criterio de evaluación de riesgos y la relación costo / beneficio.

Quienes deberían participar:

a. Gerencias de línea
b. Técnicos / especialistas del área
c. Equipo de Planeamiento de Seguridad de la Información.
d. Eventualmente con el asesoramiento de un Analista de Riesgos.

A los efectos de dimensionar el Plan, puede ser necesario consultar a la Dirección y/o Gerencia General para saber la viabilidad de contar con los recursos suficientes y así adecuar el alcance del mismo.

Salida:

Un Plan de Tratamiento de Riesgos con los correspondientes riesgos residuales, sujetos a la aprobación de la gerencia. Si se proponen riesgos residuales que estén por encima de los niveles de aceptación de riesgo tempranamente establecidos, deben de justificarse adecuadamente, para su aceptación explícita y firma de la Alta Gerencia.

3.2.8.6 Aceptación del Plan de Tratamiento de Riesgos

Entrada:

a. Plan de Tratamiento de Riesgos, con sus riesgos residuales, los recursos necesarios y un cronograma tentativo de alto nivel a los efectos de su evaluación.
b. Informe de las áreas técnicas que correspondan a los efectos de analizar la viabilidad del Plan, por ejemplo la Gerencia de Finanzas y Gerencia Jurídica en lo que refiere a la aceptación de los riesgos residuales.

Acción:

La Alta Gerencia debe dar su aprobación al Plan de Tratamiento de Riesgos, velando que se cumpla con los niveles de aceptación de riesgos especificado y si se optara por aceptar algún riesgo mayor al nivel esperado (especificado) debe dejarse explícitamente documentado en que se fundamenta la decisión.

Quienes deberían participar:

Comité de Seguridad (que tiene al menos un representante de la empresa principal del grupo empresarial).
Dirección y Gerencia de la empresa en cuestión (subordinada).
Dirección y Gerencia del grupo empresarial en el caso que involucre niveles de aceptación que están por encima de los niveles pautados en su propio SGSI y políticas corporativas, lo cual será determinado por la Dirección de la empresa menor, en este caso requerirá de su

aprobación especial. De todas formas el Plan de Tratamiento de Riesgos, con los riesgos residuales, le será siempre informado.

Salida:

La aceptación del Plan de Tratamiento de Riesgos, incluyendo las decisiones excepcionales tomadas - si las hubiera - con respecto al criterio general.

3.2.8.7 Comunicación de los riesgos

Entrada:

Todos los resultados de las etapas anteriores de la Gestión de Riesgos, en particular, el Plan de Tratamiento de Riesgos incluyendo los riesgos residuales.

Acción:

Es necesario una adecuada comunicación a los efectos de por un lado: entender los lineamientos de seguridad de la información, conocer las políticas específicas y la existencia y potencial impacto de los riesgos; por otro lado, captar los riesgos desde todos los niveles tal como son percibidos considerando aspectos técnicos, de localización, probabilidad, percepción del riesgo, medidas posibles, etc.

Esta comunicación debe ser bidireccional, tanto entre empresas como al interior de cada empresa.

La comunicación en sentido ascendente, con respecto a la relación jerárquica, permite captar la percepción de riesgos por parte de las áreas directamente involucradas, riesgos que quizás no son percibidos en su justa dimensión desde niveles superiores.

Estos planes deben establecerse para situaciones de régimen pero también contemplar situaciones de contingencia o emergencia.

De acuerdo a la norma ISO/IEC 27.005 es necesario un plan de comunicación de riesgos a los efectos de:

- Recopilar información sobre los riesgos (percibidos).
- Compartir los resultados de la evaluación de riesgos y presentar el plan de tratamiento de riesgos.
- Evitar o reducir la ocurrencia y el impacto de los incidentes e infracciones de la seguridad de la información debido a la falta de comprensión mutua o mala interpretación entre los encargados de adoptar decisiones y los involucrados.
- Apoyar la toma de decisiones.
- Obtener nuevos conocimientos de seguridad de la información
- Coordinar con otros involucrados y planificar las respuestas para mitigar su impacto.
- Dar a los responsables de la toma de decisiones y a las partes interesadas un sentido de responsabilidad acerca de los riesgos.
- Mejorar el conocimiento

Todo esto, es necesario realizarlo también entre ambas empresas relacionadas, justamente para alinear y armonizar sus necesidades de seguridad de la información, y eventualmente tomar acciones conjuntas, alineadas que den coherencia y adecuación a las necesidades de seguridad referidas. Esto por un lado evita vulnerabilidades por falta de información o de comunicación, y por otro lado permite optimizar el uso de los recursos o al menos lograr mayor eficiencia operativa.

Debe establecerse claramente, entre otras cosas, como se comunican:

- Lineamientos corporativos.
- Cambios en la Política de Seguridad y políticas específicas.
- Riesgos percibidos que deben ser escalados. Feedback bottom-up.
- Necesidad de tratamientos especiales que no cumplen los lineamientos generales (eventualmente corporativos).
- Los roles y responsabilidades en situaciones de urgencia o en escenarios de incidentes.
- Capacitación continua.

Quienes deberían participar:

a. Dirección y Gerencia de la empresa (subordinada).
b. Comité de Seguridad (que tiene al menos un representante de la empresa principal del grupo empresarial).
c. Equipo de Planeamiento de la Seguridad de la Información.
d. Departamento de Capacitación
e. Áreas involucradas.

Dado que la comunicación debe ser bidireccional, y debe asegurar una correcta y certera comunicación entre los interesados o afectados por los activos y riesgos involucrados y quienes deben tomar las decisiones, es necesario que participen profesionales con buena capacidad para transmitir estos conceptos, el riesgo residual, las decisiones y acciones necesarias. Por lo que además de buena capacidad de diálogo y exposición debe de ser un equipo con buen conocimiento del negocio y de la seguridad de la información.

Salida:

La toma de conciencia hacia el interior de la empresa, de la importancia de la seguridad de la información, el impacto potencial y las medidas que se adoptan. Mejorar continuamente el conocimiento sobre la gestión de riesgo y sus resultados.

3.2.9 Declaración de Aplicabilidad

Debe elaborarse un documento que especifique los controles adecuados que aplican al SGSI.
La norma ISO/IEC 27.001 especifica en su Anexo A - el cual tiene carácter normativo - un conjunto de Objetivos de Control y Controles generales ([19]). No obstante, aclara la propia norma que esa lista no pretende ser exhaustiva y debe ampliarse de acuerdo a las necesidades y características de la empresa y sector de la industria correspondiente.
En particular, resultan de especial interés, controles adicionales que puedan detectarse para el sector o la industria y tengan un carácter más específico.

Algunos controles podrían excluirse por no aplicar su objetivo de control y en ese caso debe explicitarse su razón en el documento, pero otros controles puede ocurrir que apliquen pero no sean viables ya sea por los recursos requeridos (técnicos o humanos), por la oportunidad del cambio, etc. En este caso, debe explicitarse también esta razón y cuándo correspondería rever su aplicación o qué condiciones deberían darse.

Quienes deberían participar:

a. Gerencia / Dirección de la empresa.
b. Comité de Seguridad
c. Equipo de Planeamiento de la Seguridad de la Información.
d. Gerentes de línea y de las diferentes unidades de negocio.
e. Responsables de los procesos sustantivos (críticos y prioritarios) de la empresa.

Una vez que se tiene la aprobación de la Gerencia / Dirección, se remite para su consideración por la Gerencia General y Dirección del Grupo Empresarial.

3.3 Implementar Y Operar (*Hacer*)

En esta fase se debe de implementar el Plan elaborado en la etapa anterior.
Para ello debe cumplirse con los siguientes objetivos, ellos son como se indica en [28]:

1. Elaboración y/o aplicación de estándares y procedimientos de seguridad de la información.
2. Implementación de controles.
3. Implementación de un programa de sensibilización y capacitación.
4. Implementación de un programa de gestión de incidentes.
5. Gestión de recursos para el SGSI.

Estas actividades serán especificados en las siguientes subsecciones.

[19] Extraídos a su vez de la norma ISO/IEC 27.002.

3.3.1 Estándares y Procedimientos para la Seguridad de la Información

Deben elaborarse y aplicarse los estándares y procedimientos dentro del alcance del SGSI, que podrán ser globales o sectoriales / específicos. En el caso que los controles sean aplicables únicamente a algún sector o procesos específicos debe explicitarse.

En ese sentido, en general, los estándares corporativos serán heredados por el grupo empresarial para su adopción por parte de la empresa en cuestión.
No obstante pueden requerirse estándares específicos o con mayor nivel de detalle para la empresa que se analiza. Los mismos no violarán las disposiciones corporativas en cuanto a estándares salvo que así sea autorizado pero podrán definir otros más específicos acorde a sus necesidades particulares.

Los estándares y procedimientos deben ser adecuadamente comunicados e impulsados para su aplicación (adhesión y cumplimiento).

Entrada:

a. Alcance del SGSI.
b. Política del SGSI.
c. Resultado de la Evaluación de Riesgos (Alto nivel y detallado).
d. Declaración de Aplicabilidad.
e. Plan de Tratamiento de Riesgos.
f. Política de Seguridad de la Información.
g. Estándares y Procedimientos de la empresa principal que comprendan a la subordinada ([20]).
h. Marco Legal, Normativo y Regulatorio.

Acción:

Deben designarse representantes de todas las Gerencias, a los efectos de definir y proponer sus estándares y procedimientos. Esto tiene un doble objetivo, por un lado, formalizar un conjunto de estándares y procedimientos alineados con la Seguridad de la Información, y por otro lado que participen profesionales y responsables con dominio del área de forma que el resultado sea compatible con las prácticas operativas, de forma de no crear obstáculos innecesarios a la operativa diaria.

Esto debe realizarse de forma *Top-Down* (refinamiento sucesivo) de forma de obtener una primer versión temprana. Las Gerencias de Línea y en particular, las de Gestión y Procedimientos y la de Planificación es probable sean protagonistas en este aspecto junto al Equipo de Planeamiento de la Seguridad de la Información.

Algunas herramientas útiles pueden ser, la Declaración de Aplicabilidad que dará la pauta de qué estándares y procedimientos deben definirse. Una sugerencia metodológica es utilizar la estructura del la norma ISO/IEC 27.002.

[20] Que correspondan al contexto y actividades de la empresa subordinada.

Quienes deberían participar:

a. Equipo de Planeamiento / Gerencia de la Seguridad de la Información.
b. Gerencias de Línea
c. (Gerencia de) Gestión y Procedimientos
d. (Gerencia) Técnicas, Planificación, Comercial y Finanzas.
e. Dueños de los Sistemas de Información.
f. Dueños de procesos de áreas estratégicas u operacionales importantes o críticas.
g. Responsable de la seguridad física.

Salida:

a. Estándares de Seguridad de la Información, y una línea base para la Organización.
b. Procedimientos correspondientes y complementarios a esos estándares.

3.3.2 Implementación de Controles

Entrada:

a. Alcance del SGSI.
b. Política del SGSI.
c. Resultado de la Evaluación de Riesgos (Alto nivel y detallado).
d. Declaración de Aplicabilidad.
e. Plan de Tratamiento de Riesgos.
f. Política de Seguridad de la Información, estándares y procedimientos.
g. Estándares y Procedimientos empresa principal que comprendan a la subordinada ([21]).

Acción:

La implementación de cada control, correspondiente a un objetivo de control, debería de analizarse como un 'mini-proyecto' en el sentido de su estrategia de implementación. Como tal, debería tener asociado su correspondiente diagrama de Gantt, con designación del responsable, los plazos, los recursos necesarios, las actividades requeridas, sus dependencias, etc.

Dependiendo de la dimensión del Control, tendrá documentación específica de su fase conceptual y de diseño y por otro lado un nivel más detallado respecto a su implementación concreta con las actividades y aspectos técnicos, instrumentación, planes de capacitación, asesorías, etc.

Es importante armonizar, por un lado, los aspectos organizacionales (Organización y Métodos) y los técnicos. Por otro lado, es necesario que los controles de la empresa menor, estén alineados con los de la empresa principal, en particular, en lo que respecta a los SGSIs y sus alcances.

También es conveniente identificar controles comunes a ambas empresas, por ejemplo, la política y controles de la seguridad física eventualmente puede ser compartida por ambas

[21] Que correspondan al contexto y actividades de la empresa subordinada.

organizaciones en el caso de compartir las instalaciones locativas, más allá de algunos controles que sean de aplicación específica a uno de ellas (lo cual se indicará en la Declaración de Aplicabilidad).
En la Figura 3.25 se ilustra la identificación de posibles controles sobre el grafo presentado anteriormente en la Figura 3.24.

No obstante, salvo controles que requieran ser elevados a la empresa principal del grupo, la implementación de los mismos, siempre que estén dentro del alcance del SGSI que se considera, serán responsabilidad de la empresa respectiva. Los controles que deben tratarse en forma global, porque trascienden a la misma o requieren aceptación por su inversión extraordinaria o el riesgo residual que debería aceptarse en caso de no implementarse, excede lo aceptable por el Grupo Empresarial, se tratarán en forma conjunta. El Comité de Seguridad actuará como nexo en este caso con la empresa principal.

Por todo lo anterior, es conveniente formular un Plan de Implementación de Controles, a los efectos de estimar recursos y tiempo que deberá ser aprobado por la Gerencia.

Quienes deberían participar:

Debe formarse un grupo de personas de los diferentes sectores dentro del alcance del SGSI, entre ellos:

a. Comité de Seguridad de la Información: Gestionará los recursos necesarios con la Gerencia y guiará prioridades en función de las políticas y lineamientos establecidos en su momento por la Gerencia / Dirección.
b. Equipo de Planeamiento de la Seguridad de la Información: Estimará recursos, propondrá alternativas técnicas y planes de implementación en un alto nivel, en particular para aquellos controles y objetivos de control relacionados.
c. Representantes de las Gerencias directamente afectadas.
d. Representantes de RR.HH.
e. Representantes de la Seguridad Física.
f. Gerencias transversales (de soporte corporativo): RR.HH, IS/IT, etc.
g. Dueños de los procesos y activos afectados (estratégicos y operacionales).

Salida:

a. Plan de Implementación de Controles (cronograma, responsable / equipo, etc.)
b. Registro y Documentación de las actividades y controles implementados.

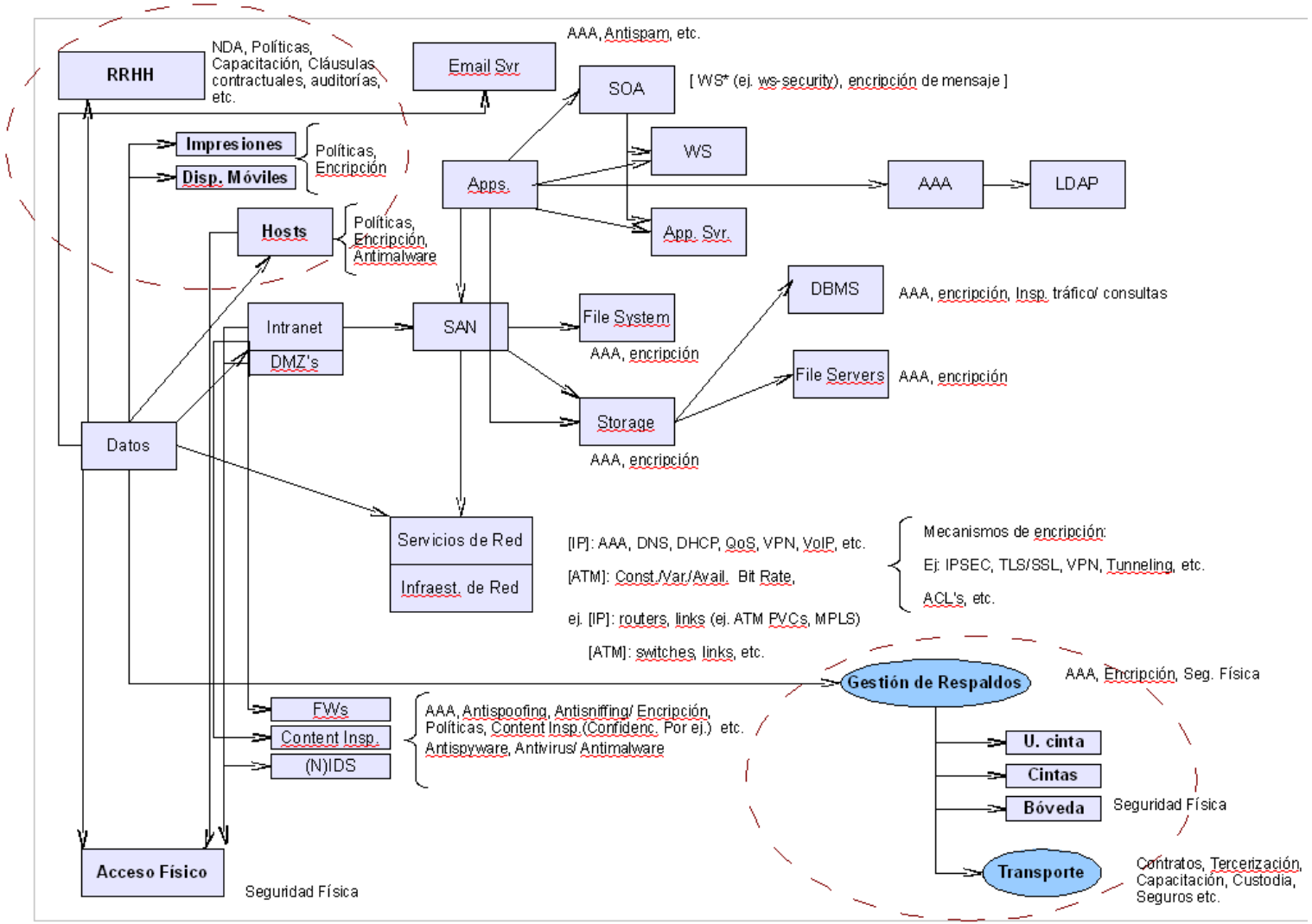


Figura 3.25 – Identificación de Controles

3.3.3 Implementación de un Programa de sensibilización y capacitación

Es fundamental implementar un Programa de entrenamiento y concienciación del personal, en todos los niveles y con alcance a toda la empresa (o todo el personal dentro del alcance del SGSI definido); a los efectos de:

- Evitar rechazo o aversión a los nuevos controles.
- Entender la importancia de la seguridad de la información, conocer los objetivos y prioridades y las consecuencias que tendría no lograr los niveles de seguridad adecuados / requeridos.
- Lograr el compromiso y la alineación al SGSI del personal, evitando fallas por falta de comprensión, mala comunicación, negligencia, etc.
- Capacitar al personal para que estén preparados a nivel conceptual y práctico para la implementación del SGSI en función de sus responsabilidades y sus actividades operativas.
- Facilitar la adopción e implementación del SGSI y su adecuación con los planes operativos y eventualmente otros planes de Gestión.
- Conocer los requerimientos de seguridad de la información no sólo a la interna de la empresa sino al momento de interactuar con terceros, y eventualmente incluir esos requerimientos en cláusulas contractuales.

Por otra parte, como se mencionó en la Introducción de este documento, de acuerdo a algunas encuestas internacionales [79], el mayor riesgo a la seguridad de la información, está dado por el factor humano, específicamente errores, conductas inapropiadas y/o negligencia generadas internamente.

Se hace prioritario por tanto, no sólo definir los procesos adecuados y más convenientes para el negocio, velando por la seguridad requerida, sino también planificar y ejecutar de forma efectiva un programa de sensibilización y capacitación en los temas de seguridad. Estos planes deberán tener el alcance que corresponda según el alcance del SGSI, deberá difundirse a todo el personal involucrado y deberán preverse capacitaciones con la especificidad requerida para algunos grupos , por sectores o afinidad en la función y responsabilidades del cargo.

Entrada:

a. Alcance del SGSI.
b. Política del SGSI.
c. Resultado de la Evaluación de Riesgos.
d. Declaración de Aplicabilidad.
e. Plan de Tratamiento de Riesgos.
f. Política de Seguridad de la Información, estándares y procedimientos.

Acción:

Atendiendo a la diversidad del personal en un grupo empresarial como el que se analiza, y en cualquier empresa mediana o grande, existe la necesidad de clasificar las necesidades de capacitación de los diferentes grupos en base a su formación, perfil profesional, experiencia y responsabilidad en la empresa.

De acuerdo a lo anterior, deben elaborarse planes de capacitación para cada área / subárea. Algunas capacitaciones serán específicas de una subárea o área (ej. para SysAdmin o DBAs o para la División de IS/IT, para el área Comercial, técnicos Instaladores, Ing. Eléctricos, etc.) y otras globales a la empresa (ej. Seguridad Física).

Debe asegurarse la cobertura total de la empresa, en el sentido que cada empleado pertenezca a alguna de las áreas en la que se realiza la clasificación a los efectos de la capacitación y debe elaborarse un plan de capacitación (objetivos, recursos, cronograma, grupo objetivo, etc.).

Se deberían cubrir aspectos generales, específicos de cada área y políticas y procedimientos generales relativos a la seguridad de la información, a modo de ejemplo:

- Riesgos y amenazas.
- Políticas de seguridad, estándares y procedimientos.
- Responsabilidades del funcionario y canales / herramientas para reportar y escalar problemas e incidentes de seguridad, etc.
- Procedimientos de auditoría.

Quienes deberían participar:

Todo el personal de la empresa debería ser capacitado, o al menos todos aquellos comprendidos por el Alcance del SGSI definido.

a. Responsable del plan de capacitación. (RRHH o Depto. de Capacitación por ejemplo)
b. Responsable de la infraestructura / recursos de la capacitación (ej. IS/IT).
c. Responsable del área capacitada.

Salida:

Plan de Capacitación incluyendo:

- Recursos
- Grupos objetivos
- Objetivos de la capacitación en cada caso (para cada grupo).
- Cronograma
- Roles y responsabilidades necesarias para la ejecución del plan.
- Recopilación de evidencia y estadística de los resultados del plan de capacitación y su asimilación por el personal.

3.3.4 Implementación de un Programa de Gestión de Incidentes

Entrada:

a. Alcance del SGSI.
b. Política del SGSI.
c. Resultado de la Evaluación de Riesgos.
d. Declaración de Aplicabilidad.
e. Plan de Tratamiento de Riesgos.
f. Política de Seguridad de la Información, estándares y procedimientos.

Acción:

Deben tomarse medidas para, por un lado, minimizar los incidentes de seguridad que ocurran, y por otro lado, si ocurren, que causen el menor daño posible.
En ese sentido deben realizarse actividades tendientes a la protección y establecimiento de controles en forma preactiva, y por otro lado, si ocurre un incidente debe detectarse y reaccionarse adecuadamente (acciones reactivas).
Para ello, además de los sistemas de monitoreo y detección de incidentes, alarmas o alertas, análisis de vulnerabilidades y tratamiento de riesgos, etc., debe existir un manual de procedimientos sobre cómo actuar cuando ocurre un incidente: cómo reportarlo, forma de escalamiento, contingencia, acciones reparatorias, etc., de forma de actuar de manera planificada y previamente analizada, y no de forma arbitraria y bajo presión.
La norma ISO/IEC TR 18.044:2004 [32] establece una guía y los lineamientos para la gestión de incidentes de seguridad de la información. Allí se especifica entre otras cosas, el *workflow* de acciones que debe tomarse para la gestión de incidentes incluyendo las responsabilidades, requerimientos, etc.

Los procedimientos deberían estar adecuadamente documentados, revisados y actualizados. Estos procedimientos deben permitir:

- Asegurar la continuidad del negocio, y gestionar incidentes de diferente naturaleza: *malware*, denegación de servicios, integridad de la información, accesos no autorizados, divulgación de información confidencial, etc.
- Clasificar y priorizar el incidente de acuerdo a un esquema preestablecido.
- Analizar e identificar las causas del incidente.
- Preservar y recolectar evidencia y pistas de auditoría que permitan técnicas forenses y su eventual uso en una acción civil.
- Planificar e implementar las medidas correctivas que correspondan, a los efectos de evitar que el incidente vuelva a ocurrir o en su defecto mitigar su impacto en un futuro.
- Acotar y minimizar el daño provocado en esta oportunidad. Aislar el problema si es posible, por ejemplo, sustituir un equipo o aislar una subred.
- Comunicar a todos aquellos afectados o involucrados en las acciones de recuperación así como escalar el incidente para su tratamiento cuando corresponda.
- Habilitar las acciones preparatorias por el daño provocado cuando corresponda (por ejemplo porque no se cumplió la calidad de servicio comprometida o sencillamente se incumplió un contrato por ejemplo).
- Informar sobre las acciones correctivas a la/s gerencia/s que corresponda/n.

También es necesario llevar una estadística de los incidentes ocurridos y que tratamiento se les dio, a los efectos de establecer métricas (frecuencia, costo: horas y recursos invertidos, etc.) y analizar la efectividad de los controles. Esta información debe ser considerada en la próxima revisión de la seguridad de la información, de acuerdo a la norma ISO/IEC 27.002 sección '*5.1.2 – Revisión de la política de seguridad de la información*'.

La Gestión de Incidentes, debe también seguir ciertos criterios y estar alineada con las prioridades de la organización, por lo tanto las decisiones de alcance, alternativa elegida y oportunidad, deben ser tomadas en consecuencia. En un grupo empresarial como el que se analiza, el incidente puede trascender a una empresa y afectar por ejemplo a la empresa principal y la subordinada, en ese caso, los mecanismos de comunicación, escalamiento, y tratamiento cobran mayor relevancia ya que se deben coordinar acciones, eventualmente conjuntas y los mecanismos de comunicación deben estar bien definidos para ser eficaces y eficientes.

En función de la relación de dependencia y autonomía de la empresa subordinada con respecto a la empresa principal en su parte operativa, y a las dimensión de la misma, pueden considerarse diferentes alternativas para la constitución de un CSIRT y la gestión de incidentes.
En [94] se presentan varias alternativas posibles de forma genérica para un CSIRT.
Allí se describen las siguientes posibilidades:

- *Ausencia de CSIRT propio*: En este caso, no existe un CSIRT establecido, y los incidentes son gestionados por profesionales en el marco de sus otras responsabilidades (por ejemplo administradores de red, IS/IT, etc.), muchas veces *ad hoc.*
- *Interno Distribuido*: se forma un equipo distribuido con personal especializado existente, coordinados por un supervisor, y que podrán cumplir las tareas relativas al CSIRT a tiempo parcial (y continuar con parte de sus otras responsabilidades) o completo.
- *Interno Centralizado*: similar al anterior pero localizado de forma centralizada, por lo que es más común que esta constitución se dé con personal dedicado a tiempo completo.
- *Interno Mixto (Centralizado y Distribuido)*: Esta combinación, maximiza la posibilidad de utilizar personal especializado en las diferentes tecnologías localizados en forma estratégica en la organización, y que sean coordinados y supervisados de forma centralizada por personal dedicado de forma completa.
- *Coordinador:* Este tipo de CSIRT en general tiene un espectro más amplio de acción en cuanto a su alcance de organizaciones externas sobre las que a veces no tiene autoridad ni sobre sus miembros que lo constituyen ni sobre las organizaciones a las que asiste.

Otra cualidad del CSIRT, es la autoridad y potestades del mismo sobre los servicios y organizaciones para las que presta servicios en el marco de la gestión de incidentes. Se distinguen las siguientes posibilidades:

- *Autoridad total*: El CSIRT tiene autoridad, durante la gestión de un incidente, para tomar las decisiones y acciones que entienda necesario y conveniente bajo su responsabilidad. Puede por ejemplo, indicar a los administradores de red y de los sistemas, aislar un servidor, o una subred durante un ataque.

- *Autoridad compartida:* En este caso, el CSIRT participa en la decisión de las acciones requeridas, recomienda, pero no toma la decisión por sí solo, la cual debe ser compartida con las gerencias relacionadas (por ejemplo IS/IT o del servicio afectado) y a nivel superior.
- *Sin autoridad:* No participa en la decisión, ni puede tomar acciones ni decisiones por si solo. Su rol es de asesor, el de brindar recomendaciones, y puede influir con ello en quien es responsable por tomar las decisiones, pero es un rol pasivo, sin voto.

