Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis

Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio

Autor
Marcia L. Maggiore

Director de Tesis
Dr. Raúl Saroka

Año 2014
Cohorte 2009

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

FIRMADO

Marcia Liliana Maggiore

DNI 6.223.111

Resumen

En virtud del avance tecnológico y la criticidad de la información que procesan las organizaciones, éstas afrontan la problemática de evaluar si la gestión de la seguridad de la información que llevan adelante es efectiva y forma parte de un proceso de mejora continua.

Una manera de realizar dicha evaluación es utilizando un modelo de madurez que establezca las metas a lograr para avanzar a través de los diferentes niveles que conforman la escala de valoración.

Ahora bien, los estándares vigentes establecen la necesidad de diseñar un plan de seguridad de la información para proteger a ésta de su divulgación o modificación no autorizada, así como para lograr su disponibilidad permanente; el cual se obtendrá como resultado de la gestión de los riesgos asociados. Es decir que, para