En el caso que analizamos, es decir, el de un grupo empresarial, alguna de estas formas constitutivas podrá ser elegida de acuerdo a la adecuación y características del grupo empresarial concreto.
En todo caso, los incidentes deben ser gestionados de forma metódica, y no *ad hoc*, y deben asignarse los recursos necesarios para este cometido.
Sin perder generalidad, atendiendo a que nos referimos a un grupo empresarial de relación jerárquica, de la empresa en consideración con respecto a otra denominada principal, creemos que la opción de CSIRT *interno* es la más adecuada, que podrá ser *descentralizado, centralizado* o *mixto* en función de las características de la empresa: su dimensión, el rubro en el que se desarrolla, la sensibilidad de los procesos de negocio respecto de la seguridad de la información, el personal disponible para la tarea, la cantidad de incidentes de seguridad que debe o proyecta atender, etc.
Si la empresa subordinada no ameritara tener un CSIRT propio o no fuera posible, entonces los incidentes deberán ser gestionados por el CSIRT de la empresa principal, y en ese caso, un CSIRT *mixto* puede ser la opción más adecuada.
También debido a la subordinación de la empresa en consideración, a la empresa principal, su autonomía, y la política de seguridad de la información establecida, la autoridad para el CSIRT que se considera, podría ser de *autoridad total* o *compartida*. Creemos que la opción *compartida,* se respeta la naturaleza jerárquica y constitutiva del grupo empresarial.

Asimismo se debe considerar la cooperación de organizaciones especializadas e informar o escalar el incidente cuando corresponda, ya sea a nivel del grupo empresarial, o a nivel nacional (CSIRT, CERT) ([22]).

Quienes deberían participar:

a. CSIRT / CERT.
b. Equipo de Planeamiento de la Seguridad de la Información
c. Operaciones
d. Seguridad Física
e. Dueños de los Sistemas de Información
f. Dueños de los Procesos Estratégicos y Operacionales.

Salida:

a. Manual de Procedimientos de Gestión de Incidentes.
b. Eventualmente podría ameritar la conformación de un CSIRT, en cuyo caso hay que especificar su alcance y responsabilidades.

[22] O incluso organizaciones como FIRST o Telecom.-ISAC para un ISP/TelCo.

c. Indicadores y seguimiento de la Gestión de Incidentes

3.3.5 Continuidad del negocio

El Plan de Continuidad del negocio debería centrarse en los objetivos de negocio prioritarios para continuar operando el mismo en un caso de desastre o de crisis (incidente/s grave/s) y se debería indicar de forma concreta los procedimientos que deben ser realizados y el nivel de servicio que debe ser provisto en estas condiciones. Esto puede incluir seguros, acuerdos con terceros, mecanismos de contingencia, etc.

En particular los procesos críticos o prioritarios podrían depender de servicios provistos por la empresa principal, o viceversa. También puede ocurrir que una de las dos empresas preste servicios en una situación de contingencia mientras la otra restablece sus operaciones, o incluso podría ocurrir que ciertos procesos (de contingencia) y/o controles (prevención) los afronten de forma conjunta para compartir y bajar costos.

Estos planes de continuidad del negocio, tienen su correspondencia con los requerimientos de la seguridad de la información, y en ese contexto establecemos una breve especificación del mismo.

Entrada:

a. Objetivos del negocio
b. Procesos críticos y prioritarios para el negocio.
c. Activos relacionados o de los cuales dependen esos procesos críticos.
d. Análisis y tratamiento de riegos. Riesgos residuales y tolerancia admisible.
e. Responsabilidades sobre los procesos y activos críticos identificados.

Acción:

Es necesario para el plan de contingencia que estén claramente determinadas las responsabilidades sobre los procesos y activos necesarios para la continuidad del negocio.
A su vez deben determinarse y aprobarse de forma explícita y documentada la tolerancia a fallos o pérdidas admisibles, por ejemplo en la disponibilidad y pérdida de calidad de los servicios o de información. Sobre la base que los riesgos tratados de forma que son eliminados o mitigados hasta que su impacto potencial se encuentre dentro de un margen tolerable, deben definirse acciones para reponerse ante fallos previsibles o no y eventualmente y determinar acciones de contingencia para continuar con la operativa de los procesos y servicios críticos.

Además de la asignación de responsabilidades y la determinación de la tolerancia a fallas sobre los procesos críticos del negocio, deben realizarse las siguientes acciones:

a) Establecer los procedimientos que permitan recuperarse y mantener operativos los servicios y procesos críticos.
b) Establecer prioridades de recuperación y tiempos máximos de tolerancia para el restablecimiento del servicio con niveles aceptables, indicando cuales son estos niveles según corresponda.

c) Especificar otros procedimientos complementarios que deban ser realizados luego de los planes de contingencias ejecutados y los procedimientos necesarios para restablecer el servicio.
d) Documentar los procedimientos acordados y autorizados.
e) Capacitar al personal para actuar en estos casos (desastres, crisis, etc.).
f) Testear y actualizar los planes regularmente.

Quienes deberían participar:

En lo que refiere a los planes y acciones respecto de la seguridad de la información, deberían participar al menos:

a. Alta Gerencia / Dirección,
b. Equipo de Planeamiento de la Seguridad de la Información,
c. Comité de Seguridad de la Información,
d. Dueños de los sistemas de información
e. Dueños de los procesos estratégicos u operacionales importantes.

Salida:

Plan de Continuidad del negocio.

3.3.6 Gestión de Recursos para el SGSI

Establecer, implantar y mantener un SGSI requiere de recursos económicos, humanos y tecnológicos. Debe analizarse como un proyecto, con diferentes objetivos e hitos a cumplir en el corto, mediano y largo plazo.

Vimos que es necesario que el SGSI esté alineado con los intereses y prioridades del negocio, pero no deben subestimarse ni sobreestimarse las necesidades y requerimientos de seguridad, ni las actividades y recursos necesarios para alcanzarlos.

Para ello, puede ser útil un buen análisis costo / beneficio de las diferentes alternativas y escenarios planteados, y dejarlo por escrito para que en el futuro no haya ambigüedades o malos entendidos.
Otra herramienta útil puede ser el análisis de ROI, que en algunos casos, siempre que sea posible mantener umbrales de certidumbre razonables, puede ser persuasivo y factor de decisión al momento de decidir una inversión.

Para el análisis de ROI, puede servir de base el análisis detallado de riesgos.

Entrada:

a. Alcance y límites del SGSI.
b. Política del SGSI
c. Resultados de la Evaluación de Riesgos
d. Declaración de aplicabilidad (con los objetivos de control y controles)
e. Plan de Tratamiento de Riesgos.

f. Política de Seguridad de la Información, estándares y procedimientos.
g. Restricciones conocidas o detectadas (financieras, técnicas, culturales, legales, de tiempo / cronograma, de capacitación y recursos humanos, de integración con otros sistemas de gestión, etc.).
h. Análisis de Gap (con el escenario deseado y los requerimientos de seguridad de la información).

Acción:

En función de toda la documentación establecida en la "Entrada", es necesario establecer un plan de asignación de recursos (técnicos y humanos) que esté ajustado al presupuesto y si es necesario, realizar posteriormente las gestiones para su ampliación con un plan que sustente el SGSI.

Como todo plan, debe adecuarse, la inversión al retorno esperado, según un criterio costo / beneficio y alineado a las prioridades estratégicas de la Organización. Deben además tenerse presente, así como los objetivos y prioridades, las condicionantes y restricciones que pueden ser de diversa naturaleza:

- De oportunidad (tiempo / plazos, cronograma)
- Económicas y/o Financieras.
- Técnicas.
- Operacionales.
- Culturales / Idiosincrasia y costumbres.
- Ambientales.
- Legales.
- De facilidad de adaptación y uso.
- De Recursos Humanos (Capacitación, especialización, etc.)
- De integración con otros sistemas de gestión o incluso con los controles existentes.

Si es necesario realizar gestiones con la Dirección a los efectos de lograr mayores recursos a los ya asignados, serán realizadas por parte del Comité de Seguridad.
Igualmente, si hubiera riesgos compartidos que ameriten su tratamiento por parte de la empresa principal y la subordinada, o coordinar acciones para el mismo, serán analizados y gestionados por parte del Comité de Seguridad.

Quienes deberían participar:

a. Alta Gerencia / Dirección,
b. Equipo de Planeamiento de la Seguridad de la Información,
c. Comité de Seguridad de la información,
d. Dueños de los sistemas de información
e. Dueños de los procesos estratégicos u operacionales importantes.
f. Finanzas

Salida:

a. Asignación de Recursos Humanos
b. Plan de recursos de IT necesarios

c. Logística
d. Financiera (requerido y real)
e. Presupuesto (requerido y asignado)
f. Diagrama de *Gantt* con el proyecto de SGSI y si fuera necesario PERT de los recursos necesarios a los efectos de analizar dependencias.
g. Documento con los "*trade-off*" o decisiones tomadas cuando debe elegirse entre diferentes alternativas que priorizan algunos aspectos de la seguridad y/o comprometen otros.

3.4 Monitorear Y Revisar (*Verificar*)

En esta fase, deben planificarse y llevarse acabo las actividades que permitan evaluar la efectividad y eficiencia del SGSI y en particular de los controles implementados en referencia a los objetivos de control planteados en las fases anteriores.

El objetivo de esta etapa es justamente detectar desfasajes o ajustes que deben ser realizados, de forma de: o bien corroborar la adecuación de los controles implementados o su rectificación en el caso que no estén logrando los objetivos previstos, ya sea por una mala elección de los mismos o por una mala implementación.

Estos chequeos y revisiones, deben realizarse, según la norma ISO/IEC 27001, de forma preestablecida y sus resultados deben ser verificables y reproducibles.
Se realizarán de forma periódica y cuando se realicen modificaciones importantes a los procesos de negocios.
Asimismo, aunque eventualmente con una frecuencia menor, se realizarán revisiones por parte de la empresa principal, con especial énfasis en los procesos de negocio y activos que impactan la actividad de la empresa principal, y/o que estén bajo el alcance de su propio SGSI.

Podemos distinguir cuatro actividades principales para esta fase, ellas son:

1. Monitoreo
2. Métricas
3. Auditorías
4. Revisión.

3.4.1 Monitoreo

A los efectos de detectar, posibles diferencias entre el estado de seguridad de la Organización (sujeto al Alcance definido para el SGSI) y el estado que se pretende alcanzar (objetivos y requerimientos de seguridad), es necesario recabar y recolectar datos precisos que permitan de forma objetiva posicionar el estado de seguridad de la empresa.

Entrada:

a. Alcance y Política del SGSI.
b. Estándares y procedimientos relacionados a la Seguridad de la Información.

c. Resultado de la Evaluación de Riesgos
d. Objetivos de Control.
e. Controles seleccionados.
f. Requerimientos específicos de la Seguridad de la Información.
g. Clasificación de Procesos y Activos
h. Registros de Incidentes de Seguridad de la Información-
i. Estado de las Actividades planificadas y que se están llevando a cabo.

Acción:

Deben realizarse revisiones y chequeos en forma regular de forma de verificar que se están aplicando adecuadamente todos los controles seleccionados. Esto debe incluir tanto controles técnicos como de procedimientos y métodos (organizacionales).

Deben coordinarse las acciones de monitoreo de forma de lograr su cometido minimizando su impacto en las operaciones de la empresa y sin que tenga un impacto en la calidad del servicio ni en los procesos diarios. Por eso esto debe estar acordado con las áreas y debe planificarse con las otras Gerencias para lograr la mayor eficiencia posible con la eficacia deseada.

Las acciones de monitoreo deben ser tendientes a:

- Detectar problemas o desviaciones de los niveles deseados.
- Tomar acciones correctivas
- Eventualmente replantearse los procedimientos y soluciones técnicas.

Quienes deberían participar:

a. Equipo de Planeamiento de la Seguridad de la Información
b. Gerencia de Seguridad de la Información
c. División Informática (IS/IT)
d. Gerencias Técnicas Involucradas, Gerencias de Operaciones.

Salida:

a. Registro de todas las actividades de monitoreo y un informe para la gerencia que sintetice el resultado de estas actividades.
b. Un informe con las recomendaciones técnicas en función de los resultados obtenidos, acompañados de un informe estimado de los costos y explicitando los beneficios concretos, a forma de guía o recomendación para ayuda a la toma de decisiones por parte de la Gerencia en cuanto a la Seguridad de la información.

3.4.2 Métricas

Es importante, una vez elegidos los objetivos de control, tener una forma lo más objetiva posible de saber como se evaluará la efectividad de los controles y del propio SGSI en cuanto a su cumplimiento.
Si los controles establecidos, no logran los niveles de seguridad requeridos y no satisfacen los objetivos de control, puede ocurrir que, o bien los controles sean insuficientes o no se hayan elegido de forma adecuada y alineados con los objetivos establecidos, y/o que los controles elegidos no hayan sido correctamente implementados. Es decir, pueden existir deficiencias o fallas tanto en las fases de Planificación y Diseño como en la de Implementación y Operación.

Para detectar situaciones como las descritas, es necesario contar con un conjunto de indicadores que permitan levantar un llamado de atención, una alerta en el caso que o bien la elección de controles o bien su implementación requieran reajustes o reconsideración.

Para cada objetivo de control, existirá un conjunto de controles con el propósito de satisfacerlo, y debe establecerse uno o más indicadores a los efectos de conocer el grado de satisfacción del objetivo. Una vez conocido este grado, debe ser posible saber de forma concreta si el objetivo fue alcanzado o dicho de otra manera, si ese grado de seguridad es suficiente o se requieren reajustes.

Es así que debe definirse para cada objetivo de control:

1. Controles establecidos.
2. Identificar Indicadores de desempeño y efectividad de cada control.
3. Establecer cómo y cuando se llevará a cabo la medición.
4. Nivel de satisfacción del indicador.

Debe estar claro la forma tanto el procedimiento para llevar a cabo la medición, como qué es lo que se va a medir, y los criterios de satisfacción de forma objetiva y cuantificable.
Deben evitarse expresiones del tipo ambiguas, subjetivas o no cuantificables.

Quienes deberían participar:

a. Gerencias involucradas
b. Responsables de los sistemas de información.
c. Responsables de la seguridad de la información.
d. Técnicos involucrados.

Pueden participar además, profesionales externos, con este fin específico.

La norma ISO/IEC 27.004 especifica los lineamientos para implementar un programa de definición, implantación y ajuste de métricas además de una serie de *templates* ilustrativos que están alineados con los requerimientos de la norma ISO/IEC 27.001.

3.4.3 Auditorías Internas del SGSI

Según la ISO/IEC 27.001, deben realizarse auditorías internas a intervalos planificados para determinar si los objetivos de control, controles, procesos y procedimientos cumplen:

a. Los requisitos de la norma, la legislación y reglamentaciones
b. Los requisitos identificados de la seguridad de la información.
c. Los controles están implementados y se mantienen de forma eficaz
d. Se desempeñan de acuerdo a lo esperado (eficiencia).

Debe documentarse, los criterios, el alcance, la frecuencia y los métodos que se llevarán a acabo.

Quienes deberían participar:

En la selección de los auditores, además de las capacidades específicas en el área de seguridad, deben considerarse algunas otras competencias o habilidades de gestión como:

a. Planificar la auditoría que se llevará a cabo.
b. Documentar los resultados.
c. Proponer acciones correctivas y preventivas.

En el plan de auditoría, es deseable que se considere cómo afectan las acciones a llevar a cabo por la auditoría con las actividades y operaciones de las áreas que serán auditadas, a los efectos de lograr su cometido interfiriendo lo menos posible los servicios.

3.4.4 Revisión

Esta etapa o proceso, debe realizarse de forma periódica y planificada, y tiene como objetivos:

- Evaluar la efectividad del SGSI
- Evaluar los recursos asignados al SGSI
- Analizar los riesgos residuales
- Actualizar los planes de seguridad

Entrada:

a. Resultados de las etapas de monitoreo en función de las métricas.
b. Cambios en la realidad del negocio que afecten el SGSI, sea a nivel estratégico o del marco jurídico por ejemplo.
c. Informes de auditoría interna.
d. Informes de auditoría y no conformidades de la empresa principal del grupo.
e. Posibles nuevas tecnologías aplicables a los controles existentes u otros nuevos.
f. Sugerencias e informes recogidos de las diferentes áreas del negocio acerca del SGSI.
g. Informe y clasificación de riesgos percibidos por la empresa principal que alcancen al SGSI de la empresa subordinada.

h. Incidentes ocurridos, con toda la información recolectada (causa, costo: impacto, horas y recursos destinados a la recuperación, frecuencia, etc.).

Acción:

La etapa de revisión debería tener para este tipo de empresas un doble objetivo, por un lado, los objetivos propios de esta etapa para un SGSI como ser:

- Revisar la vigencia de las premisas, principios y condiciones bajo cuales se tomaron las decisiones y criterios de definiciones del SGSI.
- ¿ Ha cambiado la estrategia empresarial ? ¿ Los objetivos con respecto a la seguridad de la información siguen siendo válidos ?
- ¿ Ha cambiado el marco jurídico ?
- ¿ Es el alcance del SGSI adecuado y suficiente o conviene redefinirlo de acuerdo a la nueva realidad o nuevos objetivos ?
- Los niveles de seguridad definidos en cuanto a confidencialidad, disponibilidad e integridad son suficientes ?
- ¿ Los controles definidos e implementados son efectivos ?
- ¿ Las políticas de seguridad de la información están actualizadas ?
- Están los requerimientos de seguridad de la información alineados con los contratos con proveedores y clientes ?
- Informe estadístico de los incidentes de seguridad ocurridos en el lapso considerado y su impacto. Fuente: CSIRT y Gerencia.

Pero también, en empresas que pertenecen a un grupo empresarial con una empresa principal que las comprende, debe también revisarse si:

- Ha cambiado la percepción de Riesgos de la empresa principal en activos o procesos de dominio de la empresa en cuestión ?
- ¿ Ha cambiado el alcance y/o política del SGSI de la empresa principal ?
- Cambios en la propia Organización.
- ¿ El Riesgo percibido por la empresa principal requiere una reestimación de los riesgos y eventualmente redefinir los controles ?
- ¿ Es necesario elevar informe de riesgos residuales que exceden los niveles de aceptación definidos por la empresa principal ?
- Cambios en el mapa de amenazas potenciales.
- ¿ Es necesario coordinar controles conjuntos para cierto tipo de riesgos o activos compartidos ?
- ¿ Son los recursos asignados al SGSI adecuados para implementar el mismo y además cumplir con los requerimientos de seguridad corporativos ?

Esta etapa es de alto nivel, y no busca revisar en detalle de forma exhaustiva cada activo ni cada control, sino que busca redefinir si es necesario los lineamientos generales y ayudar a la toma de decisiones gerenciales en cuanto a la seguridad de la información por ejemplo:

- Revisar la relación costo / beneficio de la inversión realizada en Seguridad de la Información y los beneficios logrados. Los beneficios pueden evaluarse en función de

la mejora de la situación actual en forma comparativa a la situación anterior a la implementación de los controles.
- Revisar los criterios de aceptación de riesgo, y su adecuación al negocio.
- Analizar alternativas más convenientes, menos costosas o más efectivas, considerando por ejemplo, la posibilidad de transferir el riesgo si los controles para mitigarlo no han sido efectivos o son muy costosos debido a una problemática inherente a la empresa que no admite soluciones efectivas económicas de forma interna.

Quienes deberían participar:

a. Cuerpo Gerencial.
b. Comité de Seguridad de la Información.

Salida:

a. Informe de mejoras para hacer al SGSI más efectivo.
b. Decisiones gerenciales que sobre una base estratégica y de costo / beneficio permiten mejorar la seguridad de la información.
c. Redefinir o ajustar el SGSI para adaptarse a los cambios de la realidad o simplemente para lograr los objetivos de control trazados.

3.5 Mantener Y Mejorar (*Actuar*)

De acuerdo a la norma ISO/IEC 27.001 e ISO/IEC (FCD) 27.003 en esta etapa se debe, en función de toda la información recabada en las etapas de monitoreo, métricas y revisión del SGSI, adoptar las decisiones y redefiniciones necesarias para corregir los aspectos y controles que no estén logrando la efectividad esperada y replantearse el acierto o no de los controles planteados así como la vigencia de los objetivos de control.

Por otra parte, debe mantenerse la coordinación con la empresa principal del grupo y entonces habrá que considerar sugerencias, no conformidades o nuevos lineamientos recibidos por parte de ésta, como consecuencia de su propia revisión y propuestas de mejora en el ámbito de su propio SGSI.

Es así que en esta etapa deberá tenerse en cuenta:

- Identificar no conformidades (del SGSI de la propia empresa subordinada).
- Identificar o tomar conocimiento de las no conformidades del SGSI de la empresa principal..
- Definir acciones correctivas y preventivas.
- Evaluar sugerencias y definir la implementación de mejoras.
- Revisar el plan de mejora continua.
- Obtener el "*ok*" de la Dirección si es necesario de los cambios propuestos.
- Obtener los recursos para llevarlos a cabo.
- Comunicar estos cambios y mejoras.
- Monitorear la implementación de estos cambios.

Algunos de estos cambios y mejoras, podrá trascender al alcance del SGSI en cuestión y por ello, podrá ameritar no sólo de la aprobación sino de un plan compartido con el Grupo Empresarial, tanto en la obtención de recursos necesarios como las etapas de avance y ejecución de los mismos.
En este caso corresponderá, informar de estas mejoras propuestas y requeridas a la Dirección del grupo y a la correspondiente Gerencia de la Seguridad de la Información (de la empresa principal) para su planificación conjunta.

Entrada:

a. Informes de Auditoría interna.
b. Informes de no conformidades de la empresa principal del grupo, que estén dentro del alcance del SGSI en cuestión.
c. Informes de conclusiones y sugerencias surgidos de la etapa de revisión.
d. Propuestas de mejoras de otras áreas y unidades de negocios.

Quienes deberían participar:

a. Equipo de Planeamiento de la Seguridad de la información: responsable de sugerir las mejoras que pueden obtenerse y estimar los recursos que serían necesarios.
b. Comité de Seguridad: a los efectos de aprobar el plan tentativo o dar lineamientos más generales.
c. Alta Gerencia y Dirección en caso de ser los cambios propuestos de un impacto considerable o requerir presupuesto adicional al ya otorgado al área.
d. Gerencia de la Seguridad de la Información de la empresa principal en el caso de tratarse de no conformidades provenientes de su propio SGSI o cambios compartidos que deben ser implementados en conjunto.
e. Eventualmente en caso de entenderse necesario, debido a la diferencia entre el estado de seguridad percibido y el que se quiere lograr, podría participar una Consultoría externa con personal especializado en el área.

Los planes de mejoras deberán ser coordinados para su instrumentación con las áreas afectadas, de forma de interferir lo menos posible en su operativa diaria, al menos de forma no prevista a los efectos de evitar molestias o interferencias no deseadas.
La comunicación de las mejoras propuestas debe hacerse a los efectos de permitir un ámbito donde se reciban propuestas y en la medida de lo posible que el área afectada sea también parte integrante y responsable de las mejoras.

Acción:

De acuerdo a la ISO/IEC 27.003 se deben realizar las siguientes actividades:
a. Identificación de no conformidades.
b. Identificación de acciones correctivas y preventivas.
c. Implementación de las mejoras.
d. Testeo del logro de las mejoras esperadas.
e. Monitoreo.
f. Comunicación de los cambios y las mejoras.

Salida:

Un Informe con el plan de mejoras, describiendo o referenciando las conclusiones más relevantes surgidas de la etapa de revisión y especificando objetivos concretos, el impacto de los cambios y quienes estarían involucrados así como un plan tentativo para llevarlos a cabo.

3.6 Documentación

Se describe a continuación, una propuesta de la estructura de la documentación, atendiendo los requisitos de la norma ISO/IEC 27.001 y a las necesidades de la estructura empresarial que se analiza.

3.6.1 Introducción

Tal como lo establece la norma ISO/IEC 27.001, 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. Mejor alternativa relativa al criterio de decisión fijado por la gerencia a tales efectos, los niveles de aceptación de riesgo especificados y recursos disponibles. Y objetivos de control que responden a la estrategia empresarial, el marco jurídico y la política del SGSI establecida y aprobada por la alta Gerencia y Dirección.

Los registros permiten hacer además de trazables esta cadena de decisiones y definiciones, reproducibles y podrían eventualmente servir además como referencia en la comunicación y coordinación con la empresa principal del grupo.

3.6.2 Estructura de documentación del SGSI

Como se vio, un SGSI abarca numerosos dominios de la seguridad de la información y tiene diferentes requerimientos en los niveles de detalle.
Por otra parte como sistema de gestión, involucra la trilogía: Personas, Procedimientos y Tecnologías.

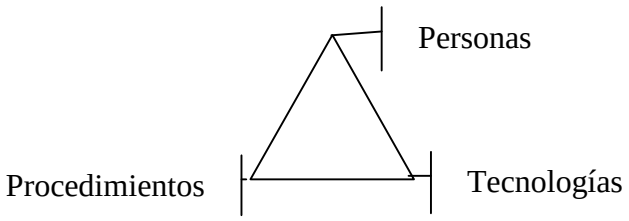


Figura 3.26 – Trilogía Personas – Procedimientos - Tecnologías

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 la estructura de un documento de un SGSI, que se adapte a estas características. Un documento principal con los lineamientos básicos, dados por la Dirección, más estables en el tiempo y que guíe 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 guardar 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, como se muestra en la Figura 3.27:

a - Un Documento Principal del SGSI.

b - Documentos de Soporte al SGSI:
- Políticas técnicas (de dominio, alcance y cometido específico)
- Procedimientos
- Guías e instructivos de operación

Se sugiere por tanto una estructura jerárquica de dos o más niveles, según se entienda necesario, con un documento principal y políticas específicas de soporte al mismo, así como especificaciones de procedimientos, instructivos y reglas operativas:

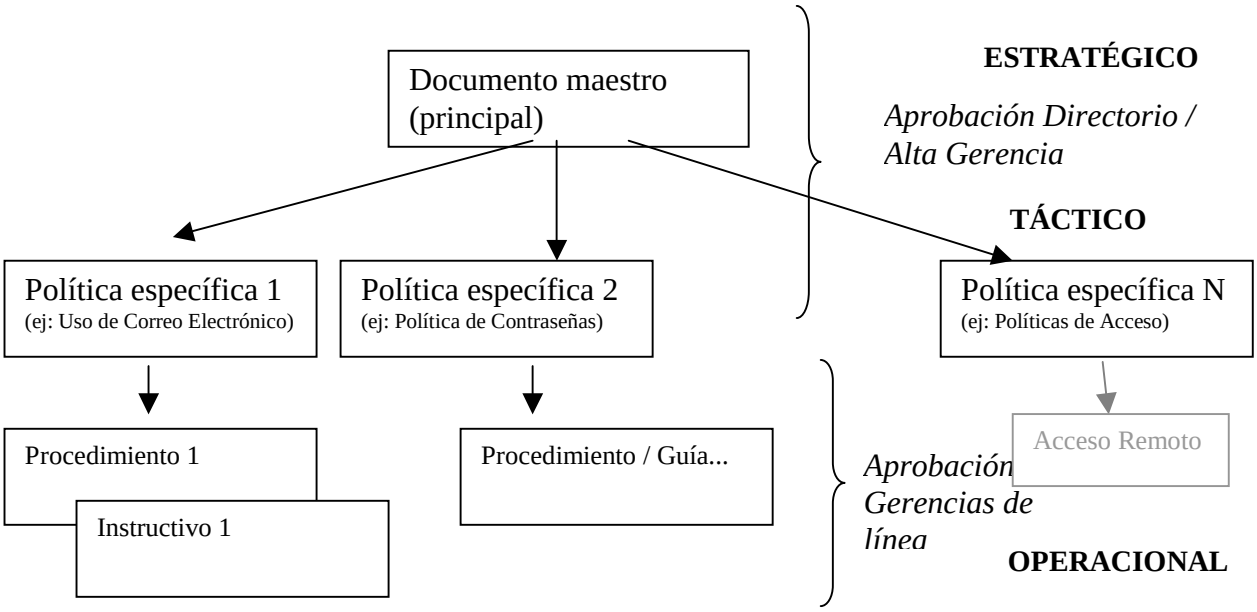


Figura 3.27 – Estructura de la documentación de un SGSI

Beneficios:

Simplicidad en la lectura y facilidad de comprensión, separando los conceptos o lineamientos y política general del SGSI por un lado, de los detalles de políticas específicas en documentos diferentes.
Clara separación de 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).

No es conveniente, que un mismo documento describa la política del SGSI y a su vez, en otro capítulo o sección, especifique políticas o reglas específicas del uso de claves o del correo electrónico corporativo, etc.
Para ejemplificar, es bastante más probable que cambie una política de uso específica o el largo / estructura de las claves de usuario por ejemplo, que la política general del SGSI.

3.6.3 Jerarquía de la documentación

En la Figura 3.28 se establece una correspondencia y un paralelismo entre la documentación requerida para la ISO/IEC 27.001 y el esquema utilizado por la norma de calidad ISO 9.001. Se establece así un esquema de cuatro (4) niveles [24], a saber:

Figura 3.28 – Jerarquía de documentación del SGSI [24]

Manual de Seguridad: En nuestro caso, como ya vimos en la sección referida de este documento, descompondremos el Manual de Seguridad en dos:

- Un *documento maestro o principal*: que tendrá la declaración de objetivos y lineamientos generales de la seguridad, la política del SGSI, responsabilidades en el alto nivel y directrices que guiarán la toma de decisiones en cada dominio de seguridad. No hace referencia a arquitecturas ni tecnologías específicas.
- *Políticas específicas anexas*: que tendrán, debido a su naturaleza, menor estabilidad en general que el documento principal.

En realidad viendo esto globalmente al grupo, si consideramos que la empresa principal tiene un SGSI propio, y que la empresa de referencia en este estudio (subordinada) tiene su propio SGSI pero está bajo el alcance del primero, tendremos en la jerarquía:

1. Manual de Seguridad de la empresa principal (del grupo empresarial).
   1.1. Política del SGSI (principal).
   1.2. Políticas específicas
2. Manual de Seguridad de la empresa de referencia.

2.1. Política del SGSI de referencia del caso de estudio.
2.2. Políticas específicas

3. Procedimientos.
4. Guías e Instructivos específicos.
5. Registros.

Procedimientos: Documentos de nivel Operativo, a los efectos que los procedimientos se realicen de forma preestablecida, aprobada, planificada y coordinada.

Guías e instructivos, Checklist, formularios: Son documentos complementarios de los Procedimientos a los efectos de formalizar la actividades y tareas requeridas para los procedimientos establecidos y las necesarias para tener mayor certeza sobre la gestión de la seguridad de la información.

Registros: Se deben registrar, de forma objetiva, las actividades e indicadores establecidos para el SGSI, de forma de documentar y hacer verificable el cumplimiento (o brecha) de los requerimientos del SGSI. En general registrarán actividades y resultados relacionados a los documentos y etapas de los niveles superiores en la pirámide de la Figura 3.28.

3.6.4 Completitud de la documentación:

De acuerdo a la norma ISO/IEC 27001, la documentación debe incluir:

1. Política y objetivos del SGSI.
2. Alcance del SGSI.
3. Procedimientos y controles que dan soporte al SGSI incluyendo:
    a) Procedimientos de control documentados
    b) Registro de los procedimientos de control
    c) Procedimientos de la auditoría interna
    d) Procedimientos para las acciones correctivas y preventivas
    e) Procedimientos de Revisión
4. Descripción de la metodología de evaluación de riesgos
5. Reporte de evaluación de riesgos.
6. Plan de tratamiento de riesgos
7. Documentación de los procedimientos para asegurar la efectividad de las etapas de planificación, operación y control del SGSI incluyendo como se medirá la efectividad de los controles.
8. Registros requeridos por la ISO/IEC 27005
9. Declaración de Aplicabilidad.
10. Informe de Auditoría.

Es responsabilidad de los auditores verificar que toda esta documentación existe.

3.6.5 La documentación y los registros como un activo más

Debe tenerse en cuenta que los registros son requeridos por la norma ISO/IEC 27.001 a lo largo de todo el ciclo PDCA ([23]) y es además un activo fundamental tanto para completar el proceso de revisión, monitoreo y mejora del SGSI. Como tal, tiene atributos de confidencialidad, integridad y disponibilidad que son necesarios preservar.
Igualmente la documentación también es un activo más. El nivel de confidencialidad que debe guardarse sobre el análisis de riesgos (vulnerabilidades, impacto, etc.) es un claro ejemplo.
Por otra parte, la disponibilidad de toda esta documentación y registros es necesaria, por parte de las personas correctas / autorizadas, para que el ciclo de Deming pueda cerrarse exitosamente.

Es conveniente entonces, contar además de con las condiciones de un repositorio adecuado para preservar esta documentación, con un sistema de consulta y acceso adecuado, que permita gestionar roles, usuarios, permisos de acceso, tipos de acceso, auditoría, etc.

Debe especificarse además el tiempo por el cual esta información debe preservarse y debe estar accesible, este tiempo podrá surgir de requerimientos legales, de certificación, contractuales o estratégicos del negocio.

3.7 Características deseables de Software de Apoyo al SGSI de un grupo empresarial

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 pretende aquí especificar formalmente los requerimientos, sino tan sólo brindar una lista de funcionalidades deseables de acuerdo a lo analizado en las secciones anteriores.

El software debería:

- Permitir heredar todos los lineamientos, metapolíticas y recomendaciones aplicables ya sean de la ISO/IEC así como aquellas más específicas que provengan de eventualmente de un Organismo de gobierno regulador o que paute los lineamientos de un plan director o de gobierno respecto de la seguridad de la información.

- Debería facilitar la armonización y ayudar a hacer eficiente el proceso de acoplamiento e integración del SGSI de la empresa subordinada con el de la empresa principal sin duplicar costos, ni controles. Se debería procurar la reutilización del conocimiento adquirido y la cooperación entre sí, tanto en un sentido como en el otro.

- Brindar funcionalidades de Gestión de Documentos, con definición de roles, gestión de permisos de consulta y modificación, de forma que la documentación sea tratada como un activo más, preservando sus requerimientos de Confidencialidad, Integridad y Disponibilidad.

[23] Ciclo de Deming

- Brindar funcionalidades de *workfolow* con gestión de roles y permisos, se puedan identificar etapas de relevamiento, definición, comunicación y delegación, supervisión, escalamiento, etc., que pueda comprender la relación jerárquica del grupo.

- Ayudar a establecer una correspondencia (y cumplimiento en lo que corresponda) entre las políticas establecidas para la/s empresa/s subordinada/s y la principal.

- Permitir 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). Un caso particular es que se traten como un mínimo aceptable (cota inferior) en el caso que las clasificaciones heredadas sean obligatorias.

- Para lograr lo anterior, el software debería ser configurable, y tratar esto mediante coeficientes de ponderación, roles y permisos para cambiar ciertos valores asignados e incluso modificar o ajustar el propio coeficiente de ponderación.

- Brindar funcionalidades de identificación y clasificación de procesos y sus activos asociados clasificando y valorizando los mismos en función de la escala establecida en cuanto a su necesidad de: confidencialidad, integridad y disponibilidad. Puede resultar interesante filtrar o seleccionar los subgrafos de dependencias inducidos por los procesos de negocios de determinada categoría (por ejemplo críticos o estratégicos, de alta prioridad).

- Utilizar algoritmia de grafos, y los mecanismos de ajuste y algoritmo definido para la valoración de activos en función de las dependencias de la seguridad entre activos (para cada uno de los atributos de seguridad), y permitir al profesional hacer ajustes sobre eso si así lo deseara.

- Detectar activos con un grado de entrada alto para su análisis, atendiendo a la concentración de dependencias de seguridad. Debería tener en cuenta además el número de activos o instancias de ese tipo de activo de información.

- Brindar funcionalidades tendientes a gestionar las dependencias interempresariales.

- Brindar la posibilidad de 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.

- Permitir analizar riesgos enfocándose 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.

- Permitir 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.

- Permitir establecer vistas y trabajar por capas de abstracción, en el sentido de estar alineado con la Recomendación ITU-T X.805, gestionando *layers* (Infraestructura, Servicios y aplicaciones), planos (gerencial, control y usuario final) y las ocho dimensiones de seguridad establecidas en la Recomendación.

4 Caso de Estudio: ISP - TelCo

En este capítulo, se analiza la aplicación de la metodología a un Caso de Estudio concreto, el de un grupo empresarial de telecomunicaciones donde se integran verticalmente un ISP y una TelCo.
Para ello se consideraron diversos estándares (ISO/IEC) y recomendaciones de la industria (ITU-T), así como investigación y análisis propio ya sea de la documentación y datos estadísticos que se referencian, como el aporte y la consulta a los profesionales de la TelCo e ISP que se tomó de ejemplo a nivel nacional ([24]).

4.1 Introducción

El sector de las Telecomunicaciones, los proveedores de servicios de internet y de contenido (ISPs) enfrentan actualmente, y es la tendencia mundial [80], desafíos de crecimiento, convergencia, transformación de sus negocios, cambios tecnológicos y regulación creciente.
Todos ellos, desafíos para la seguridad de la información.

4.1.1 Motivación

Es muy común que un ISP esté integrado verticalmente con una TelCo en un grupo empresarial, y es por ello que es un Caso de Estudio interesante para la metodología definida en los capítulos anteriores, de diseño, implementación, gestión y mejora de un SGSIs en un grupo empresarial con una estructura jerárquica.

Por lo tanto, parece natural, enfocar y caracterizar el Caso de Estudio, considerando dos componentes claros, por un lado: los lineamientos para la aplicación de la metodología para la implantación de un SGSI especificada en los capítulos anteriores, y por otro lado: las particularidades del sector de la industria elegido así como su estructura empresarial.

4.1.2 Propósito

El objetivo de esta sección es ilustrar la aplicabilidad de la metodología definida instanciando algunas secciones específicas con datos y características propios de la industria así como estadísticas internacionales del sector.

4.1.3 Alcance

Se ilustra la aplicación de la metodología analizando sobre todo la fase de Planificación para el sector.
No se pretende aquí esbozar un SGSI para un ISP ni tampoco especificar la metodología concreta de forma detallada. Tampoco se avanza en actividades metodológicas que requieren de un trabajo concreto y específico, actividades de consultoría que escapan al alcance de este trabajo de tesis.

[24] Antel y Anteldata.

4.2 Organización estructura y relacionamiento

En la Figura 4.1 se establece una adecuación de la estructura presentada en la sección "3.2.5 *Organización, estructura y relacionamiento*" con el modelo de negocios para la industria específica de las empresas del grupo (TelCo - ISP):

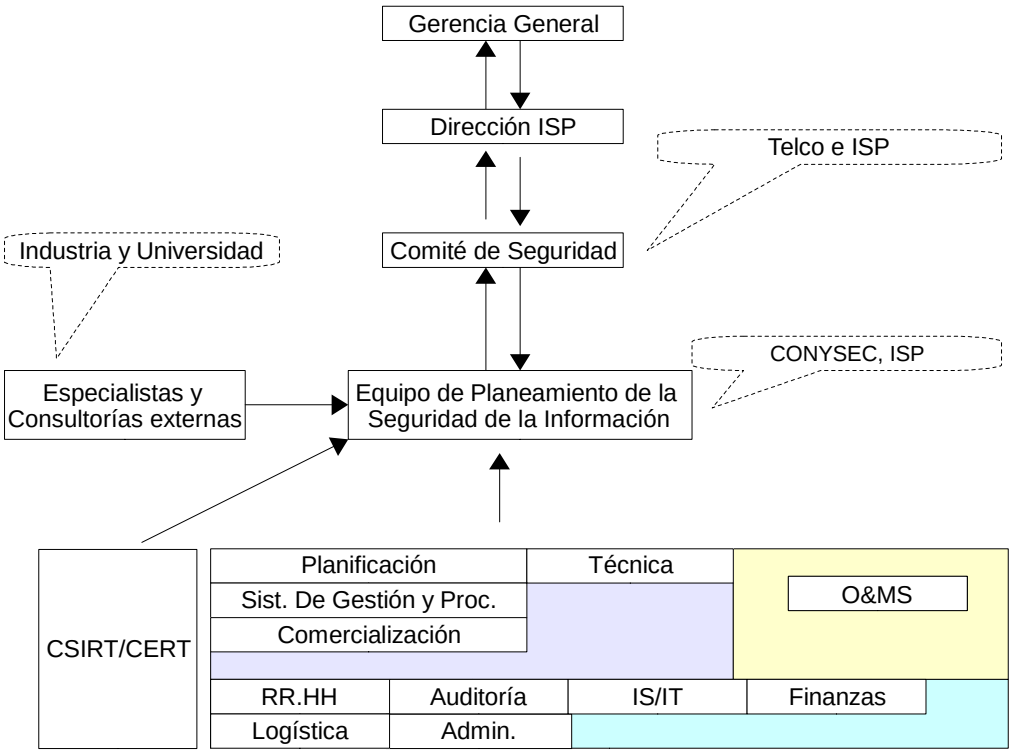


Figura 4.1 – Estructura de relacionamiento detallada para el SGSI

En la estructura propuesta para el caso de estudio, vemos que la TelCo participa en conjunto con el ISP en los niveles más altos de dicha estructura, en la definición de los criterios básicos que hacen a los lineamientos fundamentales y directrices del SGSI, que se verá reflejada en el alcance y política del SGSI del ISP.

Por otra parte, el ISP deberá contar con una estructura mínima necesaria conformada por representantes de sus unidades de negocio y dueños de procesos de negocios sustantivos aptos para integrar el Comité de Seguridad así como profesionales en Seguridad de la Información y personal capacitado para implantar, mantener y monitorear el SGSI.
En el caso extendido, o su constitución más amplia, este Comité tendrá la participación de responsables de la Gerencia de Seguridad del grupo empresarial (de la empresa principal).

Dependiendo del dimensionamiento del ISP, el Equipo de Planeamiento de la Seguridad de la Información, podría reducirse en su caso extremo a un Oficial de Seguridad, que coordinará sus acciones y los requerimientos de seguridad, con el equipo gerencial del ISP y sus pares de la

empresa principal, y eventualmente responsables relacionados de la Gerencia de Seguridad o Comité de Seguridad de la empresa principal del grupo.

En el Caso de Estudio, puede considerarse para este rol la participación de una entidad de las características del *ConySec* en el Equipo de Planeamiento de la Seguridad de la Información.

4.3 Análisis del Negocio

Como se vio en la sección "3.2.6 *Análisis del Negocio*" es necesario especificar y documentar claramente los aspectos relevantes del negocio para el cual se diseñará e implantará el SGSI. Deben contemplarse, las actividades sustantivas de la empresa, pero también el marco funcional en el que se desempeña, la estructura del grupo empresarial al que pertenece: ISP - TelCo.

Como se describe en la metodología propuesta, debe analizarse y especificarse formalmente: los aspectos más relevantes del negocio desde un punto de vista estratégico-empresarial (objetivos, prioridades, planes estratégicos), especificar formalmente el alcance y límites del SGSI, así como la política del mismo que deberá estar alineada con la estrategia empresarial y a las decisiones tomadas por la Dirección y Gerencia.

4.3.1 Establecimiento del Contexto

A los efectos de establecer el Contexto, deben considerarse aspectos organizacionales, geográficos, estándares y normativa vigente a nivel internacional y nacional así como recomendaciones y las mejores prácticas de la industria de las Telecomunicaciones, consideraciones legales, políticas de estado, políticas corporativas, etc.

Podemos en particular, diferenciar el contexto normativo y de estándares de los SGSI y las normas estándares de la ISO/IEC, y por otro lado contextualizar también el marco institucional del ISP. Contexto institucional que deberá ser tenido en cuenta para el relacionamiento de las partes y el propio SGSI a implementar.

En síntesis tendremos en cuenta:

a. Contexto Normativo
b. Contexto Institucional

4.3.1.1 Contexto Normativo

En la Figura 4.2 se ilustra el marco normativo que debe tenerse en cuenta para implantar un SGSI en el sector de actividad analizado, en este caso un ISP. En él se ven representados estándares internacionales generales y aplicables a cualquier sector de actividad, así como también otros estándares y recomendaciones que son específicas del sector.

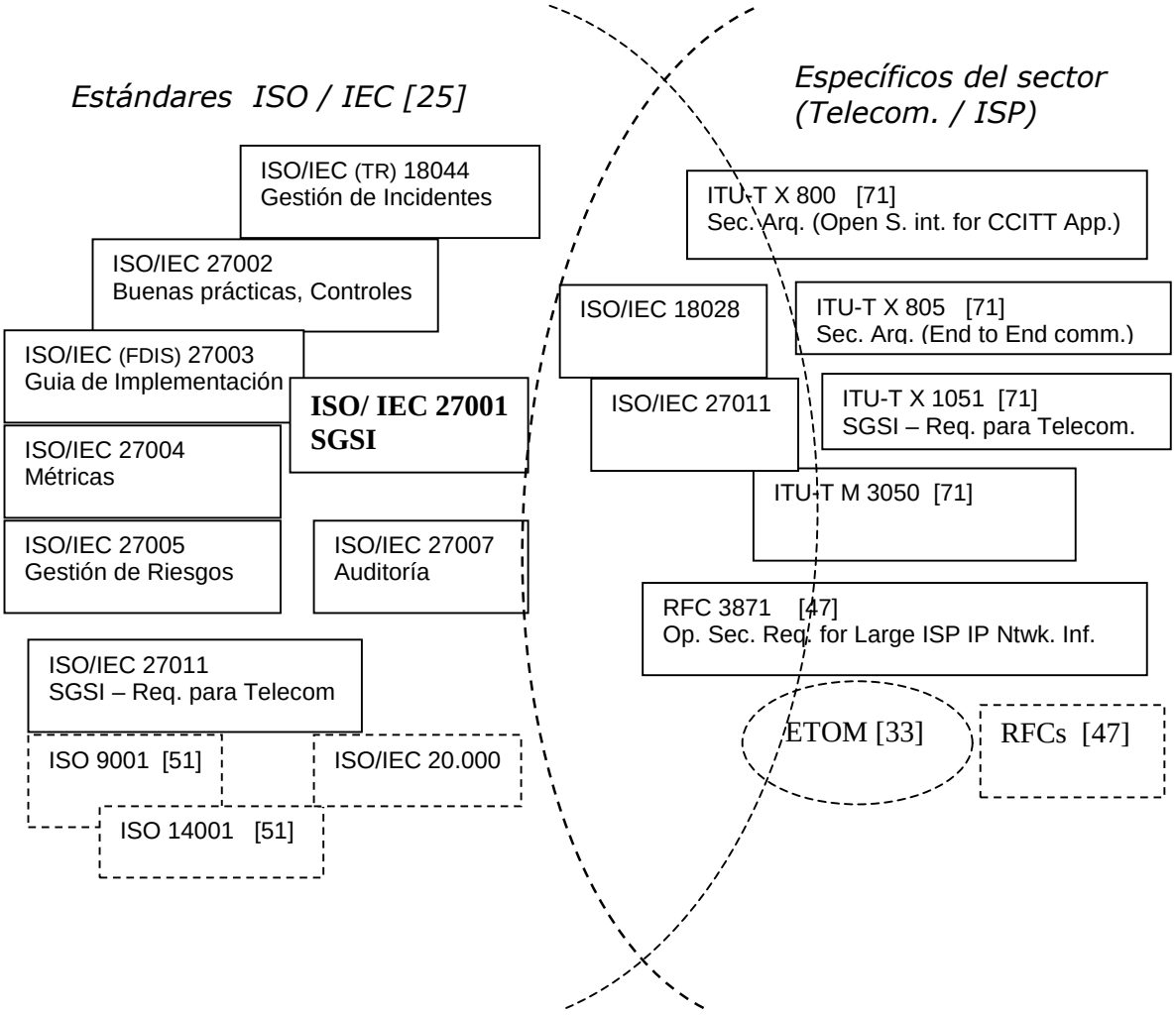


Figura 4.2 – Contexto Normativo del SGSI para un ISP

Recomendaciones específicas del sector:

Como se dijo en la sección "2.1 - Marco y Contexto Normativo – Estándares" de este documento, son recomendaciones, buenas prácticas y estándares de otras organizaciones especializadas en el sector de actividad específico de la industria.

En particular, para nuestro caso de estudio, un ISP vinculado a una TelCo, se destacan especialmente las Recomendaciones de la *International Communication Union* (ITU) [70], en particular la ITU-T: *ITU – Telecommunication Standarization Sector* [71], que como su nombre lo indica, especifica estándares para el sector de las empresas de Telecomunicaciones.
Estas recomendaciones son universalmente reconocidas y gozan del consenso y aprobación internacional. Incluso muchas veces, las mismas son luego homologados por la ISO/IEC y se convierten en Normas ISO/IEC a veces sin cambios y otras con algunos cambios menores.

A modo de ejemplo, la '*ITU-T X-1051 - Information Security Management System - Requirements for Telecommunications (ISMS-T)'* fue luego publicada como '*ISO/IEC 27011 - Information technology - Security techniques - Information security management guidelines for telecommunications organizations'*.

La 'ITU-T X.805 *Security architecture for systems providing end-to-end communications'* define los aspectos de arquitectura relacionada con la seguridad para los sistemas de comunicaciones a los efectos de favorecer la interoperabilidad entre múltiples proveedores alcanzando los niveles de seguridad requeridos [14]. Se aplica a redes de diferente naturaleza (operadoras, gubernamentales, de gestión, empresariales, etc.) y tecnologías (voz, datos, convergentes, etc.). Esta norma está técnicamente alineada con la '*ISO/IEC 18028-2 Information technology - Security techniques - IT network security - Part 2: Network security architecture*' aunque no es la misma. [14]

La Recomendación de la serie '*ITU-T M.3050.x Enhanced Telecom Operations Map (eTOM)*' [34] describe un marco de referencia para los procesos de negocios de un prestador de servicios y proveedores del sector de las telecomunicaciones: '*Enhanced Telecom Operations Map ®*' (abreviado eTOM).

eTOM: *enhanced Telecomunication Operation Map,* es un marco de referencia para los procesos de negocios de la industria de las telecomunicaciones, , desarrollado por el TM Forum (*Telemanagement Forum*) ampliamente difundido y aceptado internacionalmente permite describir y analizar de acuerdo a su prioridad los procesos de negocios, agrupando por áreas de competencia y permitiendo llegar al detalle de actividades. [33].

"ISO/IEC 27011 - Information technology - Security techniques - Information security management guidelines for telecommunications organizations" provee una guía de requerimientos específicos para las empresas del sector de las Telecomunicaciones.

"*ISO/IEC 18028 Information technology -- Security techniques – IT network security*", esta norma consta de cinco partes complementarias y refiere a la gestión de seguridad en redes.

4.3.1.2 Contexto Institucional

Como se muestra en la Figura 4.3, el ISP en consideración, debe respetar por un lado los lineamientos corporativos que en este caso provienen de la TelCo. Por otro lado debe alinearse con las pautas generales de políticas y estándares del estado.
Existe por lo tanto, además de una estructura de lineamientos jerárquicos, la necesidad de armonizar y alinear las necesidades de seguridad de forma coordinada.

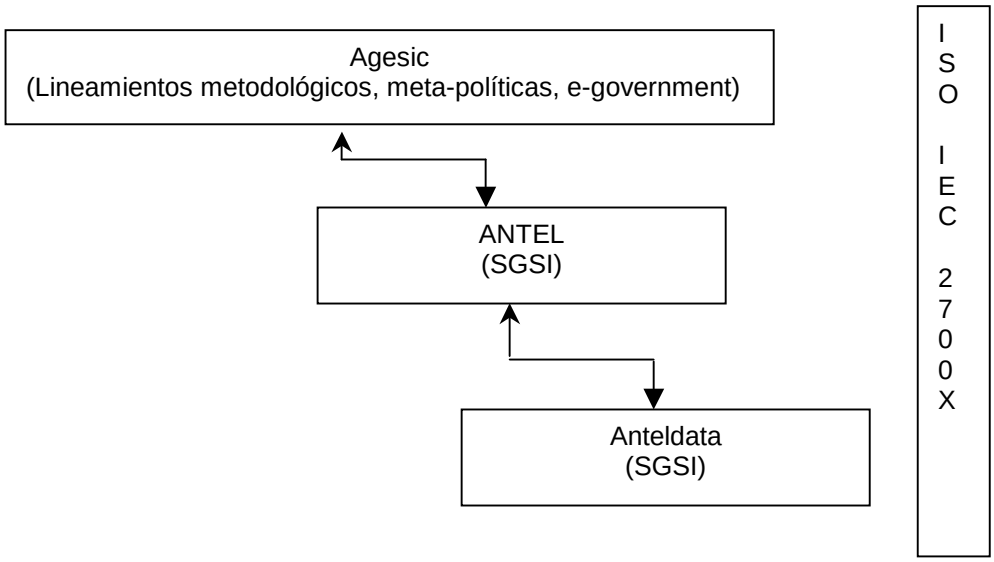


Figura 4.3 – Posicionamiento Institucional del ISP del Caso de Estudio

Aspectos a tener en cuenta:

Debe considerarse la Misión / Visión de la Organización, valores claves o estratégicos. Sector en el que se desarrolla el ISP y características propias del grupo: ISP - TelCo.
Objetivos y prioridades respecto al desarrollo de los servicios de acceso a Internet, servicios de valor agregado, telecomunicaciones, etc.
Debe considerarse aquí, la relación con las políticas globales con la TelCo. Debe explicitarse como inciden y en que grado son vinculantes y obligatorias las políticas generales sobre las particulares del ISP y cual es su relación.

En la Figura 4.4 se ilustra en un alto nivel, el contexto institucional del Caso de Estudio.

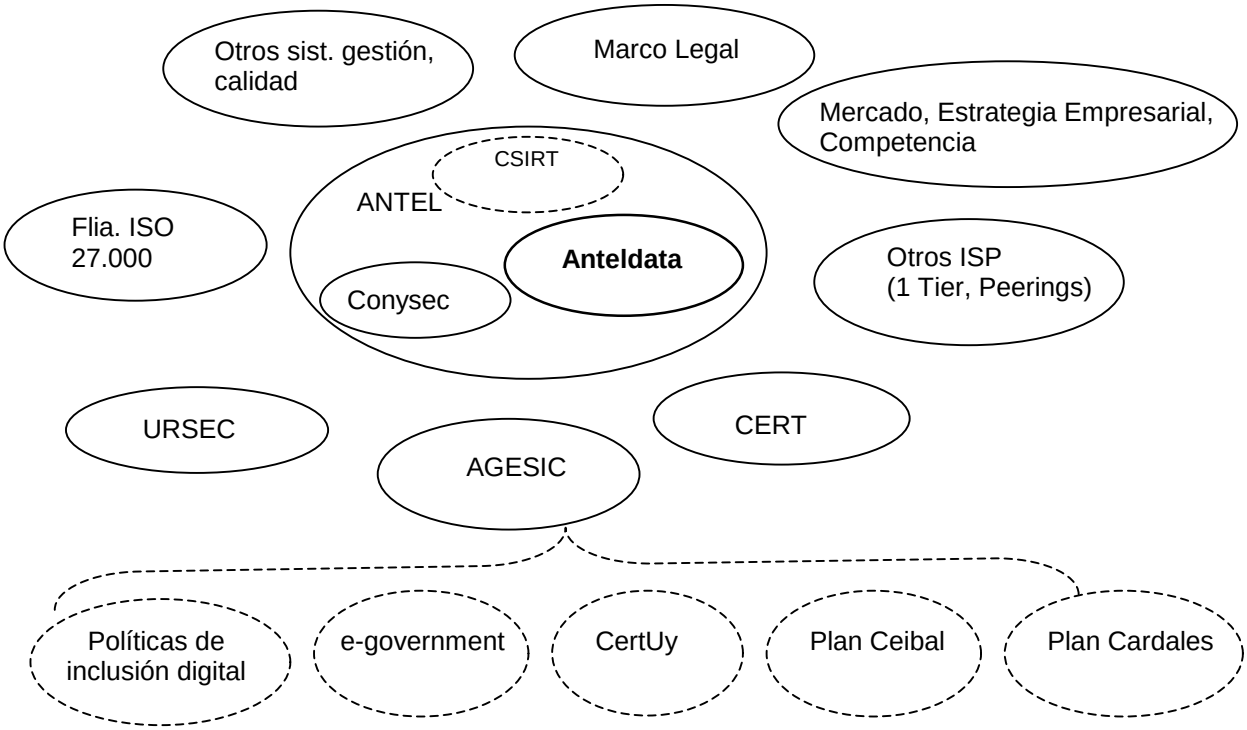


Figura 4.4 – Contexto Institucional del SGSI del Caso de Estudio

Otra forma de verlo es la ilustración de la Figura 4.5, donde se instancia con el Caso de Estudio lo representado en la Figura 3.8 de este documento, explicitándose la relación entre las diferentes empresas, organizaciones, estándares y marcos normativos y metodológicos, a los efectos de inferir los requerimientos extendidos de la seguridad de la información.

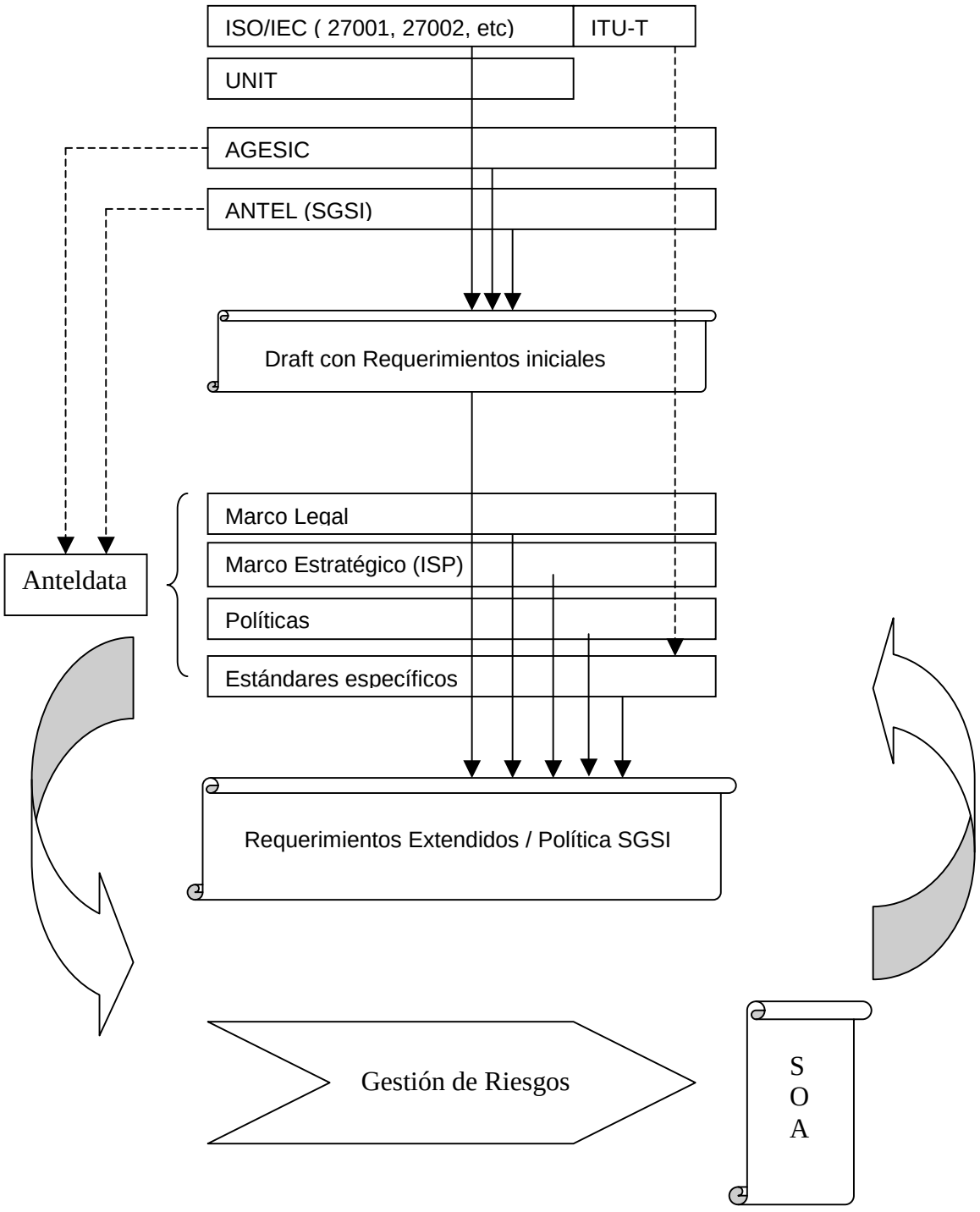


Figura 4.5 – Determinación de los Requerimientos extendidos del SGSI

4.3.2 Definición de los Requerimientos de Seguridad del Negocio

Consideraremos en esta sección:

a. Misión y Visión
b. Características inherentes al negocio / industria (TelCo - ISP)
c. Clasificación de los ISP
d. Vista conceptual de la infraestructura de Internet.
e. Infraestructura de un ISP.
f. Mapa de Operaciones - Modelo Descriptivo, Funcional y Organizacional

4.3.2.1 Misión y Visión

El SGSI deberá estar alineado con la Misión y Visión del negocio.

A modo de ejemplo se cita a continuación la Misión y Visión de Anteldata ([25]):

Misión:
'Brindar la más amplia gama de soluciones de telecomunicaciones para satisfacer las necesidades de todos los clientes potenciales, utilizando las más modernas tecnologías con eficacia y eficiencia'.

Visión:
'Ser el actor principal en el desarrollo de los negocios de conectividad y ancho de banda en Uruguay'

4.3.2.2 Características inherentes al negocio / industria (TelCo - ISP)

Existen algunas características que hacen que un ISP no sea una empresa más en lo que a la seguridad de la información e implantación de un SGSI refiere.

Una característica de los ISP es la heterogeneidad de sus clientes, y por ende, la diversidad de los niveles de seguridad existentes y también requeridos. Sumado esto a que dado que los clientes conviven en la red, las vulnerabilidades de unos pueden terminar afectando a otros, eventualmente vía el ISP.

Por otra parte debe lograrse un balance con los niveles deseados de seguridad y la calidad de servicio. Por ejemplo a veces la reasignación de un IP dinámico a una persona podría implicar 'heredar' además potenciales penalizaciones correspondientes al usuario anterior. (Por ejemplo bloquear el tráfico proveniente de un IP que es en realidad dinámico).

[25] En el Anexo A se presenta más información detallada para Anteldata y la región.

En otro sentido, vulnerabilidades que aún siendo críticas en cualquier organización, en el caso de un ISP se ven potenciadas. Este es el caso por ejemplo de una vulnerabilidad que sea explotada en un DNS. Este hecho no afecta únicamente al ISP sino a toda su comunidad de usuarios, y esto es crítico, para el negocio del ISP por supuesto, y para el negocio de terceros (los clientes).

Es decir, podemos enumerar una serie de características que conviene tener presente al momento de analizar la estrategia de la seguridad de la información o la definición, implantación y monitoreo de un SGSI.
A saber:

- Heterogeneidad de los clientes (y por ende de los niveles de seguridad).
- Perímetro de seguridad difuso. Fronteras no claras.
- Interacción y sensibilidad de la calidad del servicio entre clientes o con el propio ISP.
- La red es en este caso Internet.
- Servicios basados en software y en tráfico.
- La disponibilidad de los servicios de manera confiable es el primer cometido.
- Complejidad de la infraestructura.
- Cada elemento de la red es un potencial foco de ataque, y a su vez, un potencial recurso para un ataque, y esto cobra especial importancia en el caso de un ISP.
- La implantación de un SGSI (y sobre todo la certificación de la norma ISO 27.001), en una primera instancia puede ser un elemento estratégicamente y desde el punto de vista empresarial: diferenciador de la competencia (para un ISP), pero prontamente será una obligación y una necesidad para permanecer en el mercado, ya sea por reglamentación o porque los clientes exigirán ese nivel de calidad de servicio y será por lo tanto, un requisito para competir.

Por lo tanto, una primera observación, es que la Seguridad para el sector, si bien puede ser en una primera instancia un elemento diferenciador, seguramente pronto se convertirá en una condición necesaria para permanecer en el mercado de forma competitiva. Desde el punto de vista del mercado y del cliente, la Seguridad del ISP si bien antes y aún en el presente, puede dar un valor agregado a los productos ofrecidos en el sector, muy pronto tendrá el comportamiento similar a un "*commodity*", donde ya no es un valor adicional sino simplemente algo que se da por hecho, y por lo tanto no es diferenciador, sino imprescindible, regulado por la legislación / normativa vigente, requerido por los estándares internacionales y exigible por los clientes. Por ejemplo puede ser un requisito exigido en un pliego particular de condiciones de licitación.

4.3.2.3 Clasificación de los ISP

Podemos clasificar los ISP según determinados criterios, por ejemplo, alguno de ellos pueden ser:

- Jerarquía de Internet: Tier 1-ISP/ ISP de Backbone, Tier 2-ISP, CDN-ISP (Content Distribution, Hosting) [5]
- Estatales vs. Privados,

- Con infraestructura de comunicaciones propia vs. subarrendada (grado de independencia, contingencias de enlace internacional, satélite etc.),
- Nacionales vs. Internacionales.
- Por su dimensión / escala: Cobertura (Internacional, nacional, regional, etc.), ancho de banda, etc.
- Por las tecnologías utilizadas (*wireless* o *wired*)
- Estructura del mercado: en régimen de monopolio, oligopolio o competencia.
- Por el sector del mercado al que apuntan (empresarial / corporativo o doméstico) etc.
- Por la diversidad de la oferta (portafolio de productos): adsl, wireless: banda ancha móvil, LMDS, cable modem, etc.

Sin embargo, una clasificación que resulta interesante para este trabajo entre todas las posibles, es la de los ISP que están relacionadas verticalmente ([26]) con una empresa de telecomunicaciones (en adelante TelCo). Entre ellas podemos distinguir:

- Aquellas cuya empresa principal (o madre) es una Telco que además da origen al ISP como área de negocio específica.
- Un ISP que adquiere (o eventualmente establece una alianza de negocios) con una Telco.

Sin pérdida de generalidad, pero intentando concretar el caso de estudio por claridad, nos concentraremos en el primer caso. Este caso es además, el de uno de los ISP más importantes de nuestro país, Anteldata, el cual es motivo de referencia concreta de este trabajo que se describen en el Anexo A.
En estos casos, la propia estructura empresarial, hace que la relación jerárquica afecte y defina, no sólo las estrategias empresariales sino las diferentes políticas, lineamientos y procedimientos a seguir en los diferentes ámbitos. En especial, y en lo que nos atañe, a las políticas de seguridad, y por ende a la implantación de un SGSI.

4.3.2.4 Vista Conceptual de la Infraestructura de Internet

En la Figura 4.6 se ilustra una abstracción de la Infraestructura de Internet, en términos conceptuales, ubicando a los ISP entre los proveedores de servicio de *Backbone* y los usuarios finales.

[26] En general en estos casos, se da que el ISP es propiedad de la TelCo, pero podría ser al revés, o incluso que la dependencia sea parcial.

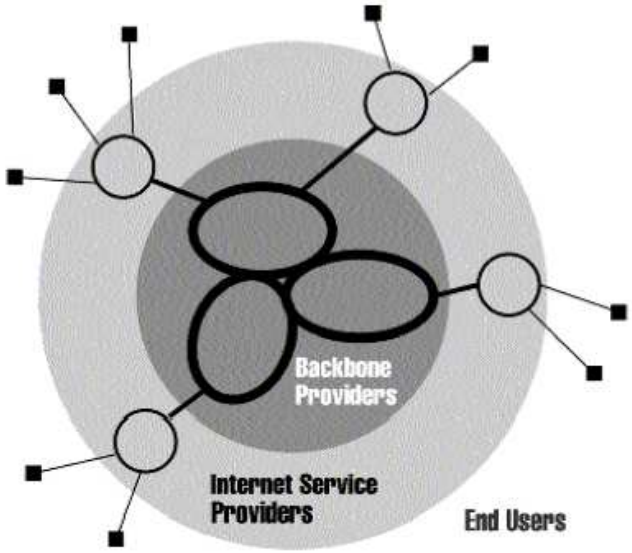


Figura 4.6 – Vista Conceptual de la Infraestructura de Internet [5]

4.3.2.5 Relación ISP – TelCo

Un ISP y una TelCo se pueden integrar verticalmente como muy buenos aliados o socios de negocios de la siguiente manera:

Por un lado la Telco provee al ISP de servicios de infraestructura, por otro lado amplía su portafolio de servicios (sobre IT) permitiéndole reaccionar de forma ágil y enfocada a las necesidades de los mercados y la evolución tecnológica. El ISP puede además proveer servicios técnicos.

Además eventualmente pueden compartir la infraestructura edilicia y eventualmente los servicios de soporte, logísticos y administrativos que se requieren en ambas empresas.

En la Figura 4.7 se observa como el ISP y la TelCo se pueden complementar en la provisión de servicios de comunicaciones [85]. Para ilustrarlo se utiliza el modelo OSI y se establece además una correspondencia ([27]) con el modelo TCP/IP [87].

[27] Existe más de un paralelismo o mapeo en la literatura con pequeñas diferencias que no son relevantes para el tema que aquí se trata, algunos ejemplos: [86][87][88].

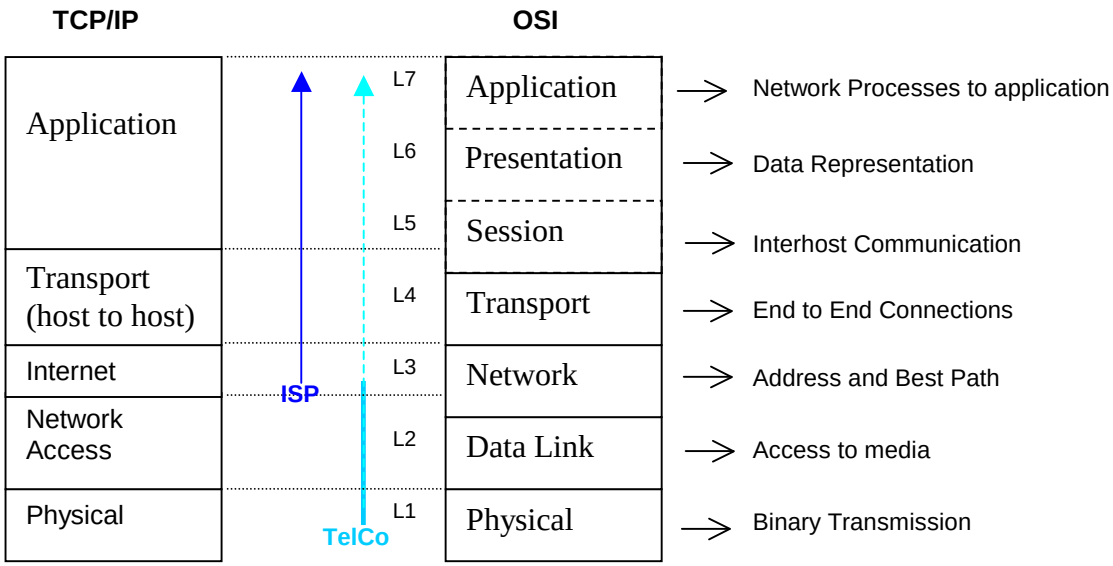


Figura 4.7 - Servicios ISP – TelCo, respecto del modelo OSI y TCP/IP [85] [87]

No se pretende aquí, modelar el alcance del negocio ni generar polémica de hasta dónde llegan o desde dónde deben partir los servicios de la TelCo y el ISP, ya que ese posicionamiento tiene aspectos técnicos y de modelo de negocios, el punto que interesa reflejar es que existirán dependencias interempresariales, en la calidad de los servicios prestados y en la seguridad de los mismos.

En particular podemos instanciar una posible configuración como se muestra en la Figura 4.8, donde se ilustra como servicios e infraestructura de la TelCo soportan servicios del ISP:

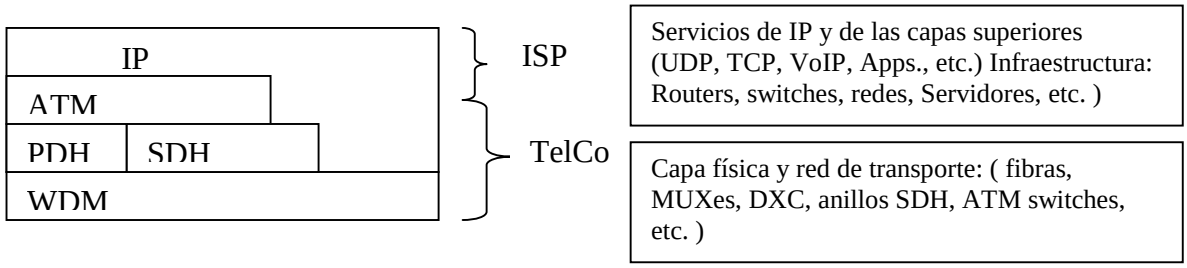


Figura 4.8 – Protocolos del Stack IP (fisico/ acceso al medio, Transporte e IP)

Tal como se mencionó en "*3.1.1 Aspectos relacionados a la estructura jerárquica empresarial*" esas dependencias entre empresas, que generan riesgos con complejidades adicionales, y hablando ahora en general ya no referidos ni acotados al ejemplo anterior, deben ser analizados y tratados en todo su alcance y de forma consistente y coordinada, de forma de que los controles que se implementan sobre ciertos servicios no se vean burlados por falta de controles en otros servicios posiblemente dependientes de la otra empresa. Esto requiere de esfuerzos coordinados y alineados.

4.3.2.6 Infraestructura de un ISP

En términos de infraestructura, un ISP básicamente se compone de:

- Backbone / Core
- Agregación / Distribución
    - Servicios internos
    - Servicios al Cliente (ADSL, Frame Relay / ATM, etc.)
- Convergencia (de ambos: Servicios y Protocolos).
    - Red Multiservicio
    - Servicios TV (IPTV),
    - Plataforma de Pagos,
    - VoIP
    - Correo electrónico
    - Datos
    - MPLS
    - VideoStreaming
    - 3play, 4play
    - Video en Redes 3G (DVB-H)
    - SaaS (Software as a Service)
    - Otros (VPN, L2 Tunneling, etc.).

En la Figura 4.9 se muestra de forma gráfica en un alto nivel la infraestructura de internet (y de un ISP). Allí podemos diferenciar tres capas, ellas son:

- *Core*
- Distribución
- Acceso

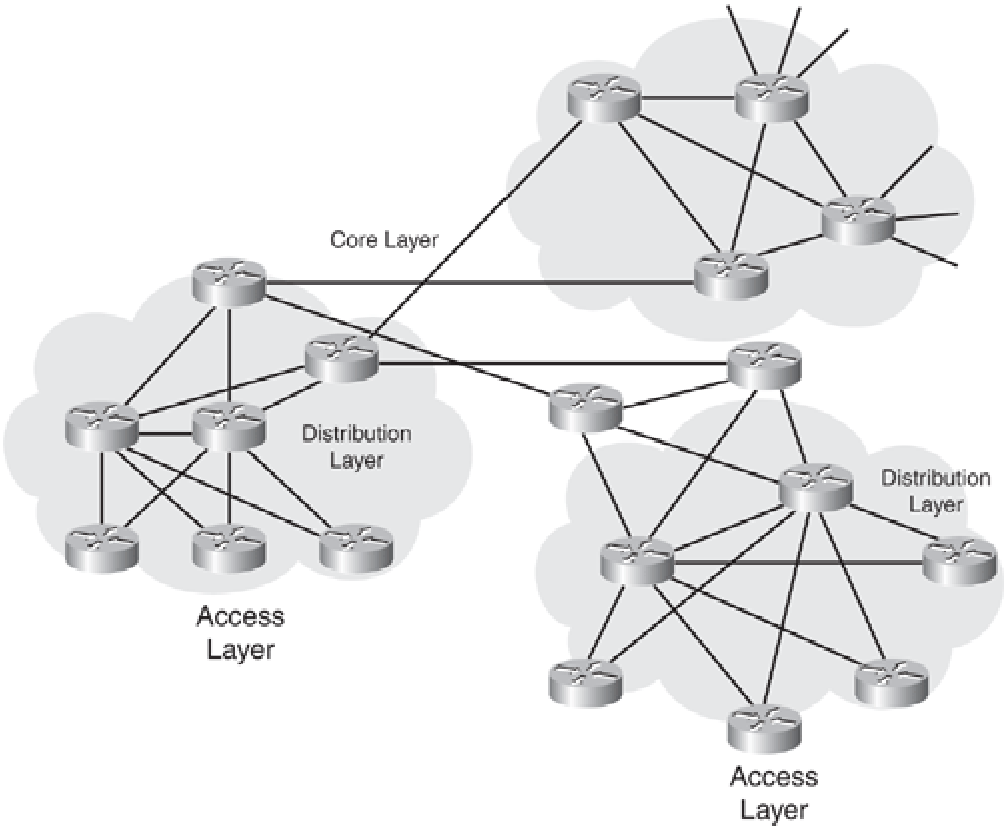


Figura 4.9 – Vista Conceptual de la Infraestructura de un ISP [45]

4.3.2.7 Mapa de Operaciones - Modelo Descriptivo Funcional y Organizacional

A los efectos de alinear los enfoques, el análisis de procesos, estrategias, activos, etc., atendiendo a la necesidad de armonización antedicha, es conveniente que tanto el ISP como la TelCo en cuestión, utilicen herramientas de análisis y enfoques que sean *mapeables* de forma de facilitar la identificación de prioridades, estrategias, dependencias, etc. y armonizar tanto sus planes de gestión, como lo que nos ocupa en este trabajo de tesis, sus Sistemas de Seguridad de la Información.

Atendiendo a los nuevos servicios digitales, al crecimiento de los servicios ofrecidos, a la convergencia y a la necesidad por lo tanto de interoperabilidad y de integrarse, tanto los sistemas y aplicaciones como las empresas (el ISP con la TelCo, con otros ISP y proveedores), es conveniente que exista un modelo descriptivo de gestión en el que fácilmente se puedan comparar, identificar y *mapear* aspectos comunes y coincidencias, así como también detectar diferencias a salvar.

Es por eso que decíamos que si bien, el modelo no está orientado a la Gestión de la Seguridad de la Información, sirve como *framework* y punto de partida para establecer un lenguaje común para 'dialogar' e interpretar las realidades de cada empresa.

Este modelo común, facilita la interpretación de la organización y procesos de negocios del ISP y la TelCo, permitiendo alinear planes estratégicos, establecer un criterio y cierto orden para la agrupación y clasificación de la información, activos, procesos y evaluación de riesgos.

Por lo tanto, en la medida que se comparta el enfoque, en descripción de modelos de gestión y planes estratégicos y operativos comparables, será más fácil la tarea de establecer, integrar y armonizar sus Sistemas de Gestión de la Información, de forma colaborativa y/o cooperativa, buscando eficacia, eficiencia y la autonomía requerida de cada una de las empresas, pero a su vez respetando los lineamientos y políticas corporativas.

Existe un modelo del Foro de TeleGerenciamiento (parte de la ITU-T) denominado eTOM (*enhanced Telecom. Operations Map*) que, si bien no está orientado a la Seguridad de la Información, es un modelo descriptivo que contextualiza el alcance de los procesos de negocios requeridos por un proveedor de servicios y sus interacciones. Como puede observarse en la Figura 4.10, el mismo además identifica áreas y actividades tanto de carácter vertical (de especialización y diferenciación del negocio) como transversal (de soporte y globales a toda la empresa).
Este modelo fue adoptado como *ITU-T International Recommendation M.3050*.

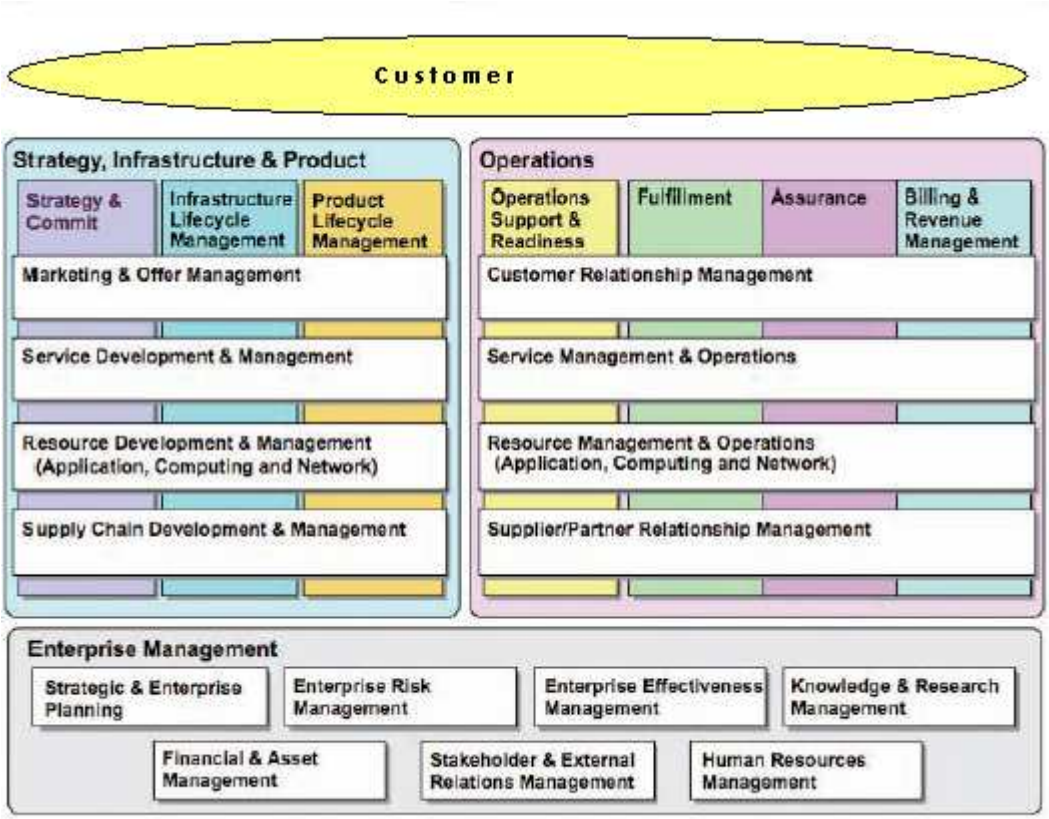


Figura 4.10 – enhaced Telecomunication Operations Map (eTOM)

En particular, el Proceso *Enterprise Risk Management* (Gestión de riesgos) se compone como se ilustra en la Figura 4.11.

Figura 4.11 – Desagregación del Proceso de Gestión de Riesgos de eTOM

Es decir:

Gestión de Continuidad del Negocio: Aseguramiento de los planes de contingencia y protección de los activos y procesos críticos para que el negocio continúe funcionando aún ante la ocurrencia de imprevistos e incidentes. Definición de estrategias, planes, políticas, procedimientos, y definición y asignación de roles y responsabilidades para que así ocurra.

Gestión de la Seguridad ([28])

Gestión Anti-Fraude: Políticas, lineamientos, mejores prácticas, controles y procedimientos a los efectos de evitar o minimizar las posibilidades de actividades fraudulentas.

Auditoría: Aseguran la adopción de los estándares relevantes y vigilan la efectividad de los controles definidos para los procesos y activos empresariales.

Gestión de Seguros: Asesora y gestiona los activos empresariales contra riesgos asegurables.

Gestión de Cobranza y Rentabilidad: Establece una política para asegurar la cobranza, minimizar la morosidad en pro de la rentabilidad de la empresa.

En el Anexo E se describe más detalladamente el modelo completo de eTOM.

Por otra parte, en el Reporte Técnico "TR143 Building Bridges ITIL and eTOM" [35] se establece una estrategia que permite combinar ITIL y eTOM a los efectos de complementar ambos modelos y obtener las ventajas de ambos.

4.3.3 Alcance y limites

Deben considerarse el marco legal y estratégico del ISP, así como las condicionantes (aspectos socio-culturales, regulaciones, distribución geográfica, autonomía, expectativas de los clientes,

[28] En este contexto refiere a: Gestión de amenazas, vulnerabilidades, controles, etc.

restricciones financieras, de potestad, etc.). También debe considerarse el contexto a nivel de políticas del gobierno o de estado con respecto a las tecnologías y seguridad de la información.

Algunos ejemplos de alcance y límites pueden ser: Una aplicación crítica, la infraestructura de IT, un proceso de negocio, o una parte de la organización. En este caso, el ISP.

Como se menciona en la metodología definida deben considerarse: planes estratégicos, operativos y de continuidad del negocio, así como el marco legal. A continuación se mencionan algunos de los componentes que deben ser tenidos en cuenta:

Hardware: Routers, *Servidores*, *Switches*, *Firewalls*, etc.
Software de base: SO, DBMS, etc.
Otros: *Firewalls*, *IDS*, etc.
Software de Gestión: Aplicaciones ([29]) / ERPs, *Scripts*, Herramientas / *Case*
Datos: Bases de datos, repositorios de información.
Documentación: Políticas, procedimientos, mejores prácticas.
Políticas e infraestructura de Control de Acceso: AAA
Técnicas de Seguridad Forense: Preservación de Evidencia.
DataCenter / Colocation
Backup Storage (SANs, cintas, discos, otras)
Protección de la Privacidad de los Datos. Información de Clientes.
Informes de Auditorias. Vulnerabilidades conocidas.
Información estadística.
Información Comercial. Información Técnica. Proyectos. Finanzas, etc.
Negocios, Contratos y Marco Legal.
Servicios: HTTP, DNS, SMTP, NTP, tráfico / datos, etc.
Plataformas / Aplicativos: Correo electrónico, Servicios de TV ([30]) , Plataforma de Pagos. Red Multiservicio.
Relaciones con otros ISP (*Tier* 1, *Peerings*, etc.)
Relaciones con Proveedores.
Relaciones y Calidad de Servicio al Cliente.

4.3.4 Política del SGSI

Como se vio en la metodología propuesta, deben especificarse los criterios, principios y lineamientos fundamentales con respecto a la seguridad de la información. Si serán heredados de la TelCo (lineamientos Corporativos) y además se complementarán con criterios propios más específicos. Cómo se gestionarán los riesgos y que mecanismos existirán para escalar los riesgos y priorizar los mismos para su atención.
Deben especificarse los requerimientos del ISP en cuanto a la seguridad de la información, atendiendo a la normativa / legislación vigente, a los estándares de la industria y las mejores prácticas del sector. Deberán atenderse además las cláusulas relativas a la seguridad de la información incluidas en los contratos (SLAs).

[29] Comerciales o a medida
[30] Por ej. Adinet TV

Cuando la política del SGSI de la TelCo alcanza también al ISP, puede esperarse en general que los principios y lineamientos directrices de la seguridad de la información sean muy similares o coincidan, sin embargo la estructura normativa y requerimientos contractuales pueden ser diferentes.

Quien debería participar:

a. Gerencia / Dirección.
b. Comité de Seguridad.

4.3.5 Análisis de Gap

Antes de definir un plan de acción concreto tanto para el corto, mediano y largo plazo, debe evaluarse cuanto dista la situación actual del ISP en lo que a la seguridad de la información se refiere, considerando la política definida.

Los objetivos y alcance deberán estar alineados con la realidad del ISP y sus prioridades, así como salvar las condicionantes y prever recursos acorde a la dimensión de la tarea a realizar considerando el escenario de partida y el escenario planteado como meta.

Entrada:

a. Análisis del negocio y posicionamiento del ISP en lo que a la seguridad de la información refiere.
b. Normas, Estándares y Recomendaciones. (ISO/IEC, UNIT, ITU-T, etc.)
c. Marco jurídico normativo y contractual.
d. SGSI de la TelCo y políticas corporativas.

Acción:

Posiblemente los procesos más relevantes ya estén identificados como resultado de otros planes estratégicos y operativos. Puede además, utilizarse como guía, los modelos TAM – eTOM [33][42]. Y para analizar los requerimientos en términos de confidencialidad, integridad y disponibilidad, las Recomendaciones de la ITU-T (además de los estándares ISO/IEC).
Como se mencionó en la metodología, esta etapa puede ser guiada por un consultor o especialista en Seguridad de la Información, que podría ser interno o externo con experiencia en el sector ISP-TelCo.

Quienes deberían participar:

a. Gerentes de línea y de las diferentes unidades de negocio, por ej.: Sistemas de Gestión y Procedimientos, OM&S ([31])
b. Comité de Seguridad.
c. Responsables de los procesos sustantivos (críticos y prioritarios) de la empresa.
d. Profesionales y especialistas con buen entendimiento del negocio así como los requerimientos y aspectos relevantes de la Seguridad de la Información.

[31] Organización, Mantenimiento y Servicios

e. La participación de Personal especializado en el área con experiencia en la implantación de SGSI en la industria puede ser un valor considerable.

Salida:

Un informe de situación respecto de el estado de la empresa en cuanto a la Seguridad de la Información y la distancia o los aspectos pendientes de resolver para llegar al nivel deseado.

4.3.6 Gestión de Riesgos

Como se vio en la metodología, la gestión de riesgos implica a grandes rasgos: la definición de criterios básicos, la identificación de riesgos, la estimación de los mismos y su tratamiento según corresponda.

En las siguientes secciones nos centraremos en las dos primeras actividades ya que la estimación de riesgos y su tratamiento ameritan focalizarse en riesgos concretos, y actividades de consultoría y una especificidad que escapan al carácter metodológico de este trabajo de tesis.

Quienes deberían participar:

De acuerdo a la Figura 4.10, la Gestión de riesgos del modelo eTOM se compone de:

- Gestión de la Continuidad del Negocio.
- Gestión de la Seguridad de la Información.
- Gestión de Prevención del Fraude.
- Auditoría.
- Gestión de Seguros.
- Gestión de Cobranzas y Rentabilidad.

Por lo tanto, será una responsabilidad de todas las gerencias involucradas. Una buena guía son las gerencias de línea y de soporte a la empresa que pueden observarse en la Figura 4.11.

La Dirección y Gerencia General tendrá la última palabra sobre cuales son los procesos / activos críticos y fundamentales para la continuidad del negocio, la cual se apoyará en las gerencias técnicas y asesorías especializadas.
Como se dijo en la especificación de la Metodología, deben participar profesionales especialistas en el negocio, con cabal conocimiento de los objetivos y estrategia de la organización, así como complementariamente de los aspectos relevantes de la seguridad y como puede afectar los intereses y objetivos empresariales.
Para ello es imprescindible el trabajo en conjunto y complementario entre los especialistas del negocio con especialistas en Gestión de Riesgos y Seguridad de la Información.

A otro nivel, el aporte de técnicos y especialistas en la materia así como otros en seguridad de la información, es imprescindible para identificar vulnerabilidades, amenazas, controles, etc. con una granularidad más fina.

Particularmente distinguimos:

a. Gerencia / Dirección del ISP.
b. Gerentes de línea o a cargo de unidades de negocio.
c. Responsables de procesos de negocios importantes ([32])
d. Otras personas con las características descritas.
e. Analista de Riesgos.
f. Especialista/s en la Seguridad de la Información.

4.3.6.1 Definición de Criterios Básicos

Para un ISP, el foco, objetivos a perseguir y lineamientos prioritarios pasan básicamente por:

- Escalabilidad, de la infraestructura y los servicios.
- Performance (Calidad de servicio requerida).
- La Disponibilidad (conectividad y servicios) es el principal cometido.
- Foco en la Seguridad para mantener la Disponibilidad.
- Robustez / sensibilidad a fallas.
- Visión y alcance de múltiples tecnologías y diversos planos de acción que requieren de diversas especializaciones técnicas y una metodología para coordinación de esfuerzos y maximización y alineación de beneficios.
- La empresa desarrolla su actividad dentro de un marco de competencia.
- Adopción e Integración con nuevas tecnologías / nuevos servicios.
- Marco Legal, Contratos, SLAs, etc.

Deben definirse en función de lo anterior, criterios específicos y concretos para: evaluación de riesgos, análisis de impacto y aceptación de riesgos, respectivamente.

Entre los principales activos que tiene un ISP sin dudas están: la confiabilidad de sus clientes en el servicio que redunda en el grado de fidelidad con la empresa.
La disponibilidad de las comunicaciones y los servicios es uno de los principales cometidos donde se requiere una determinada calidad de servicio en general comprometida en contratos y cláusulas de calidad de servicio acordado (SLAs).

Un incidente de seguridad que afecte esta percepción, puede causar más daño que la rotura de un servidor u otro hardware. Sabido es de los mercados financieros, que la confianza que se pierde, cuesta mucho más recuperarla que si se hubiese prevenido el incidente.
Otro ejemplo es, en un mercado donde se compite por productos similares o que pueden ser percibidos como equivalentes, la confidencialidad y oportunidad de la información, como puede ser la liberación de un nuevo producto o servicio, tiene eventualmente un impacto positivo en la diferenciación del servicio como un valor agregado, oportunidad y valor que se pierden si no se llega primero al mercado.

[32] Ver Figura 38 - Procesos de alto nivel alineados con el esquema de TAM - eTOM

4.3.6.2 Identificación de Riesgos

En la identificación de riesgos distinguimos: identificación de procesos prioritarios, identificación de activos, de amenazas, controles existentes y vulnerabilidades.

4.3.6.2.1 Identificación de los Procesos (e Información) Críticos

En el caso de un ISP, la disponibilidad de las comunicaciones y las calidades de servicio comprometidas (SLAs) son claves para el negocio y preservar la confianza de los clientes en un régimen de competencia (además de las connotaciones en términos contractuales y de regulación).
Una interrupción prolongada de las operaciones podría tener un impacto grave en la imagen institucional y en la confianza de los clientes de acuerdo a la calidad de servicio percibida. Esa desconfianza e incertidumbre seguramente impacte también los procesos de negocios de los clientes empresariales con pérdidas potenciales.
Pero por otro lado también, y más allá de incidentes operativos y recuperación de fallas – o eventualmente – desastres, debe evaluarse el impacto al negocio en términos estratégicos y de ventaja competitiva. ¿ Como afectaría por ejemplo a la empresa la revelación del plan de negocios o del lanzamiento de un nuevo producto a la competencia ?

Entrada:

a. Identificación de los procesos críticos y prioritarios desde la percepción de la TelCo.
b. Know – How del negocio.
c. Planes existentes de Continuidad del Negocio.
d. Plan Estratégicos y Operativos.
e. Análisis de Organización & Métodos.

Acción:

Referirse a la Metodología, en el capítulo 3.2.8.4.3 – Identificación de Riesgos.

Salida:

En la Figura 4.12, extraído de los modelos eTOM – TAM, se clasifican los procesos y responsabilidades principales por áreas y/o Gerencias, lo cual es una buena base que sirve de ejemplo para identificar en un alto nivel, los procesos críticos.

Market/Sales	
V	Campaign Management
V	Channel Sales Management
V	Corporate Sales Management
Product Management	
V	Product Performance Management
V	Product Catalog Management
V	Product Strategy/Proposition Management
V	Product Lifecycle Management
Customer Management	
V	Customer Information Management
V	Customer Self Management
V	Customer Contact, Retention & Loyalty
V	Order Management
V	Quotation Engine
V	Customer QoS/SLA Management
V	Customer Service/Account Problem Resolution
V	Customer Billing Management
V	Invoicing
V	Collections Management
V	Bill Formatting
V	Receivables Management
Service Management	
V	Service Specification Management
V	Service Inventory Management
V	Service Configuration Management
V	Service Design/Assign
V	SLA Management
V	Service Problem Management
V	Service Quality Monitoring and Impact Analysis
V	Service Performance Management
V	Service Rating/Discounting Management

Resource Management	
V	Workforce Management
V	Resource Specification Management
V	Resource Inventory Management
V	Resource Design / Assign
V	Resource Provisioning / Configuration
V	Resource Logistics
V	Resource Testing Management
V	Resource Activation
V	Resource Planning / Optimization
V	Resource Domain Management (IT Computing, IT Application, Network)
V	Resource Performance Monitoring / Management
V	Resource Problem Management
V	Correlation & Root Cause Analysis
V	Resource Status Monitoring
V	Resource Data Mediation
V	Arbitrage Management
V	Voucher Management
V	Billing Data Mediation
V	Real-time Billing Management
Enterprise Management	
V	Revenue Assurance Management
V	HR Management
V	Financial Management
V	Asset Management
V	Security Management
V	Knowledge Management
V	Fraud Management
Supplier/Partner Manager	
V	Partner Management
V	Supply Chain Management
V	Wholesale/Interconnect Billing Application

Figura 4.12 - Procesos de alto nivel alineados con el esquema de TAM - eTOM

Identificación de Activos

Como se especifica en [18], debe realizarse un inventario clasificando los activos, asignando un dueño / responsable del mismo, sus políticas de uso, y donde deben además determinarse claramente las responsabilidades de la empresa con terceros, esto incluye, a la propia TelCo, otras empresas relacionadas, por ejemplo otras empresas de telecomunicaciones.

Algunos aspectos a considerar para el caso concreto de un ISP:

a) Información:

Información de nuevos proyectos y nuevos productos. Workflow de un nuevo producto desde su concepción, planificación, diseño hasta el lanzamiento comercial.
Información de (potenciales) clientes y aspectos comerciales (contratos). Información privada / personal de terceros.
Información técnica (Operaciones, Soporte, etc.). Configuraciones. Problemas detectados, vulnerabilidades conocidas, utilización de ancho de banda, etc.
Datos de Comunicaciones: tráfico, información de ruteo, logs, información estadística, patrones de comportamiento, información de cobranza, etc.
Planificación estratégica. Aspectos competitivos.
Planes de Continuidad del negocio.
Información financiera y contable: cuentas de clientes y proveedores, movimientos, pagos, etc.
Documentos y pistas de Auditoría.
Documentación de sistemas / aplicaciones, manuales.
Documentación de I+D.
Bases de datos, repositorios, archivos, logs, etc.

b) Software:

Aplicaciones (desarrollos propios y de terceros, a medida y paquetes), software de base (DBMS, SO, etc.), ERPs, herramientas de desarrollo, CASE, etc.
Específicamente además, software de control y gestión de operaciones, analizadores de tráfico, gestión de red, gestión de cobranza, etc.

c) Recursos Humanos:

Profesionales, técnicos, administrativos etc., con sus calificaciones y capacidades (formación y aptitud), know-how, experiencia, etc. Relaciones con terceros.

d) Aspectos de Infraestructura y Servicios:

- Backbone / Core
- Agregación / Distribución
    - Servicios internos
    - Servicios al Cliente
- Infraestructura edilicia, acondicionamiento térmico y eléctrico. Infraestructura anti-incendios y desastres naturales, etc.
- Hardware: infraestructura de red (elementos de red activos: routers, switches, etc. y pasivos: cableado por ejemplo), servidores, PCs / terminales, otros.
- Servicios:

Del negocio:

Convergencia (de ambos: Servicios y Protocolos).

- Red Multiservicio
- Servicios TV,
- Plataforma de Pagos,
- VoIP
- Correo electrónico
- Datos
- MPLS
- Servicios sobre ADSL, etc.

Otros (propios o relacionados al negocio):

- Generación y distribución de contenidos.
- Software as a service (SaaS).

De soporte y actividades transversales (o no sustantivas):

- Call center / atención al cliente,
- Gestión financiera y de cobranza, etc.

Intangibles: Percepción de la empresa en el mercado / opinión pública, reputación, imagen, posicionamiento frente a la competencia, know-how organizacional, etc.

En particular, la convergencia, y la tendencia a los servicios basados en IP, en conjunción con el crecimiento que ha tenido la banda ancha, la masificación de servicios on-line, y el impulso que esto le ha dado a la economía, hace que aparezcan nuevas amenazas así como atractivos o incentivos para quebrar la seguridad que tienen una clara motivación económica. Por otra parte, la convergencia genera dependencia y mayor criticidad de la infraestructura y los protocolos que deberá considerarse para el análisis de riesgos.

4.3.6.2.2 Identificación de Amenazas

Entrada:

a. Incidentes reportados, estadísticas locales (CSIRT / CERT).
b. Reportes específicos, de organizaciones reconocidas, de amenazas para ISPs. (ej. *Arbor Networks*). Estadísticas de amenazas globales.
c. Informes y aportes de los “dueños de los activos” (de información).
d. Especialistas y técnicos del dominio de aplicación.
e. Especialistas en Seguridad de la Información.

Acción:

Debe tenerse un mapa estadístico o catálogo de amenazas bien identificado y lo más completo posible, considerando, tanto amenazas internas como externas, factores humanos y acciones deliberadas como accidentales, ambientales, etc.

Es muy importante referirse a estadísticas globales de los ISP, así como aquellas que afectan y se detectaron en otros ISPs comparables o cercanos ("*Peerings*") y por supuesto estadísticas propias y detectadas a nivel nacional.
Deben clasificarse las amenazas según su naturaleza.
Recordamos aquí que es importante mantener actualizado este escenario de amenazas debido a que las mismas muchas veces son variantes de otras anteriores y surgen nuevas.

En la Recomendación ITU-T Rec. X.800, *Security architecture for Open Systems Interconnection for CCITT applications*, y creemos que aplica también para el Caso de Estudio, se detectan como amenazas:

- Destrucción de la información y/o otros recursos;
- Corrupción o modificación de la información;
- Robo, pérdida y/o borrado de la información y otros recursos;
- Divulgación de la información ([33]);
- Interrupción de los servicios.

Por otra parte en la Recomendación X.805 [14], como se detalla en el Anexo D de este documento, se presenta una matriz donde se hace un cruzamiento de las amenazas detectadas con las dimensiones de la seguridad de la información, ilustrado en el Cuadro 4.1.

Dimensión	**Amenazas**				
	Destrucción	Alteración/ Corrupción	Robo/ Borrado o Pérdida	Divulgación	Interrupción de los servicios
Control de Acceso	Si	Si	Si	Si	
Autenticación			Si	Si	
No Repudio	Si	Si	Si	Si	Si
Confidencialidad			Si	Si	
Comunicaciones			Si	Si	
Integridad	Si	Si			
Disponibilidad	Si				Si
Privacidad				Si	

Cuadro 4.1 Cruzamiento de las amenazas y dimensiones de la Seguridad de la Información

También es importante conocer la motivación en el caso de las amenazas deliberadas llevadas a cabo por acciones humanas.
Otro elemento a tener en cuenta que puede resultar de gran ayuda para la comprensión de ese mapa de amenazas son los vectores o vías por las que finalmente se llevan a cabo.

[33] no pública, a personas no autorizadas.

Tanto la motivación y las vías de concreción de las mismas (vectores) pueden ser el foco para las acciones preventivas y establecimiento de controles (o sanciones) que combatan o mitiguen el impacto no deseado o la concreción de la amenaza.

Salida:

Una lista de amenazas reales, clasificadas según su tipo y origen.

En la Figura 4.13 se presenta una gráfica con las amenazas más preocupantes para los ISPs según la encuesta representativa que se referencia en [4].

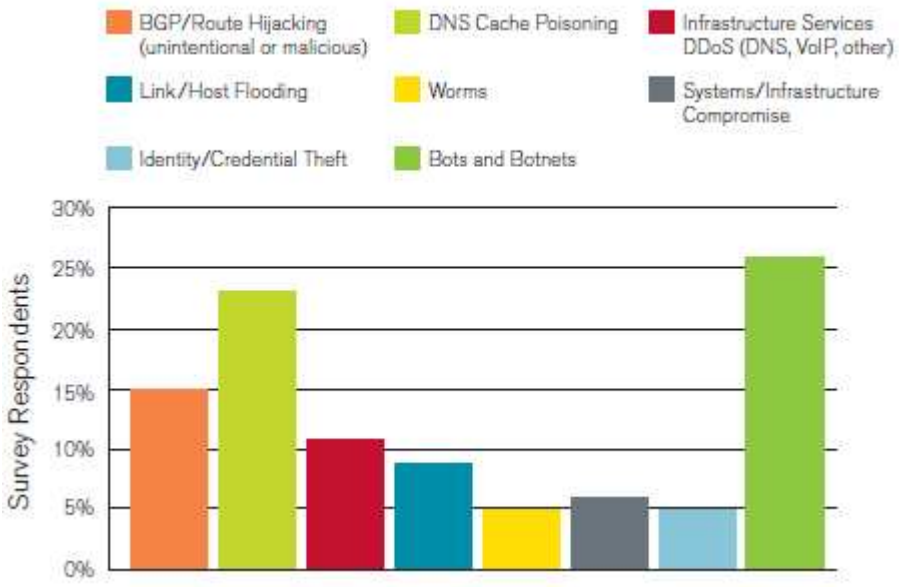


Figura 4.13 – Percepción de las principales Amenazas de un ISP [4]

En esta última gráfica podemos observar la dimensión de la percepción (creciente) de amenazas tales como *DNS Cache Poisoning* y de los *Botnets*, asociadas con la utilización de técnicas de *DNS Fast Flux* (*Single Flux* y *Double Flux*) [20] y [21].

4.3.6.2.3 Identificación de Controles

Entrada:

Documentación de los controles existentes.
Documentación de la Implementación del Plan de Tratamiento de Riesgos.
Informes y recomendaciones del Departamento de Jurídica, respecto a la legislación vigente aplicable.
Informes de Auditoría del propio ISP.
Informes o la percepción de los propios usuarios involucrados y el “dueño” de la información (especialistas del dominio).

Observaciones *on-site* de los controles físicos por ejemplo.
Informes de especialistas en seguridad de la información. (Grado de uso y efectividad de los controles). Estadísticas.
Informes de Auditorías previas de la TelCo.
Plan de Tratamiento de Riesgos del ISP y de la TelCo.
Informe de Controles implementados en el ISP y la TelCo

Acción:

Deben mantenerse actualizados y vigentes los informes de implementación de controles de planes de tratamiento de riesgos anteriores así como informes de auditoría. Deben considerarse tanto los controles existentes como aquellos incluidos en el Plan de Tratamiento de Riesgos.

También es importante armonizar los planes de tratamiento de riesgos del ISP como el de la TelCo relacionada, en aquellos riesgos que así lo permitan, o corresponda. Esto permite tener todos los elementos para una mejor evaluación de los riesgos reales y una utilización más racional de las inversiones en seguridad, priorizando con mayor certeza.

En el Anexo C se especifican una serie de Controles específicos para un ISP – TelCo, en el sentido de controles específicos que extienden los especificados en las normas ISO/IEC 27.001 (Anexo A) e ISO/IEC 27.002, tal como lo prevé la propia norma ISO/IEC 27.001.

Para la definición e implementación de controles, deben considerarse tanto: a) aspectos tecnológicos y de infraestructura así como b) aspectos humanos y procedimentales.

Salida:

Un escenario claro de los controles existentes y los planificados, su grado de implementación, uso y efectividad.

Considerando el Dominio de los ISP y sólo a modo de ejemplo porque escapa al alcance de este trabajo de tesis, algunos aspectos a considerar son:

a) Aspectos tecnológicos y de infraestructura:

Identificamos a continuación, con fines ilustrativos, algunos componentes tecnológicos de infraestructura de alto nivel, sobre los que habrá que establecer los controles apropiados, algunos de los cuales se listan a modo de ejemplo ([34]).

- Backbone / Core
  - Integridad de dispositivos / elementos de red
  - Autenticación de rutas
- Agregación / Distribución
  - Integridad de dispositivos / elementos red
  - Autenticación de rutas

[34] En algunos casos lo que se describe son objetivos de control.

  - Stateful / Stateless Firewall
  - Criptografía
  - Prevenir, la interceptación de comunicaciones no autorizadas, incluso en las interconexiones con otros ISPs
  - Controles de Spoofing, DDoS (L3).
- CPE Perímetro / Acceso
  - Gestión de Routers:
    - Cambios de Configuración
    - ACLs (IP, TCP, UDP)
  - Seguridad Gestionada
    - L3 filtros, mitigación DDoS (L3)
    - Seguridad L2 (*Firewall*, AAA, Integridad dispositivos)
    - Filtros url
    - Detección de patrones de comportamiento sospechosos o comportamientos reconocidos de tráfico hostil, uso de (N)IDS (*(Network) Intrusion Detection System*), *HoneyNets*, *Spamnets*
    - *Email: Spam, Phishing*, etc. Politica, listas negras, acciones cooperativas con otros ISP / TelCos.
    - Controles adecuados y gestión de los dispositivos (de red, servidores, etc.) e información de *routing* y control (ej. *DNS Poisoning*).
    - Protección de la información sensible de las comunicaciones y de la información personal y/o privada.
    - Detección y Prevención de ataques desde *botnets*
- Punto Final (*EndPoint*):
  - Integridad de dispositivos
  - AAA de usuarios y dispositivos. Autenticación, prevenir los accesos no autorizados, auditoría, etc.
  - Protección Hosts (*Firewall*, AV, *Spyware*, *hardenning*, OS *patches*, etc.)
  - Instalación: *Spyware*, *Adware*, *Keylogging*, *Click Fraud* (*Ad Sense* de Google por ej.)
  - File System (encripción)
  - Vulnerabilidad a Scanning

Como se afirma en [63], al igual que se da con otras áreas, la investigación en temas de seguridad, presenta la paradoja de la falta de información o elementos para poder analizar, ya sea porque se desconoce o por temas de confidencialidad, la misma se provee una vez detectados los riesgos, y a veces, cuando está disponible su solución; es decir, el riesgo ya tuvo su ventana de oportunidad y una amenaza pudo haberse hecho efectiva. Pero para identificar los riesgos es necesario investigar ("*problema del huevo y la gallina*").

A los efectos de salvar esta dificultad, es que se utilizan los *honeypots y honeynets* para detectar los comportamientos y técnicas utilizadas para intentar violar la seguridad. Además se establecen acuerdos entre CSIRTs y CERTs a los efectos de favorecer una comunicación oportuna de la forma más temprana posible.

b) Aspectos humanos, comerciales y procedimentales:

Deben considerarse además de los aspectos tecnológicos, aquellos que son propios de los procedimientos definidos y donde el factor humano tiene una especial relevancia. Un ejemplo de ello, son los controles necesarios en el manejo y gestión de la información confidencial. A continuación se mencionan algunos ejemplos.

- Información del lanzamiento de nuevos productos.
- Gestión y manejo de claves de acceso a información privilegiada
- Gestión de la información confidencial o privada / reservada.
- Datos privados, de la empresa y de clientes.
- Acceso Físico.
- Relaciones contractuales, comerciales y laborales.
- Acceso y gestión de la información privilegiada (infraestructura, futuros proyectos, información técnica, información confidencial de interés para la competencia), considerando aún los funcionarios que eventualmente dejan de pertenecer a la empresa.
- Advertir a los usuarios acerca de actividades de *spam*, crímenes cibernéticos, virus, *malware*, etc.

4.3.6.2.4 Identificación de Vulnerabilidades

En la Figura 4.14 se grafican los principales vectores de ataque a los ISP en el año 2008.

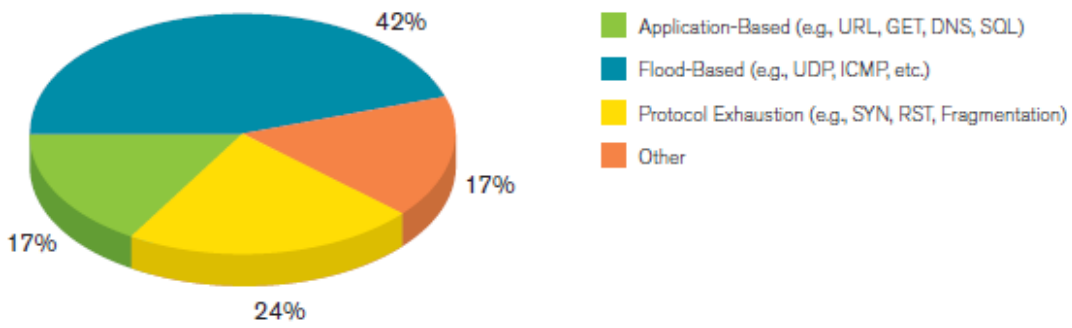


Figura 4.14 – Principales vías / vectores de ataque [4]

No obstante cabe recordar que deben considerarse además de los factores tecnológicos, factores humanos, procedimentales y de organización.

Es fundamental contar con un equipo técnico especializado y actualizado, así como estar en permanente contacto con organizaciones especializadas a nivel internacional, tanto del sector industrial como académico.

Es saludable la participación de Consultorías específicas y auditorías.

Las vulnerabilidades y las amenazas pueden deberse a factores internos, cuyo control está bajo el dominio de la empresa, pero también pueden deberse a factores externos, en nuestro caso, por ejemplo, si analizamos el servicio de VoIP, más allá de todas las vulnerabilidades que pudiera tener el servicio en si mismo, y las necesidades de QoS, debe tenerse en cuenta que el mismo, justamente por estar implementado sobre IP, dependerá de la red de transporte (ATM, SDH, capa física, etc.) que puede estar bajo el dominio de acción de la TelCo.
En otros casos, pueden existir dependencias, incluso fuera del grupo empresarial. Por ejemplo en [63] se analizan las dependencias mutuas que pueden darse entre una TelCo y la empresa generadora y proveedora de la energía eléctrica. Cómo un corte de energía podría condicionar la normal operación de la TelCo, pero también la dependencia que la empresa de energía eléctrica puede tener de la TelCo para la comunicación de sus sistemas de control y gestión operativa entre centrales.

4.4 Declaración de Aplicabilidad

Esta sección debe especificar los controles adecuados que aplican al SGSI.

Recordamos aquí que la norma ISO/IEC 27.001 especifica en su Anexo A, con carácter normativo un conjunto de Objetivos de Control y Controles. No obstante, esa lista no pretende ser exhaustiva y debe ampliarse de acuerdo a las necesidades del ISP – TelCo en este caso, como lo especifica la propia norma, de un modo general.

En particular, resulta de especial interés, los Objetivos de Control y Controles formulados en la recomendación ITU-T X.1051 / ANEXO C [18] que extienden el conjunto de controles generales y son específicos para el sector.

Entrada:

ISO/IEC 27.001, ISO/IEC 27.002, ITU-T X.1051, Análisis del Negocio y Evaluación de Riesgos.

Acción:

Deben considerarse:

- Los objetivos de Control y Controles para el Tratamiento de Riesgos (ISO/IEC 27.001-2, ITU-T X.1051 / ISO/IEC 27011 y eventualmente otros).
- Los objetivos de Control y Controles actualmente implementados (referirse a la sección “ 3.9.1.4 Identificación de Controles”).
- La justificación de la exclusión de cualquier Objetivo de Control o Control del Anexo A de la ISO/IEC 27.001.

Quienes deberían participar:

a. Gerencia / Dirección de la empresa.
b. Comité de Seguridad
c. Gerentes de línea y de las diferentes unidades de negocio.
d. Responsables de los procesos sustantivos (críticos y prioritarios) de la empresa.

Salida:

Declaración de aplicabilidad, justificando los controles que quedan excluidos.
Una vez que se tiene la aprobación de la Gerencia / Dirección, se remite para su consideración por la Gerencia General y Dirección del Grupo Empresarial.

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 atendiendo este aspecto estructural y jerárquico, con criterios alineados a la estrategia empresarial, y además de cooperación en todas las etapas del ciclo PHVA (*PDCA*), pero a su vez con la flexibilidad y agilidad operativa suficiente para alcanzar los niveles de seguridad necesarios y específicos a cada empresa, respetando los lineamientos corporativos.

Este trabajo aporta una metodología con esta concepción de enfoque global y sistémico, atendiendo a la pertenencia de la empresa a un grupo empresarial, y a su vez pragmático, a los efectos que la misma sea, no sólo viable, sino conveniente y efectiva, dando una estructura u organigrama para lograr la coordinación necesaria y especificando los procedimientos que deben cumplirse en cada fase, promoviendo no sólo la reutilización y coherencia integral de la seguridad sino también fomentando la sinergia entre las empresas del grupo.
Un producto parcial y homónimo de este trabajo de tesis, se ha constituido en una ponencia en el marco del "*V Congreso Iberoamericano de Seguridad Informática (CIBSI'09)*" en Montevideo, Uruguay, en noviembre de 2009.

En referencia a la estrategia de análisis y gestión de riesgos así como de planificación, implementación y seguimiento del SGSI, 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 adecuada y efectivamente el alcance del SGSI, una estrategia multifase que determine en una primera etapa los procesos y activos críticos, permite, en fases posteriores, dedicar el esfuerzo y recursos a los activos y procesos que así lo ameritan, dotando a la metodología de eficiencia además de eficacia.
Este redimensionamiento del alcance, puede ser importante a los efectos dar conformidad a la norma ISO/IEC 27.001 en cuanto a la identificación y clasificación de todos los activos alcanzados por el SGSI, y a su vez mantenerse alineado con las reales necesidades del negocio de forma oportuna, sin un costo excesivo de análisis detallado de la totalidad de los procesos y activos.

Se propone una estrategia de ajuste de valoración de activos ([35]) que hace uso de técnicas y algoritmia de grafos sobre la relación de dependencia de la seguridad de otros activos. Se formaliza y define ese algoritmo de ajuste.
Este ajuste, que puede determinarse algorítmicamente, logra acotar por debajo la estimación de los activos que pondrían en riesgo otros activos eventualmente más apreciados, y revisar así, si algunos activos están subestimados. En particular, una aplicación directa, es el establecimiento de una valoración inicial por parte de la empresa principal, sobre un activo que está bajo el

[35] En su acepción más amplia, incluyendo los procesos.

dominio y responsabilidad de la empresa subordinada. Esta valoración – que funciona como cota inferior - podrá luego ser incrementada o ponderada como corresponda por ésta última en función del criterio aplicado a las directivas de la empresa principal.

Se definen además dos tipos de subgrafos a los efectos de hacer análisis específicos de riesgos, ellos son: subgrafo inducido por un activo / proceso, y subgrafo inducido por un atributo de seguridad específico (C, I, o D). Esto permite, en el primer caso, analizar riesgos específicos relativos a un activo / proceso, y en el segundo caso hacerlo concentrándose en los aspectos más relevantes con respecto al atributo de seguridad analizado y/o a la amenaza y riesgo en cuestión. Por ejemplo analizar el impacto en los activos de la organización ante la concreción de una amenaza que viole la confidencialidad de determinado activo de información.

Sugerimos la adopción de estándares y modelos operativos de negocios, eventualmente específicos para el sector, que permitan alinear los modelos de negocios y utilizar una herramienta que facilite la coordinación y comunicación entre ambas empresas y los diferentes actores. Un ejemplo de esto es eTOM para el caso de las empresas de Telecomunicaciones.

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.

Se fundamenta en el presente trabajo, la necesidad de un software que apoye la metodología y se describen brevemente los requerimientos principales del mismo, sin pretender dar aquí una especificación formal, pero sí delinear las características funcionales que ofrecer el mismo. Se propone una lista de los requerimientos principales.
Este software debe principalmente, fomentar la coordinación y cooperación de las empresas en lo que a seguridad de la información se refiere, con procedimientos e hitos bien definidos para cada fase del SGSI, e interfaces que promuevan la adopción de los lineamientos directrices corporativos y a su vez permitir una retroalimentación de las fuentes de seguridad de la información específicas de las diferentes áreas.
Además debe: permitir la definición de roles, fomentar el flujo de percepción y estimación de riesgos en forma bidireccional con mecanismos claramente definidos para los lineamientos "macro" y corporativos que establezcan el contexto, pero también el *feedback* desde los sectores más específicos y técnicos, de los dominios locales hacia los estratos superiores del organigrama de seguridad establecido a nivel corporativo (intra e inter empresa).

En cada etapa del ciclo PHVA 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, y permitir escalar riesgos locales percibidos así como heredar los riesgos percibidos y priorizados desde los estratos superiores, buscando alinear los planes de gestión de seguridad al negocio de la forma más conveniente, en función de los recursos, objetivos concretos y condicionantes.

6 Trabajo Futuro

A los efectos de validar, de forma empírica, la metodología que se presenta en este trabajo, es necesario obtener confirmación experimental de la efectividad de las propuestas realizadas, tanto cualitativa como cuantitativamente. Es decir, cotejar mediante un mayor trabajo de campo (que excede el alcance de este trabajo), los resultados esperados con la realidad, y corroborar así la eficacia y la eficiencia de la metodología propuesta, y enriquecerla con los ajustes necesarios si fuera conveniente.

Es de interés, la especificación formal del software sugerido, con casos de uso concretos, basados en un grupo empresarial específico a los efectos de su identificación pero generalizables en su aplicación. Para ello sugerimos profundizar en el *workflow* en el cual se apoye el SGSI así como en la algoritmia aplicable a los grafos de dependencias entre activos, y la posibilidad de visualización de subgrafos inducidos por determinado atributo de seguridad.

Otra línea de investigación interesante, con un grupo empresarial representativo de un sector industrial, creemos puede ser la identificación y análisis de árboles de ataque [96] aplicables al sector industrial específico, como por ejemplo TelCo – ISP, y en particular, instanciando la metodología que aquí se presenta, detectar potenciales dependencias interinstitucionales y cómo ello condiciona las actividades y resultados propios de cada fase del SGSI. Para esto sería deseable trabajar con un grupo empresarial concreto, representativo del sector, que favorezca la identificación de estas dependencias, pero con el objetivo de obtener resultados generalizables.

7 Referencias bibliográficas

[1] BuddeCom. "Latin America - Telecoms, Mobile and Broadband in Southern Cone", Marzo de 2008, Publicación Anual.
http://www.budde.com.au/Research/4511/2008_Latin_America_-_Telecoms_Mobile_and_Broadband_in_Southern_Cone.aspx?sub=EXECUTIVE (noviembre de 2009)

[2] BuddeCom. "Uruguay - Telecoms Market Overview & Statistics", 2008.
http://www.budde.com.au/Research/1888/Uruguay_-_Telecoms_Market_Overview__Statistics.aspx (noviembre de 2009)

[3] Ministerio de Administraciones Públicas – Gobierno de España. "MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información",
http://www.csae.map.es/csi/pg5m20.htm (octubre de 2009)

[4] Arbor Networks. WorldWide Infrastructure Security Report, Volume (I, II, III, IV), Noviembre de 2008 (Volumen IV)
http://www.arbornetworks.com/report (octubre de 2009)

[5] Werbach K. "Digital Tornado: The Internet and Telecommunications Policy". Federal Communications Commission, Office of Plans and Policy, 1997.
http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf (noviembre de 2009)

[6] Kende M. "The Digital Handshake: Connecting Internet Backbones". Federal Communications Commission, Office of Plans and Policy, Setiembre de 2000.
http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp32.pdf (noviembre de 2009)

[7] Administración Nacional de Telecomunicaciones (ANTEL), *http://www.antel.com.uy/*

[8] Anteldata, *http://www.anteldata.com.uy/*

[9] Carozo E., Freire G., Martínez G., "Análisis del Sistema de Gestión de Seguridad de la Información de ANTEL", ANTEL.

[10] 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.

[11] RFC 3871 – "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", Setiembre de 2004.
http://www.apps.ietf.org/rfc/rfc3871.html (octubre de 2009)

[12] Andrzej Białas, Krzysztof Lisek, "Integrated, Business-Oriented Two Stage Risk Analysis". (2007)
http://www.proceedings2007.imcsit.org/pliks/60.pdf (octubre de 2009)

[13] Sandstrom O., "Proceso de implantación de un SGSI, adoptando la ISO 27001". Arsys Internet.
http://www.borrmart.es/articulo_redseguridad.php?id=1724&numero=33 (noviembre de 2009)

[14] ITU-T Recommendation X.805 – "Security architecture for systems providing end-to-end communications" (alineada con iso/iec 18028 –2)
http://www.itu.int/rec/T-REC-X.805-200310-I/en (octubre de 2009)

[15] ITU-T Recommendation X.800, "Security architecture for Open Systems interconnection for CCITT Applications".

[16] ITU-T. "La Seguridad de las Telecomunicaciones y las Tecnologías de la información", Diciembre de 2003.
http://www.itu.int/itudoc/itu-t/85097-es.pdf (noviembre de 2009)

[17] National Institute of Standards and Technology, U.S. Department of Commerce (NIST), "National Vulnerability Database v. 2.2", 2008, *http://nvd.nist.gov/* (octubre de 2009)

[18] ITU–T X.1051 "Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (02/2008)" (ISO/IEC 27011:2008)
http://www.itu.int/rec/T-REC-X.1051/en (noviembre de 2009)

[19] J.F. Kurose, K.W. Ross, "Computer Networking: A Top Down Approach", 4th edition. Addison Wesley, Julio de 2007.

[20] Carlos Martinez, "Nuevas Amenazas: Fast Flux Service Networks", Antel – FIRST TC, Nov. 2008.
http://www.csirt-antel.com.uy/main/public/Nuevas-amenazas-fastflux-CSIRT-ANTEL.pdf
(noviembre de 2009)

[21] Arbor, ""Summary Report: Global Fast Flux"
http://atlas.arbor.net/summary/fastflux (octubre de 2009)

[22] Internet World Stats
http://www.internetworldstats.com/ (octubre de 2009)

[23] Grupo Radar, "Perfil del internauta uruguayo", 2008.
http://www.gruporadar.com.uy/info/El perfil del Internauta uruguayo-2008.pdf (octubre de 2009)

[24] ISO27000.es. "Sistema de Gestión de la Seguridad de la Información".
http://www.iso27000.es/doc_sgsi_all.htm (octubre de 2009)

[25] ISO/IEC 27000 "Information technology - Security techniques - Information security management systems - Overview and vocabulary"

[26] UNIT - ISO/IEC 27001:2005. "Tecnología de la información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos".

[27] UNIT - ISO/IEC 27002: 2005. "Tecnología de la información – Código de buenas prácticas para la gestión de la Seguridad de la Información".

[28] ISO/IEC FDIS 27003. "Information technology - Security techniques - Information security management system implementation guidance", noviembre 2009.

[29] ISO/IEC FDIS 27004. "Information technology - Security techniques - Information security management – Measurements", agosto 2009.

[30] ISO/IEC 27005. "Information technology — Security techniques -- Information security risk management".

[31] ISO/IEC CD 29100. "Information technology - Security techniques - Privacy Framework", agosto 2009.

[32] ISO/IEC TR 18044: 2004. "Information Security incident management".

[33] TMForum. "Business Process Framework (eTOM v. 8.0)".
http://www.tmforum.org/browse.aspx?catID=1647 (octubre de 2009)

[34] TMForum. ITU-T International Recommendation M.3050, *http://www.tmforum.org/* (octubre de 2009)

[35] TMForum, "TR143 Building Bridges ITIL and eTOM". Julio 2009. *http://www.tmforum.org/TechnicalReports/TR143BuildingBridges/35824/article.html* (octubre de 2009)

[36] RFC 3013 - "Recommended Internet Service Provider Security Services and Procedures", Noviembre de 2000. *http://www.rfc-archive.org/getrfc.php?rfc=3013* (octubre de 2009)

[37] RFC 3871 – "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", Setiembre de 2004. *http://www.rfc-archive.org/getrfc.php?rfc=3871* (octubre de 2009)

[38] Industry Canada, "The Digital Economy in Canada - Companion Document to Best Practices for Internet Service Providers and Other Network Operators". *http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00340.html* (octubre de 2009)

[39] B.R. Greene, "BGPv4 Security Essentials", ISP Essentials Supplement, Cisco Press. (2004), *http://www.nanog.org/mtg-0206/ppt/BGP-Risk-Assesment-v.5.pdf* (octubre de 2009)

[40] Network Reliability and Interoperability Council, "NRIC Best Practices for ISP Security", *http://www.nanog.org/mtg-0306/pdf/callon.pdf* (octubre de 2009)

[41] M. Swanson, B. Guttman, "Generally Accepted Principles and Practices for Securing - Information Technology Systems (BP 800-14)", National Institute of Standards and Technology -Technology Administration - U.S. Department of Commerce (Setiembre de 1996). *http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf* (octubre de 2009)

[42] TMForum, "Develop IP MasterPlan using eTOM and TAM" *http://www.tmforum.org/CaseStudiesBusiness/DevelopITMasterPlan/36933/article.html* (noviembre de 2009)

[43] Roger Cutts, "Architecting the enterprise", NGOSS Collaboration Project. TMForum (2007), *http://www.architecting-the-enterprise.com/pdf/presentations/Open_Cal_for_The_Open_Group_NGOSS_Collaboration_Project.pdf* (octubre de 2009)

[44] ISECT Ltd., ISO27001 Security Home *http://www.iso27001security.com/* (Octubre de 2009)

[45] InformIT, "Structuring and modularizing the Network with Cisco Enterprise Architecture" *http://www.informit.com/articles/article.aspx?p=1073230* (octubre de 2009)

[46] Tim Bass, "The Top Ten Cybersecurity Threats for 2009 - Draft for Comments". Enero de 2009. *http://www.thecepblog.com/2009/01/05/the-top-ten-cybersecurity-threats-for-2009-draft-for-comments/* (octubre de 2009)

[47] The Internet Engineering Task Force (IETF), *http://www.ietf.org/*

[48] Club de la Sécurité de l'Information Français, Mehari *https://www.clusif.asso.fr/* (setiembre de 2009)

[49] CERT – Software Engineering Institute, Carnegie Mellon, Octave *http://www.cert.org/octave/* (setiembre de 2009)

[50] Callio Technologies
http:www.callio.com (setiembre de 2009)

[51] Coras Risk Assessment Platform
http://sourceforge.net/projects/coras (setiembre de 2009)

[52] European Network and Information Security Agency (Enisa).
http://www.enisa.europa.eu/rmra/rm_home.html

[53] SANS Institute, *http://www.sans.org/*

[54] Instituto de Derecho Informático. Facultad de Derecho, UdelaR. "Índice Analítico de Derecho Informático Uruguayo".
http://www.fder.edu.uy/contenido/idi/normativa_1.html - 2.-_Derecho_de_la_Informaci%C3%B3n
(setiembre de 2009)

[55] Poder Legislativo, Uruguay. *http://www.parlamento.gub.uy/*

[56] Antel, "Respuesta de Antel a la consulta pública sobre la Consultoría internacional en contabilidad regulatoria en Telecomunicaciones.", Diciembre 2008.
http://www.ursec.gub.uy/scripts/locallib/imagenes/ANTEL.pdf (octubre de 2009)

[57] Red USI – Uruguay Sociedad de la Información, "Acuerdo Operativo – Antel – LATU", Enero 2009. *http://www.usi.org.uy/es/noticias/81-acuerdo-operativo-antel-latu.html* (octubre de 2009)

[58] Daniel Fuentes, "Convergencia: Caso Antel - Uruguay", Antel.
http://www.cantv.com.ve/Portales/Cantv/Data/Eventos/AHCIET/LaconvergenciahoyAntelUruguayDanielFuentes.pdf
(noviembre de 2009)

[59] EAR/ Pilar. Entorno de análisis de Riesgos
http://www.ar-tools.com/ (setiembre de 2009)

[60] CSIRT de Antel, *http://www.csirt-antel.com.uy/principal/* (octubre de 2009)

[61] International Organization for Standarization (ISO), *http://www.iso.org/*

[62] María Eugenia Corti, Gustavo Betarte, Reynaldo de la Fuente, "Hacia una implementación exitosa de un SGSI", Actas del 3º Congreso Iberoamericano de Seguridad Informática CIBSI'05, 21-25 de Noviembre de 2005, Valparaíso, Chile, (457-471).

[63] Ciancamerla E., Minichino M., "Tools and techniques for interdependency analysis (Deliverable D 2.2.2)", IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems, Julio de 2007.

[64] International Register of ISMS Certificates
http://www.iso27001certificates.com/ (octubre de 2009)

[65] Siemens Enterprise Communications Ltd. "CRAMM toolkit"
http://www.cramm.com/ (octubre de 2009)

[66] ISM3 Consortium, "Information Security Management Maturity Model v. 2.10"
http://www.ism3.com/ (octubre de 2009)

[67] Hervé Schauer, Alexandre Fernández, ISO 27005: "Gestion de risque", Clusif – Club Ebios, mayo de 2007.
http://www.hsc.fr/ressources/presentations/mehari-ebios-iso27005/iso27005.pdf (octubre de 2009)

[68] Areiza, Barrientos, Rincón, Lalinde. "Hacia un Modelo de Madurez para la Seguridad de la Información", Universidad EAFIT - Colombia, Congreso Iberoamericano de Seguridad Informática CIBSI'05, 21-25 de Noviembre de 2005, Valparaíso, Chile. *http://cibsi05.inf.utfsm.cl/presentaciones/sesion10/Modelo_de_madurez_SI.pdf* (octubre de 2009)

[69] Alan Bryden, COPANT Seminar on Security Standards, La Paz, 25 de abril de 2006. *http://www.iso.org/iso/livelinkgetfile?llNodeId=21657&llVolId=-2000* (octubre de 2009)

[70] International Telecommunication Union (ITU), *http://www.itu.int/net/home/index.aspx*

[71] ITU-Telecom Standarization Sector, *http://www.itu.int/net/ITU-T/info/Default.aspx*

[72] ISO/IEC 18028-2 "Information technology - Security techniques - IT network security - Part 2: Network security architecture"

[73] Stoneburner G., Goguen A., Feringa A., "Risk Management Guide for Information Technology Systems", NIST SP 800-30, National Institute of Standards and Technology, U.S. Department of Commerce *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf* (octubre de 2009)

[74] Ross R., Katzke S., Johnson A., Swanson M., Stoneburner G., "Managing Risk from Information Systems - An Organizational Perspective (second public draft)", NIST SP 800-39, National Institute of Standards and Technology, U.S. Department of Commerce *http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf* (octubre de 2009)

[75] Information Systems Audit and Control Association. ISACA, *http://www.isaca.org/*

[76] IT Infrastructure Library, ITIL. IT Service Management (ITSM), Office of Government Commerce (OGC), UK. *http://www.itil-itsm-world.com/* (octubre de 2009)

[77] Peter Senge, "La Quinta Disciplina. El arte y la práctica de la organización abierta al aprendizaje". Ed. Granica, 1999.

[78] Federal Office for Information Security – Germany. IT Grundschutz, *http://www.bsi.bund.de/* (octubre de 2009)

[79] Federal Office for Information Security – Germany, "The IT Security Situation in Germany in 2007", *http://www.bsi.bund.de/english/publications/securitysituation/Lagebericht_2007_englisch.pdf* (octubre de 2009)

[80] Ernst & Young, Services and Reports for Telecommunication Companies. "Tackling next generation challenges" *http://www.ey.com/UY/es/Industries/Telecommunications* (octubre de 2009)

[81] Financial Director – Technological Issues, "Value Beyond Measure", Julio/Agosto 2006. *http://ivory.vnunet.com/assets/binaries/financial-director/pdf/value-beyond-measure.pdf* (octubre de 2009)

[82] Potter C., "Information Security – Security conscious", Financial Director, 2004. *http://www.financialdirector.co.uk/accountancyage/features/2040335/information-security-security-conscious* (octubre de 2009)

[83] Instituto Uruguayo de Normas Técnicas (UNIT), *http://www.unit.org.uy/*

[84] Kecia Gubbels, "Hands on the Honeypot". SANS Institute, Noviembre de 2002. *http://www.sans.org/reading_room/whitepapers/detection/hands_in_the_honeypot_365?show=365.php&cat=detection* (noviembre de 2009)

[85] Nii Quaynor, "Role of ISPs and i-economy development", Ghana.com *http://www.itu.int/africainternet2000/Documents/ppt/05_Quaynor-Role of ISP 2Jun00.ppt* (octubre de 2009)

[86] Behrouz A. Forouzan, "Data Communications and Networking"

[87] Stallings W., "Data and Computer Communications". Prentice Hall, 2006.

[88] Kozierok, Charles M. "The TCP/IP guide: a comprehensive, illustrated Internet protocols reference", 2005.

[89] Uwe Beyer, Felix Flentge, "Towards a Holistic Metamodel for Systems of Critical Infrastructures", ECN CIIP Newsletter, Vol.2, No.3, October/November 2006.

[90] Uwe Beyer, Felix Flentge, "The ISE Metamodel of Critical Infrastructures", In: "Critical Infrastructure Protection: Issues and Solutions". Springer, 2007

[91] Massera M, Fovino I.N., 2008, en IFIP International Federation for Information Processing, "Critical Infrastructure Protection II", eds. M. Papa, S. Shenoi. (pp. 367 – 376)

[92] Critical Information Infrastructure Research Co-ordination Project *http://www.ci2rco.org/*

[93] Pallas G. y Corti M.E., "Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica", Congreso Iberoamericano de Seguridad Informática (CIBSI'09), Noviembre de 2009, Montevideo, Uruguay.

[94] Killcrece K.; Kossadowski K.P., Ruefle R, Zajicek M., "Organizacional Models for Computer Security Incident Response Teams (CSIRTs)", Carnegie Mellon – Software Engineering Institute. Diciembre de 2003.

[95] Forum for Incident Response and Security Teams (FIRST) *http://www.first.org* (octubre de 2009)

[96] Schneier B., "Modeling security threats" en "Attack Trees", Dr. Dobb's Journal, Diciembre de 1999. *http://www.schneier.com/paper-attacktrees-ddj-ft.html* (noviembre de 2009)

[97] Von Solms, B., "Information Security governance: CObIT or ISO 17799 or both?", Computers & Security 24, Elsevier, 2005, pp. 99-104.

[98] Sánchez, L.E., Villafranca, D., Fernández-Medina, E. y Piattini, M; Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799, International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES, IEEE Computer Society. Viena, Austria. (2006). Pp. 585-592.

[99] Sánchez L.E., Villafranca D., Fernández-Medina E y Piattini M., "MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES", V Congreso Iberoamericano de Seguridad Informática (CIBSI'09), Noviembre 2009. *http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia2-Sesion3%283%29.pdf* (noviembre de 2009)

[100] Villafranca D., Sánchez L.E., Fernández-Medina E y Piattini M., "Metodología para la selección de métricas en la construcción de un Cuadro de Mando Integral" V Congreso Iberoamericano de Seguridad Informática (CIBSI'09), Noviembre 2009. *http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia2-Sesion3%285%29.pdf* (noviembre de 2009)

[101] Sánchez, L.E., Villafranca, D., Fernández-Medina, E. y Piattini, M. Management of Scorecards and Metrics to manage Security in SMEs. The 18th ACM Conference on Information and Knowledge Management (CIKM 2009) - International Workshop on Data Quality and Security (DQS'09). Noviembre 2009. Pp. 9-16.

[102] Aho A. V., Hopcroft J. E., Ullman J. D., "Data Structures and Algorithms". Addison-Wesley, 1983

[103] Bondy J.A., Murty U.S.R., "Graph Theory with Applications". American Elsevier

[104] Carré B., "Graphs and Networks". Oxford Applied Mathematics and Computing Science Series.

GLOSARIO

Activos*	Extensión del concepto de Activos, que incluye procesos
(D)DoS	(Distributed) Denial of Service
(N)IDS	(Network) Intrusion Detection System
AAA	Autentication, Authorization, Accountability
ACL	Access Control List
ADSL	Asymmetric Digital Suscriber Line
BGP	Border Gateway Protocol
Botnet	Conjunto de sistemas comprometidos (*zombies*) usualmente corriendo *malware* ([36]), bajo el comando de una entidad central remota ([37]), usualmente para coordinar un ataque, con fines de ocasionar daño.
CERT	Computer Emergency Response Team
CobIT	Control Objectives for Information and related Technology
CSIRT	Computer Security Incident Response Team
DAG	Directed Acyclic Graph
DBMS	DataBase Management System
Delphi	"Puede ser caracterizado como un método para estructurar el proceso de comunicación grupal, de modo que ésta sea efectiva para permitir a un grupo del individuos, como un todo, tratar con problemas complejos" ([38]) "Es un programa cuidadosamente elaborado, que sigue una secuencia de interrogantes individuales a través de cuestionarios, de los cuales se obtiene la información que constituirá la retroalimentación para los cuestionarios siguientes" ([39]).
DNS	Domain Name System
DNS Cache Poisoning	Envenenamiento del Cache de DNS
DXC	Digital Cross Connect
ERP	Enterprise Resource Planning
eTOM	Enhanced Telecom Operations Map
Focus Groups	Es una herramienta de análisis, mediante sesiones de grupo, en general moderadas y con visiones complementarias (interdisciplinario), con un objetivo específico y concreto para analizar un concepto, estrategia, producto, servicio, etc.
Hijacking	Práctica de ataque a la seguridad de la red o al canal de comunicación por el cual el atacante toma el control de la comunicación entre dos partes / entidades haciéndose pasar por una de ellas.

[36] worms, troyanos, backdoors
[37] normalmente utiliza el protocolo IRC
[38] Linstone y Turoff (1975)

[39] Helmer y Rescher (1959)

Honeynet	Es una red de honeypots seteados imitando una red real con los propósitos de analizar tácticas, métodos y técnicas de los atacantes (investigación) y monitorear su actividad simulando eventualmente una red de producción.
Honeypot	Son servidores de señuelo o sistemas instalados vulnerables con el objetivo de recabar información sobre la actividad (*logs*) de un atacante o intruso en el sistema y así poder monitorear, conocer y aprender sobre las conductas y técnicas utilizadas para ello. La idea es atraer a un atacante simulando ser un sistema real.
I+D	Investigación y Desarrollo
I-CAT	Internet Categorization of Attacks Toolkit
IEC	International Engineering Consortium
IP	Internet Protocol
IPTV	Servicio de televisión por IP.
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
ISM3	Information Security Management Maturity Model
ISMS	Information Security Management System
ISO	International Organization for Standarization
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union, Telecommunications Sector
LDAP	Lightweight Directory Access Protocol
LMDS	Local Multipoint Distribution Service
LPDP	Ley de Protección de Datos Personales
MPLS	Multiprotocol Label Switching
MUX	Multiplexor
NIST	National Institute of Standards and Technology
OM&S	Organización, Mantenimiento y Servicios
PDCA	Plan, Do, Check, Act
PHVA	Planificar, Hacer, Verificar, Actuar
PyME	Pequeña y Mediana Empresa
ROI	Return of Investment
SGSI	Sistema de Gestión de Seguridad de la Información
SGSI	Sistema de Gestión de Seguridad de la Información
SLA	Service Level Agreement
Sniffing	La práctica de monitorear o ‘escuchar’ (en una red) subrepticiamente informaciones electrónicas.

SO	Sistema Operativo
Spam	Correo / Mensaje no deseado.
Spammer	Persona que utiliza el spamming como práctica
Spamming	Abuso de los sistemas de mensajería electrónica para enviar mensajes (correos por ejemplo) no solicitados de forma masiva con fines publicitarios.
Spoofing	La práctica de emular un sistema confiable para obtener acceso por ejemplo a información confidencial. Un ejemplo es el IP spoofing que consiste en enmascarar la dirección IP por alguna otra que le corresponde a un tercero.
TAM	Telecoms Applications Map
TCP	Transmission Control Protocol
TelCo	Telecommunication Company
TIR	Tasa Interna de Retorno
TMN	Telecommunications Management Network
UDP	User Datagram Protocol
UNIT	Instituto Uruguayo de Normas Técnicas
VAN	Valor Actualizado Neto
VoIP	Voice over Internet Protocol
VoIP	Voice IP
VPN	Virtual Private Network

A N E X O S

ANEXO A

AntelData

En el presente Anexo se describen algunos datos relevantes de las telecomunicaciones en la región y se ilustra brevemente con las características de Anteldata.

Características de la Región. Perfil socio-económico relevante:

De acuerdo al informe *"2008 Latin America - Telecoms, Mobile and Broadband in Southern Cone"* [1]:

Argentina, Chile y Uruguay, se destacan en América Latina en una serie de indicadores claves como ser: estándar y calidad de vida, alfabetización, teledensidad y acceso a Internet. Argentina y Uruguay tienen la mayor penetración móvil ([40]) y Chile es líder en lo que a Internet y en lo que a banda ancha refiere.

Aspectos a destacar de Uruguay y la región ([41]):

- Uruguay (ANTEL) mantiene el monopolio estatal de la telefonía fija, y sin embargo tiene la tasa de teledensidad en telefonía fija más alta de América Latina. En los otras áreas de telecomunicaciones existe un régimen abierto a la competencia. Argentina y Chile tienen un régimen liberal y privatizado en todas las áreas de las telecomunicaciones.
- Mientras que la telefonía fija está en general en una meseta (estable), la telefonía móvil ha venido creciendo, y en particular en Uruguay rápidamente (debido a su desarrollo más tardío), en este sector la competencia en la región es fuerte, y la penetración ha alcanzado o está cercana al 100%.
- La banda ancha tuvo un crecimiento explosivo, en particular en Chile que lidera la tasa de penetración, seguido de Argentina y Uruguay. Sin embargo en Uruguay, la dependencia de la TelCo estatal (Antel), le da a su ISP (Anteldata) una posición dominante, sumado además a la inexistencia de banda ancha por cable-modem.
- En los tres países se han desarrollado redes WiMAX y tecnología 3G. En particular, en Uruguay la tecnología 3G fue lanzada por los tres operadores de telefonía móvil: Ancel (estatal), Telefónica-Movistar, América Móvil – CTI / Claro que compiten intensamente en el sector.
- La convergencia en Uruguay tiene menos desarrollo que en Chile y Argentina debido a que los operadores de cable por ejemplo no pueden prestar servicios de Internet ni de voz.
- En cuanto a servicios de valor agregado como IPTV, Chile fue el primer país de Latinoamérica en implementarlo (Junio 2007). En Argentina la regulación no permite que las TelCos vendan servicios de TV. En Uruguay fue anunciado el lanzamiento para 2009 ([42]).

Por otra parte según figura en Internet World Stats [22]

[40] salvo algunas islas Caribeñas
[41] Cono Sur
[42] http://www.espectador.com/1v4_contenido.php?id=142563&sts=1 (Enero 2009)

Latin American Internet Usage					
LATIN AMERICA COUNTRIES / REGIONS	Population (Est. 2009)	Internet Users, Latest Data	% Population (Penetration)	User Growth (2000-2009)	% Users in Table
Argentina	40,913,584	20,000,000	48.9 %	700.0 %	11.6 %
Bolivia	9,775,246	1,000,000	10.2 %	733.3 %	0.6 %
Brazil	198,739,269	67,510,400	34.0 %	1,250.2 %	39.3 %
Chile	16,601,707	8,368,719	50.4 %	376.2 %	4.9 %
Colombia	43,677,372	18,234,822	41.7 %	1,976.9 %	10.6 %
Costa Rica	4,253,877	1,500,000	35.3 %	500.0 %	0.9 %
Cuba	11,451,652	1,450,000	12.7 %	2,316.7 %	0.8 %
Dominican Republic	9,650,054	3,000,000	31.1 %	5,354.5 %	1.7 %
Ecuador	14,573,101	1,634,828	11.2 %	808.2 %	1.0 %
El Salvador	7,185,218	763,000	10.6 %	1,807.5 %	0.4 %
Guatemala	13,276,517	1,320,000	9.9 %	1,930.8 %	0.8 %
Honduras	7,833,696	658,500	8.4 %	1,546.3 %	0.4 %
Mexico	111,211,789	27,400,000	24.6 %	910.2 %	15.9 %
Nicaragua	5,891,199	155,000	2.6 %	210.0 %	0.1 %
Panama	3,360,474	778,800	23.2 %	1,630.7 %	0.5 %
Paraguay	6,995,655	530,300	7.6 %	2,551.5 %	0.3 %
Peru	29,546,963	7,636,400	25.8 %	205.5 %	0.6 %
Puerto Rico	3,966,213	1,000,000	25.2 %	400.0 %	0.6 %
Uruguay	3,494,382	1,340,000	38.3 %	262.2 %	0.8 %
Venezuela	26,814,843	7,552,570	28.2 %	695.0 %	4.4 %
TOTAL	569,212,811	171,833,339	30.2 %	865.7 %	100.0 %

Fuente: http://www.internetworldstats.com/ [22]

Según el informe del Grupo Radar: "Perfil del internauta uruguayo", de diciembre de 2008 [23], Uruguay tiene 1.340.000 internautas, es decir un 41% de la población.

Además, entre quienes se conectan a internet desde sus casas, la penetración de banda ancha es de 62%. El informe advierte una desaceleración del crecimiento explosivo observado en 2005 y 2006.

A esto debe sumarse el impacto del Plan Ceibal que ha incrementado el número de internautas.

Características del sector:

Las características del sector, fueron analizadas en el documento principal, como parte del Caso de estudio.

Anteldata:

Anteldata es el ISP estatal; la misma se desarrolla y funciona en un ámbito competitivo.

A continuación, se describen las características fundamentales de la empresa en cuanto a su estrategia empresarial y posicionamiento en el mercado. Fuente:

Misión, Visión, Políticas Generales y Líneas de Acción

Se presentan a continuación, la misión, visión, políticas generales y líneas de acción extraídos del sitio web y/o presentaciones de la empresa [8], todas ellas referenciadas.

Misión:

'Brindar la más amplia gama de soluciones de telecomunicaciones para satisfacer las necesidades de todos los clientes potenciales, utilizando las más modernas tecnologías con eficacia y eficiencia'

Visión

'Ser el actor principal en el desarrollo de los negocios de conectividad y ancho de banda en Uruguay'

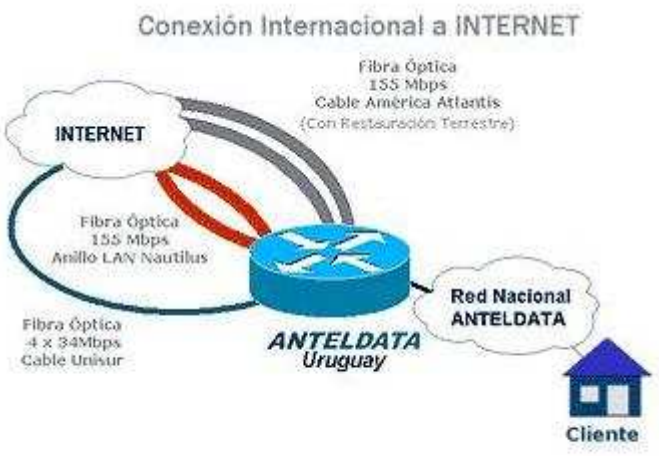
Cobertura del mercado, linea fija y adsl [58]

Lineas Fijas: 90% de hogares (comercializadas)
99% " " (cobertura)

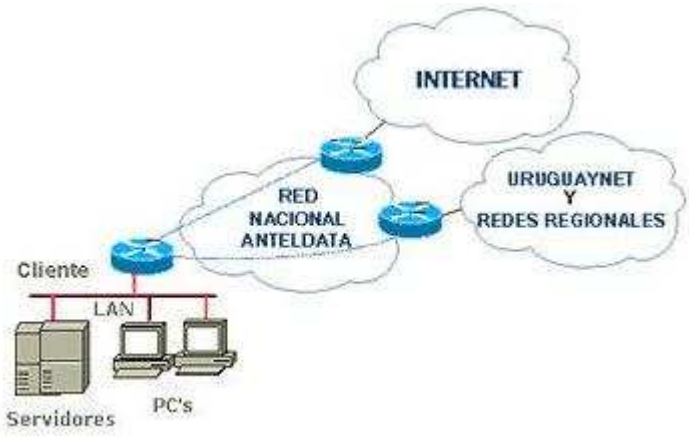
Banda Ancha: 20% de hogares (comercializadas)
95% " " (cobertura)

Principales Desarrollos de Redes y Servicios [58]

Adsl (Contenidos exclusivos banda ancha)
AdinetTV (video on demand, señales en vivo)
3Play, 4play (Convergencia)
VideoStreaming
Piloto: Video en Redes 3G (norma DVB-H)
Piloto: IPTV



Conexión del cliente / empresarial



Estrategia de Negocio

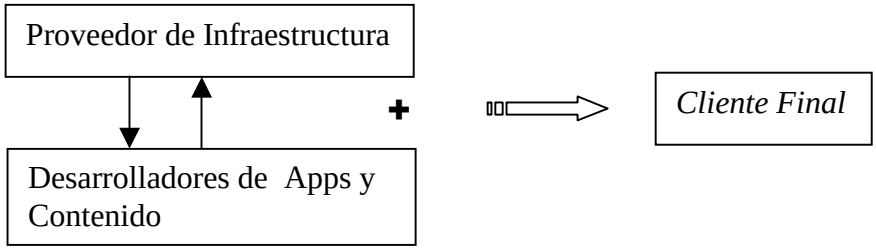
- *Nuevos productos / negocios y convergencia:*

  Construir redes, desplegar servicios, acelerar demanda.
  Requieren: Optimizar negocio, eficiencia, velocidad de reacción.

- *Estrategia Comercial:*

  Primera Etapa: Mantener precio y mejorar producto, de forma de generar un impacto positivo en los canales de venta, con consecuente aumento de demanda y de economía de escala. Impacto positivo en el mercado y en la rentabilidad.

  Segunda Etapa: Baja de precio de nuevos productos.



Políticas Generales de Antel (Líneas de acción 2005 - 2009) [7]**:**

De orientación a los Clientes

• Dar la mayor prioridad a la atención al cliente, apuntando a las necesidades de los distintos segmentos, mejorando la comercialización de los servicios y las comunicaciones con los clientes.

De eficiencia en la gestión

• Mejorar la eficiencia de la empresa: racionalizando procesos, gastos e inversiones.

• Implantar mecanismos de incentivos asociados al desempeño en toda la empresa.

De relacionamiento con la sociedad

• Contribuir a la inclusión social por vía de las telecomunicaciones:

- mediante asociaciones con la ANEP, organizaciones del estado u otras organizaciones de la sociedad civil
- a través de la telefonía pública
- con el desarrollo del servicio universal.

De orientación tecnológica y de servicios

• Potenciar la sinergia de la empresa al brindar simultáneamente servicios de telefonía fija, móvil y datos, apuntando a la convergencia entre telefonía fija y móvil.
• Instalar una red multiservicio que brinde entre otros TV distributiva o interactiva, tele-educación y datos.

De relacionamiento con otras empresas y el sector académico

• Establecer alianzas estratégicas con empresas de la región o del mundo para conseguir dar mejores servicios en forma global y para conseguir mejores precios en las compras por cantidad.

• Fortalecer la relación con el sector privado, en particular proveedor de contenidos o de tecnologías.

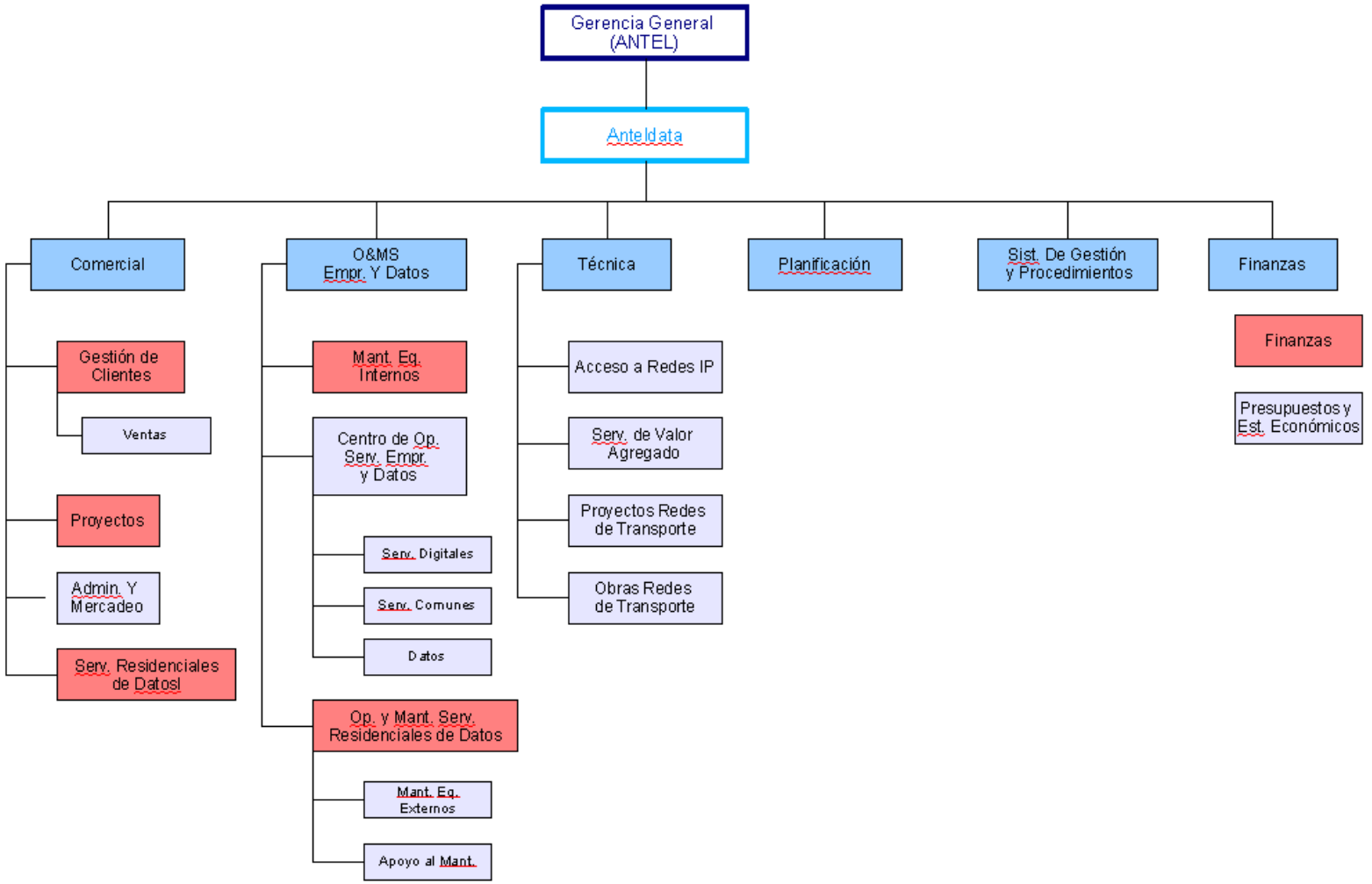
• Fortalecer la relación con el sector académico.

De promoción de la industria nacional

• Fomentar la compra de tecnología nacional, siempre que responda a normas de calidad, sea competitiva y ofrezca las debidas garantías de soporte durante la vida útil del servicio.

• Proponer al Uruguay como laboratorio de prueba para nuevas tecnologías o servicios. En efecto, su tamaño, geografía, nivel cultural e infraestructura lo hacen apto para lanzar pilotos, lo que a su vez tendría un efecto dinamizador de las industrias locales.

Organigrama de Anteldata [Fuente: Anteldata]



ANEXO B

MARCO LEGAL - URUGUAY

Derecho de la Información (privacidad, datos personales)

- Derecho de acceso - Art. 694 de la Ley 16.736 de 05.01.1996
- Libre flujo de información en la Administración Pública - Art. 14 del Decreto 500/991 de 27.09.1991
- Ley 18.046, Arts. 54 y 55 - Sobre la Creación, constitución y competencia de Agesic.
- Ley 18.172, Art. 118 – Redefinición de la misión de Agesic.
- Ley 18.331 – "Ley de Protección de Datos Personales y Acción de *Habeas Data*"
- Ley 18.362, Art. 72 – Creación de la "Dirección de Derechos Ciudadanos" en la Agesic.

  Art. 73 - Creación del "Centro Nacional de Respuesta a Incidentes de Seguridad Informática" (CERTuy) en la Agesic.

  Art. 74 – Facultades de apercibimiento de la Agesic sobre los Organismos que no cumplan con las normas y estándares de tecnología de la información según la normativa vigente
- Ley 18.381 "Derecho de acceso a la información pública"

Decretos

- Decreto s/n (CM/827) "Principios y Líneas Estratégicas para el Gobierno en Red"
- Decreto s/n (CM/828) "Regularización del "Centro Nacional de Respuesta e Incidencias de Seguridad Informática (CERTuy)"
- Decreto s/n CM/829 "Política de Seguridad de la información para organismos de la Administración Pública"

Nombres de dominio

- Acuerdo de registro de dominio ".com.uy" ante ANTEL
- Instructivo técnico para el registro de nombres bajo el dominio ".uy" ante SECIU
- Marcas, nombres comerciales, indicaciones geográficas, boletín de la propiedad industrial, agentes de la propiedad industrial y otros puntos afines - Ley 17.011 de 25.09.1998
- Lista de clase de productos y servicios
-Decreto reglamentario 34/999 de 03.02.1999

Presupuesto Nacional – Sección Telecomunicaciones

- Ley 17.296 – Presupuesto Nacional para el actual periodo de gobierno (art. 86 y Sección VIII Telecomunicaciones)

ANEXO C

Controles extendidos específicos para un ISP - Telco

Además de los controles establecidos en el Anexo A, de carácter normativo, con los objetivos de control y controles de la norma ISO/IEC 27.001 aplicables a un ISP, y en general, de todos aquellos establecidos en la norma ISO/IEC 27.002 – en los cuales se basan los primeros -; se describen aquí una serie de objetivos de control y controles aplicables y recomendados para un ISP. Los mismos también se basan en la recomendación ITU-T Rec. X.1051 – *Anexo A - Telecommunications extended control set*, donde se realizan recomendaciones de controles específicos para empresas de telecomunicaciones.

Se destacan algunos de ellos de aplicación específica, por información detallada y completa, consultar el documento referido.

A.10 Gestión de Operaciones y Comunicaciones

A.10.6 Gestión de Seguridad de Red

Objetivo: Proveer seguridad de la información en las comunicaciones y protección de la infraestructura que las soporta.
En el caso de los ISP este punto es especialmente importante debido a que, como se dijo, la frontera de seguridad es difusa o trasciende la propia empresa. Deben tenerse consideraciones legales y contractuales y se requerirán adecuados controles de monitoreo y protección, particularmente para la información sensible que circule por redes públicas (Internet).
Es conveniente explicitarlo en los contratos, SLAs, descripción de servicios y explicitar las responsabilidades del ISP y las que no (responsabilidades de la Telco, del usuario, de otros ISP o vulnerabilidades inherentes a los protocolos e infraestructura de internet).

A.10.6.3 Gestión de seguridad de los servicios de telecomunicaciones

Control:

Los ISPs / Telcos deben especificar los niveles de seguridad para los servicios que proveen y anunciarlos a los clientes, debiendo monitorear y mantener los mismos.

Guia de implementación:

a) Especificar claramente las condiciones y niveles de seguridad de los servicios a los clientes.
b) Advertir a los usuarios acerca de actividades de spam, crímenes cibernéticos, virus, malware, etc.
c) Prevenir, en la medida de sus competencias y responsabilidades la interceptación de comunicaciones no autorizadas, incluso en las interconexiones con otros ISPs.
d) Controles Sniffing y de Spoofing.
e) Control de spam
f) Control de denegación de servicios (DoS y DDoS)

g) Control de vulnerabilidades técnicas de los dispositivos activos y pasivos de red y la infraestructura y activos de información en general.
h) Detección de patrones de comportamiento sospechosos o comportamientos reconocidos de tráfico hostil (vía (N)IDS)
i) Controles adecuados y gestión de los dispositivos (de red, servidores, etc.) e información de routing y control (ej. DNS Poisoning).
j) Utilización de mecanismos de AAA (autenticación, encripción, etc.).
k) Protección de la información sensible de las comunicaciones y de la información personal y privada.
l) Gestión de prioridades de tráfico. Por ej. tráfico de control, o de gestión frente a ataques de inundación de host o denegación de servicios, etc.
m) Control de ataques desde botnets.

A.10.6.4 Respuesta ante Spam

Control:

Deben establecerse políticas anti-spam y establecer controles y condiciones adecuadas para el uso de e-mail.

Guía de implementación:

Cuando se reconoce un *spammer* como cliente propio debe advertírselo a los efectos de que no continúe con esta práctica. De hacerse caso omiso, y continuarse con esta práctica debería suspenderse el servicio a los efectos de bloquear el Spam.
Debe operarse en conjunto y en forma cooperativa, con otros ISPs, con organizaciones anti-spam (listas negras) y eventualmente con la propia Telco.
La política anti-spam debe respetar y estar alineada con la legislación vigente (al momento de su implementación).

A.10.6.5 Respuesta a ataques de Denegación de Servicios (DoS y DDoS)

Control:

Deben de especificarse políticas y controles para prevenir y combatir ataque de denegación de servicios y favorecer las condiciones para las calidades de servicio comprometidas (o esperadas).

Guía de implementación:

Deben tomarse las medidas para reducir o eliminar las vulnerabilidades a ataques de denegación de servicio.
Frente a ataques de denegación de servicios debe de ser posible:
a) filtrar los paquetes hacia el sitio atacado.
b) Posibilidad de filtrar comunicaciones o limitar anchos de banda utilizados, por IP, puertos, protocolos, etc.
c) Posibilidad de priorizar protocolos y comunicaciones.
d) Si el ataque se produce desde el servicio de un cliente, advertirlo de la situación y si es necesario, bloquear el servicio.

e) Si el ataque es desde un servicio de otro ISP, coordinar acciones para bloquear o terminar el ataque.

Debe trabajarse en forma conjunta y cooperativa, con otros ISP, la TelCo, y organizaciones dedicadas a la investigación y el combate de esta tipo de ataques.
También la política anti-spam debe estar alineada a la legislación vigente y adecuarse a las cláusulas contractuales, o mejor dicho, en las cláusulas contractuales debería especificarse la posibilidad de este tratamiento en caso de ser necesario, así como las acciones pasibles de ser tomadas por el ISP.

También debe trabajarse en forma coordinada con CSIRT / CERT nacionales y del exterior, aprendiendo y compartiendo experiencias y recomendaciones. En particular se debe estar preparado para evitar o en su defecto detectar y mitigar / cortar ataques desde *botnets* (ej. Fast Flux DNS).

A11 – Control de Acceso:

A.11.4 Control de acceso a la red:

Objetivo: Prevenir los accesos no autorizados a los servicios en red.

Control:

Deben proveerse:

a) Deben proveerse interfaces adecuadas entre la red de la empresa y las de otras organizaciones o empresas y de Internet. Utilizando diferentes zonas y niveles de seguridad, con diferentes exigencias de seguridad y requisitos de acceso.
b) Mecanismos adecuados de autenticación, de los usuarios y los equipos.
c) Controles de autorización y *logging*.

A.11.4.8 Identificación y Autenticación del propio ISP.

Deben proveerse mecanismos apropiados y adecuados para que los usuarios puedan identificar y autenticar al propio ISP. De lo contrario, no es posible asegurar comunicaciones confidenciales por ejemplo dado que sería propensa a ataques de "*man in the middle*", o *phishing* entre otros.

ANEXO D

Síntesis de la Recomendación ITU-T X.805

La Recomendación de la X.805 de la ITU-T: "*Security architecture for systems providing end-to-end communications*" define una arquitectura, un modelo de seguridad de red a los efectos de proveer seguridad de extremo a extremo, y es independiente de la tecnología de red subyacente y es aplicable a redes complejas con tecnologías combinadas ([43]).

En particular, es útil su aplicación como forma de aplicar un enfoque sistemático y sistémico en lo que a las comunicaciones de red se refiere.

En un contexto como en el que se analiza en este trabajo de tesis (ISP y TelCo), donde se utilizan múltiples protocolos, hardware, software de gestión y operación, etc., donde además los servicios tienden a converger e integrarse, este modelo ofrece la posibilidad de analizar la seguridad en el plano tecnológico (de red) de forma sistemática y atendiendo a los diferentes niveles de abstracción y a las interacciones propias de los servicios y protocolos.
Es por ello que su uso es adecuado para detectar, predecir y mitigar vulnerabilidades y riesgos que eventualmente no surgen en el análisis aislado de un elemento de red sino en el enfoque sistémico del plano tecnológico atendiendo a la naturaleza e interacción de la infraestructura, servicios y protocolos intervinientes.
Esta abstracción de arquitectura, facilita el análisis y planificación de la seguridad de las redes.

Su enfoque apunta a responder preguntas del tipo:
- Qué activos se requiere proteger y contra qué amenazas.
- Cuales son los diferentes elementos de red y como se asocian para su protección.
- Cuales son las diferentes actividades y servicios que requieren protección.

La misma define Dimensiones, Capas (*Layers*), y Planos de Seguridad respectivamente.

Las ocho (8) Dimensiones de Seguridad son:
1. Control de Acceso
2. Autenticación
3. No Repudio
4. Confidencialidad
5. Seguridad de las comunicaciones (tráfico)
6. Integridad
7. Disponibilidad
8. Privacidad

Define además tres (3) Capas o *Layers*:

1. Infraestructura, que soporta los:
2. Servicios de red, prestados a:
3. (las) Aplicaciones

[43] wireless, opticas, wired, voz, datos, convergencia, etc.

Cada *Layer* de las anteriores tiene sus propias vulnerabilidades, protocolos, gestión y controles.

A su vez, se definen tres (3) planos:
1. Gerencia / Gestión.
2. Control.
3. Usuario Final.

Estos planos refieren a las necesidades de gestión de actividades, control de red y actividades o aplicaciones relacionadas al usuario final respectivamente.

La seguridad en cada plano debería de garantizarse de forma independiente de los otros, por ejemplo las actividades del usuario final (fallas o ataques) no deberían afectar las operaciones y tráfico de Control y Gestión de la red. De lo contrario, se volvería problemático cortar ciertos tipos de ataques.

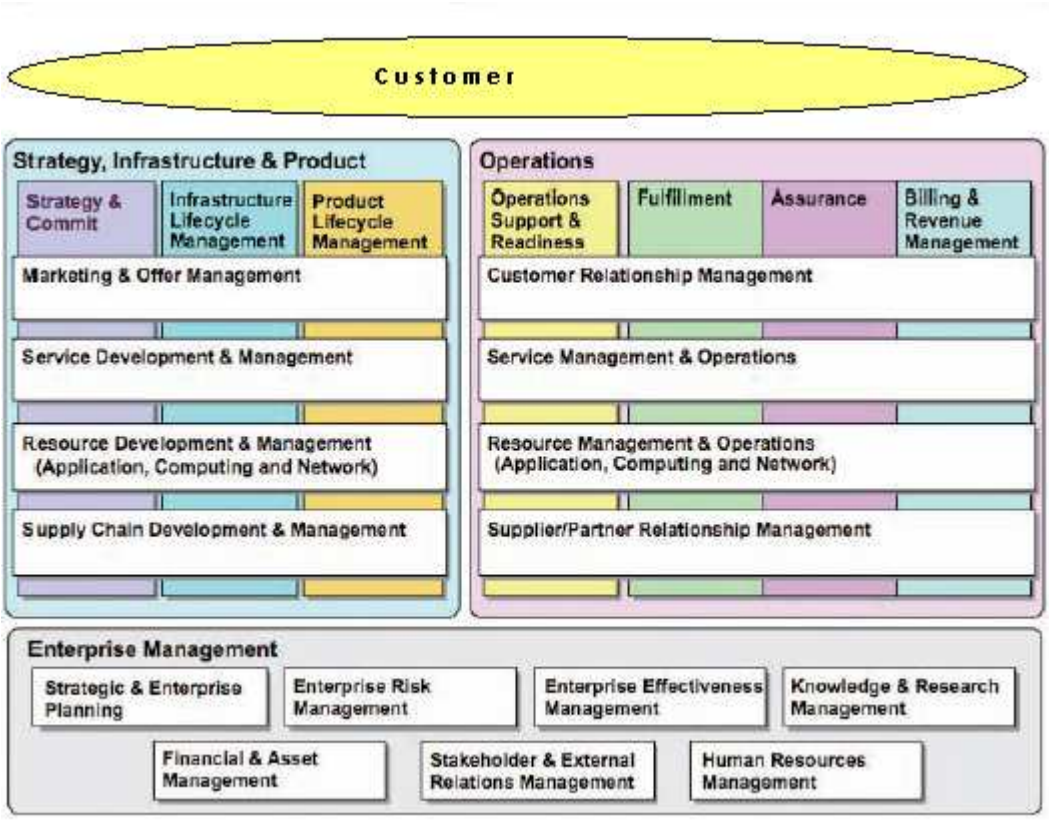
En la siguiente tabla se muestra como afectan las amenazas típicas a las ocho dimensiones definidas:

Dimensión	**Amenazas**				
	Destrucción	Alteración/ Corrupción	Robo/ Borrado o Pérdida	Divulgación	Interrupción de los servicios
Control de Acceso	Si	Si	Si	Si	
Autenticación			Si	Si	
No Repudio	Si	Si	Si	Si	Si
Confidencialidad			Si	Si	
Comunicaciones			Si	Si	
Integridad	Si	Si			
Disponibilidad	Si				Si
Privacidad				Si	

ANEXO E

Enhaced Telecommunications Operations Map (eTOM)

El Mapa de Operaciones de una TelCo (TOM) es un modelo de gestión creado por el Foro de TeleGerenciamiento (parte de la ITU-T) y reemplaza el modelo anterior de *Telecommunications Management Network* (TMN). eTOM (*enhanced TOM*) es la versión actual y describe el alcance de los procesos de negocios requeridos por un proveedor de servicios y sus interacciones. Este modelo fue adoptado como *ITU-T International Recommendation M.3050* [34].



Satisfacción / Calidad de Servicio (*Fulfillment*):
Comprende los procesos y operaciones necesarias para proveer a los clientes de los productos y/o servicios con los niveles de servicio esperados / comprometidos (en tiempo y forma). Incluye el servicio al cliente y vela por su satisfacción.

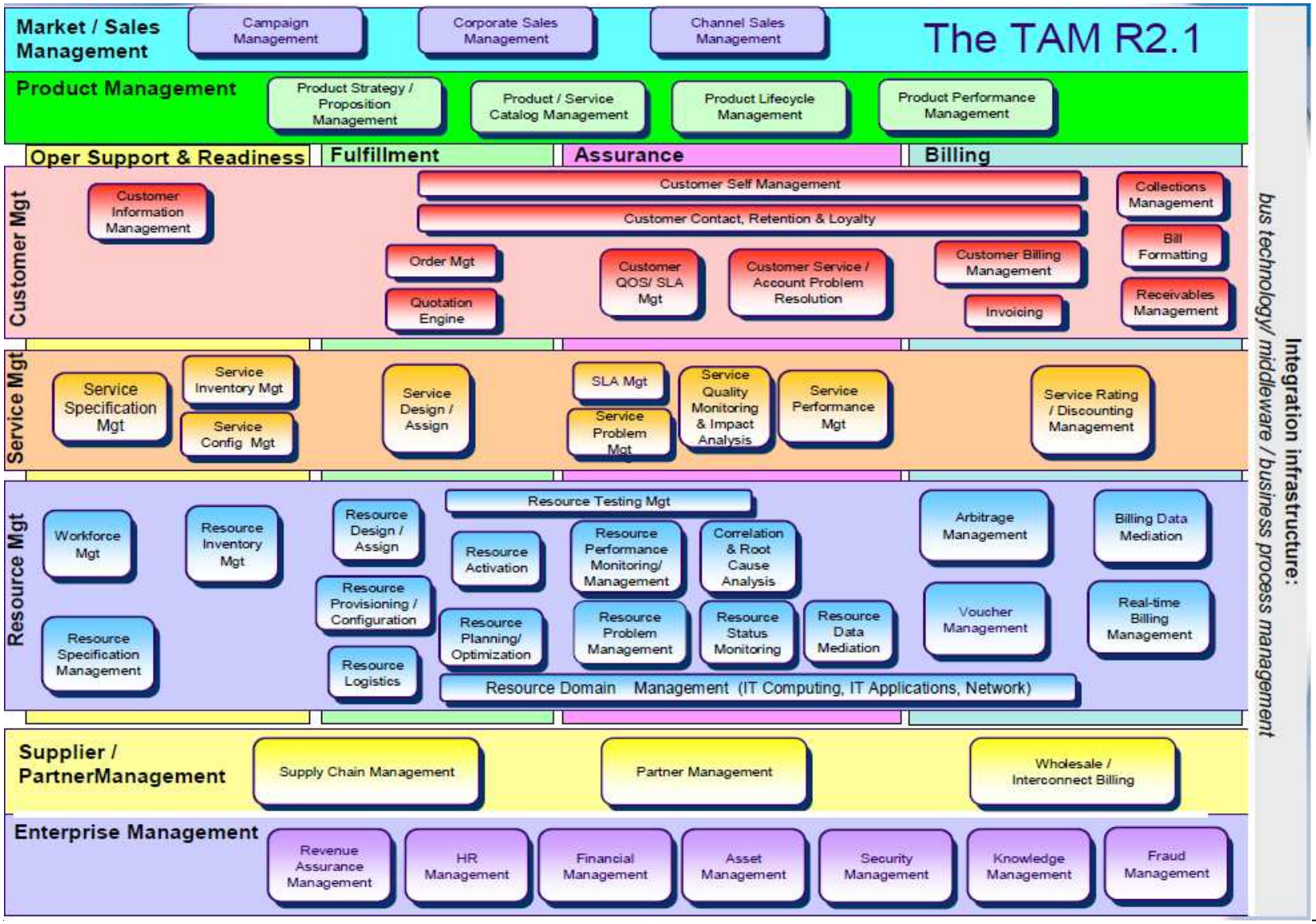
Aseguramiento (*Assurance*):
Brega por todas las actividades necesarias tanto proactivas como reactivas (mantenimiento preventivo y reactivo) para asegurar la continua disponibilidad de los servicios, y el cumplimiento de los niveles de servicio comprometidos (*SLAs*) y niveles de calidad esperados

(QoS). Implica el continuo monitoreo y revisión de los procesos para detectar potenciales fallas de forma proactiva, analizando la información e indicadores de servicio para detectar posibles anomalías antes que impacten en el servicio al cliente (o sean percibidos por éste por ej. por degradación del servicio). En caso que las fallas, anomalía o fallas en el servicio ocurran, velan por y actúan para su restauración a los niveles adecuados.

Facturación y Cobranza (*Billing*):
Todo lo referente a la información de tiempo de uso de los servicios, servicios prepagos, facturación y cobro.

Operaciones y Soporte (Operations Support & Readiness):
Es responsable por el gerenciamiento y gestión, logística y administración de las actividades de soporte necesarias para la eficiencia operativa de los tres grupos anteriores. En general no tienen cara visible al cliente.
A su vez, las tres primeras áreas se abren en:

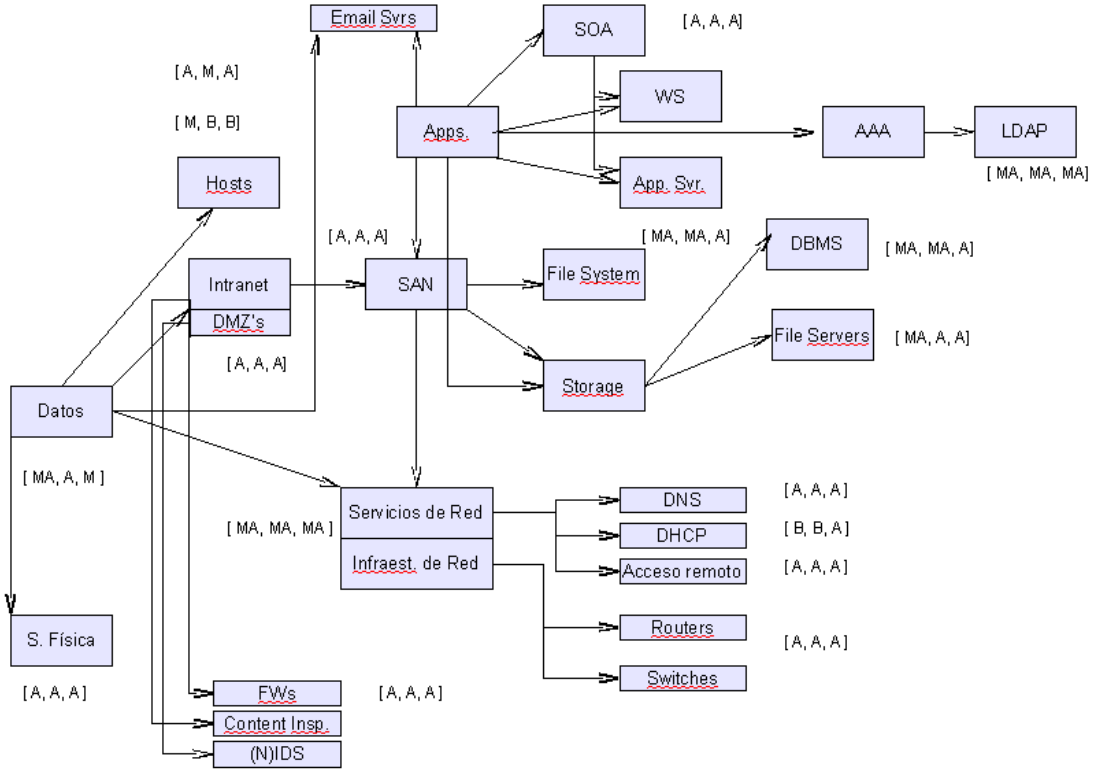
- Gestión de Clientes
- Gestión de Servicios
- Gestión de Recursos / Logística
- Gestión de Proveedores / Socios de negocios
- Gerencia Corporativa y Gestión Empresarial.


The TAM R2.1
Market / Sales Management
Campaign Management
Corporate Sales Management
Channel Sales Management
Product Management
Product Strategy / Proposition Management
Product / Service Catalog Management
Product Lifecycle Management
Product Performance Management
Oper Support & Readiness
Fulfillment
Assurance
Billing
Customer Mgt
Customer Information Management
Customer Self Management
Customer Contact, Retention & Loyalty
Collections Management
Bill Formatting
Order Mgt
Quotation Engine
Customer QOS/ SLA Mgt
Customer Service / Account Problem Resolution
Customer Billing Management
Invoicing
Receivables Management
Service Mgt
Service Specification Mgt
Service Inventory Mgt
Service Config Mgt
Service Design / Assign
SLA Mgt
Service Problem Mgt
Service Quality Monitoring & Impact Analysis
Service Performance Mgt
Service Rating / Discounting Management
Resource Mgt
Workforce Mgt
Resource Inventory Mgt
Resource Design / Assign
Resource Testing Mgt
Resource Activation
Resource Performance Monitoring/ Management
Correlation & Root Cause Analysis
Arbitrage Management
Billing Data Mediation
Resource Provisioning / Configuration
Resource Planning/ Optimization
Resource Problem Management
Resource Status Monitoring
Resource Data Mediation
Voucher Management
Real-time Billing Management
Resource Specification Management
Resource Logistics
Resource Domain Management (IT Computing, IT Applications, Network)
Supplier / PartnerManagement
Supply Chain Management
Partner Management
Wholesale / Interconnect Billing
Enterprise Management
Revenue Assurance Management
HR Management
Financial Management
Asset Management
Security Management
Knowledge Management
Fraud Management
Integration infrastructure:
bus technology/ middleware / business process management

ANEXO F

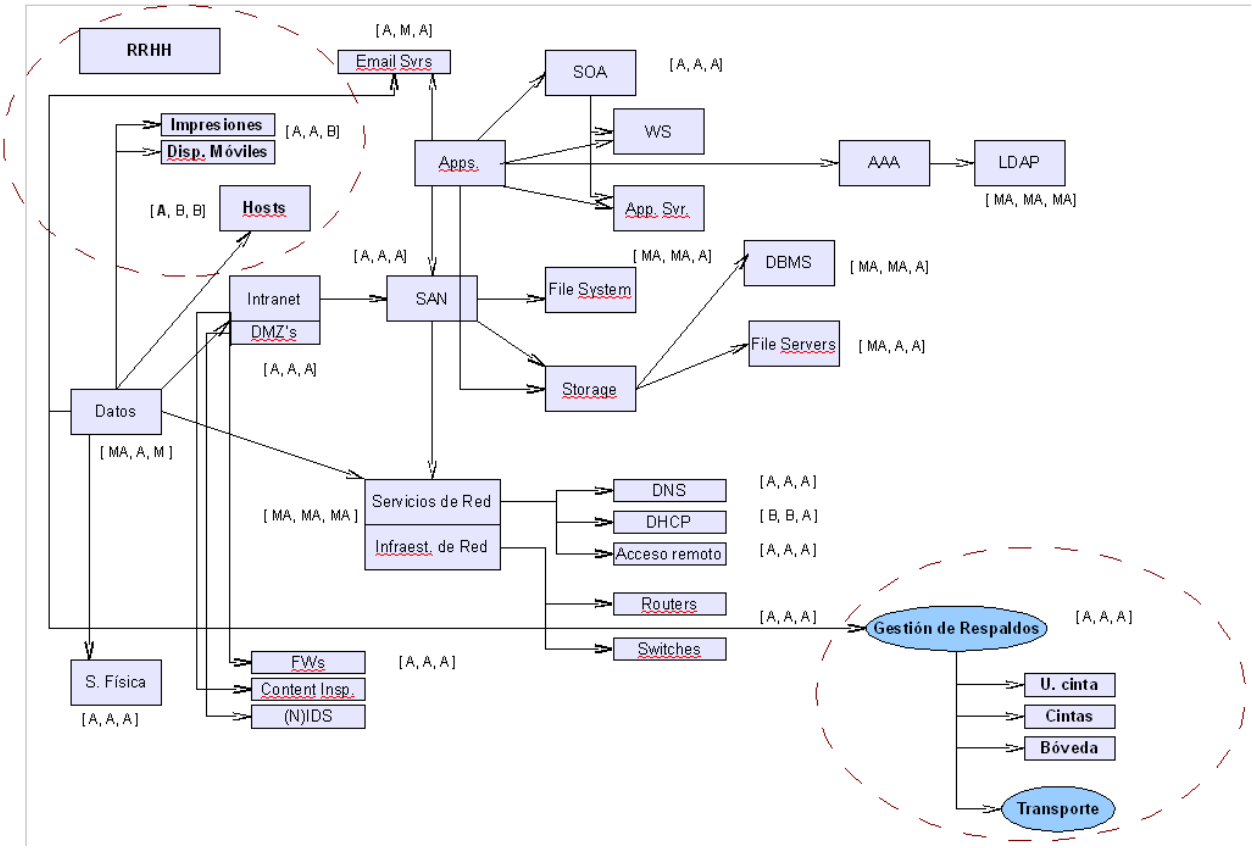
Grafos y Subgrafos de Valoración de la Seguridad de la Información

Como se describe en el documento principal, un grafo de dependencias de valoración de los activos, contiene un vínculo dirigido desde el activo dependiente hacia su activo requerido. Es posible valorar cualitativamente a los activos asignando según una escala adecuada y conveniente para la organización, valores a una terna [C, I, D] de: Confidencialidad, Integridad y Disponibilidad respectivamente.



A su vez**,** es posible construir un subgrafo de valoración específico para determinada propiedad o dimensión de seguridad que sea relevante o prioritaria para la Organización. Este subgrafo se construye a partir del grafo de valoración pero filtrando por la propiedad analizar y quedándose con el subgrafo inducido por los activos y procesos relevantes.
Esto permite no sólo focalizarse en un problema específico y por tanto más simple, y así aparecerán nuevos activos que quizás no hayan sido tenidos en cuenta.

Subgrafo de valoración con foco en la Confidencialidad:



De la misma manera, focalizados en la Confidencialidad, sobre el subgrafo de valoración específico para analizar este aspecto, es posible analizar las amenazas y establecer los Controles a implantar.

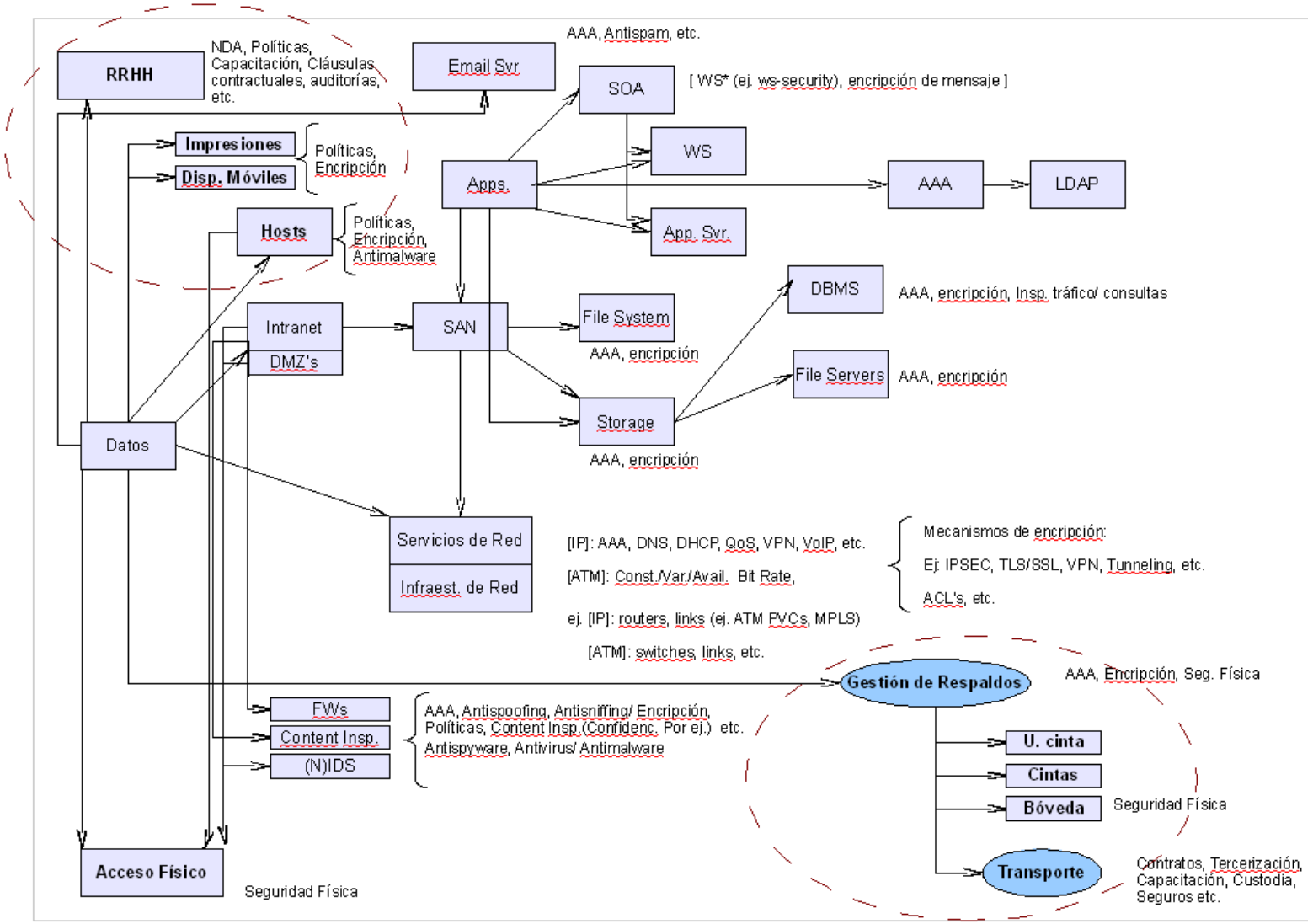
Observar por ejemplo que la dinámica del contexto puede hacer variar el escenario de valoración de riesgos y activos a los que eventualmente hay que prestar mayor atención y quizás cambien su valoración.
Un ejemplo es la Ley de Protección de Datos Personales, sin dudas la necesidad de la confidencialidad y la privacidad no surgen con esta ley, pero si toma otro peso y otra dimensión el carácter y la responsabilidad legal que puede hacer que por ej. información que antes no era clasificada como confidencial, ahora sí lo sea, y por lo tanto haya que o bien cambiar los procedimientos o bien revisar y aumentar los controles sobre por ejemplo: *hosts*, dispositivos móviles, impresiones, etc. Un ejemplo muy básico sería por ejemplo un PC de secretaría de RRHH que recibía *Curriculums Vitae* (CV) de potenciales aspirantes a integrarse a la empresa, ese mecanismo deberá ser revisado tanto desde la recepción de esos CV así como su almacenamiento y acceso dentro de la empresa.

Este tipo de gráficos también permite detectar ciertos procesos que requieren de controles específicos, en el ejemplo se resalta la Gestión de Respaldos con el subproceso de transporte de los mismos a un sitio secundario.

En la página siguiente se muestra el mencionado grafo con algunos ejemplo de posibles controles o estrategia para el tratamiento de riesgos:

Anexo F

Subgrafo de dependencias con foco en la confidencialidad y ejemplo de posibles controles:



Además, para el enfoque en el análisis de riesgos, se sugiere utilizar la Recomendación ITU-T X.805 (ISO/IEC 18028-2) a los efectos de considerar la seguridad por capas, en los diferentes planos y atendiendo las ocho dimensiones.

A modo de ejemplo, si consideramos la red IP, la Capa de Infraestructura del modelo presentado en la Recomendación ITU-T referida ([44]), comprende los routers y los links entre routers (por ej. ATM pvc) y las servidores requeridos para los servicios de red. La Capa de Servicios refiere a los servicios básicos de red, por ej.: conectividad, AAA, DNS, DHCP, etc., así como también otros servicios de mayor nivel: VoIP, QoS, VPN, etc.
La Capa de Aplicaciones, refiere a las aplicaciones en sí mismas sobre los servicios IP, por ej. el email, servicios web, etc.

La Recomendación referida propone una estrategia de análisis que sirve a los efectos de guia al momento de analizar y establecer controles adicionales a los que aparecen en el Anexo A de la norma ISO/IEC 27.001.
En ese sentido, se adecua fielmente a los principios conocidos de "Seguridad por en profundidad" (por capas) y la estrategia de "Divide & Conquer" en el sentido de focalizarse en un problema parcial o más focalizado para luego combinar las soluciones encontradas en cada nivel de abstracción y en cada contexto técnico.

En lo que refiere específicamente a las Telecomunicaciones, de acuerdo a como lo establece la Recomendación ITU-T X1051 ([45]), las empresas del sector deberían guardar confidencialidad de: a) la existencia, b) el contenido, c) la fuente, d) el destino y e) fecha y hora de las comunicaciones.
Esto involucra, desde dispositivos de red, servidores y las propias comunicaciones entre ellos.

La ventaja de la arquitectura presentada en los documentos de referencia, es que es aplicable a diferentes niveles de abstracción (y protocolos en el stack de comunicaciones), por ej. para una red ATM, la Capa de Infraestructura refiere a los switches, links entre switches, etc. La Capa de Servicios, refiere a los diferentes servicios de transporte en una red ATM (constante / variable / *available Bit Rate*, etc.)). La Capa de Aplicaciones refiere en este caso, a aplicaciones finales sobre ATM, como una video conferencia.

[44] Correspondiente a la norma ISO/IEC 18.028-2
[45] Correspondiente a la norma ISO/IEC 27.011

ANEXO G

Propiedades del Grafo Valuado de Dependencias

Sea G = (V, R, grado), un grafo dirigido y valuado donde:

Sea V el conjunto de Activos([46]) de la Organización.
Sea R: VxV que definimos de la siguiente manera:

iv) R es irreflexiva, es decir dados i, j/ $(V_i,V_j) \in R$ entonces $i \neq j$.
v) R es transitiva, es decir, dados i, j, h/ $(V_i,V_j) \in R$ y $(V_j,V_h) \in R$ entonces $(V_i,V_h) \in R$.
vi) $(V_i,V_j) \in R$ si la seguridad requerida para V_i depende (de la seguridad requerida) de V_j. Dicho de otra manera, si un incidente que vulnere la seguridad de V_j vulnera también la seguridad de V_i.

Sea además $g_{ij} = grado_{<atributo>}(V_i \rightarrow V_j)$, el grado de dependencia de V_i respecto de V_j, en cuanto a la seguridad de la información definido de la siguiente manera:

$grado_{<atributo>}(A \rightarrow B) =$

- 0 si la seguridad (*) de A no depende, ni siquiera parcialmente, de la seguridad de B.
- 1 si la seguridad de A depende totalmente de la seguridad de B y la violación de seguridad de B implica la violación de la seguridad de A (respecto de <*atributo*>).
- x / $0 < x < 1$, es decir, un valor intermedio entre 0 y 1 si la dependencia es parcial. Cuanto mayor sea el grado de dependencia respecto del <*atributo*>, mayor es la dependencia del activo en cuestión o dicho de otra manera el activo es más sensible a la seguridad del activo del cual depende.

NOTA(*): En todos los casos donde dice 'seguridad' se refiere a la seguridad respecto del <*atributo*>, es decir: Confidencialidad (C), Integridad (I) o Disponibilidad (D), siendo sus grados g_c, g_i, o g_d respectivamente.

Al grafo G = (V, R, g) lo llamaremos Grafo Valuado de Dependencias.

Afirmamos:

1. G es un grafo dirigido acíclico.
2. Es posible, revisar los vértices del grafo, según un orden topológico, revisando que $Val(V_j) >= g_{ij} * Val(V_i)$, . $(V_i,V_j) \in R$ con i < j, o redefiniendo $Val(V_j)$ en caso contrario.

[46] En su acepción más amplia, incluyendo también los procesos (de negocios).

NOTA:

Si se utiliza valuación cualitativa de sus nodos, siendo el dominio: Val_1, Val_2,..., Val_h,...Val_n por ejemplo, a los efectos de poder operar con los mismos, definimos la siguiente aritmética para el operador '*':

Sea Val_h un valor cualitativo cualquiera, por ejemplo el de Ai, esto es: $Val(A_i)=Val_h$, definimos:

$$gij * Val_h = \begin{cases} Val_{(trunc\ (h\ x\ gij)\ +\ 1)}\ , & \text{si } h\ x\ gij > trunc(h\ x\ gij) \quad (^{47}), \\ Val_{(trunc\ (h\ x\ gij))}\ , & \text{sino.} \end{cases}$$

Demostraremos que G = (V,R,g) es acíclico:

R define sobre V un orden parcial estricto, es decir:
i) R es irreflexiva por definición: $(V_i,V_i) \notin R\ \forall_i$.
ii) R es transitiva por definición.

Por lo tanto G(V,R,g) es un grafo dirigido acíclico.

En efecto, por absurdo *supongo que existe al menos un ciclo* $\{ V_p, ..., V_h, ...V_p\}$
Por clausura transitiva tengo que $(Vp, Vp) \in R$ ([48])**,** lo cual es absurdo ya que contradice la definición de G = (V,R,g). Por lo tanto *lo supuesto es falso* y *queda demostrado que G es acíclico*.

Como G de dirigido y acíclico, existe al menos un orden topológico (S) de G, siendo ([49]):

S = $(\ldots V_i,\ldots V_j\ldots)$ que cumple:

(i) cada nodo de G aparece exactamente una vez en S.
(ii) Si $V_i, V_j \in V$ / V_j es alcanzable desde V_i, se cumple que V_i precede a V_j en S.

[47] trunc: *R* -> N, es la parte entera de *R*.
[48] La clausura transitiva de R es R, por definición de R.
[49] Por definición de Orden topológico, Teoría de Grafos.

ANEXO H

Códigos de estados de los estándares ISO.

Se presentan a continuación los códigos utilizados por la ISO [61] durante las diferentes etapas en el proceso de publicación de un estándar desde que el mismo es propuesto hasta que es aprobado.

Código	*Descripción*	*Etapa*
NP	Proposal for new project	Proposal stage
WD	Working Draft	Preparatory stage
CD	Committee Draft	Committee stage
DIS	Draft International Standard	Enquiry stage
FDIS	Final Draft International Standard	Approval stage
	International Standard	Publication stage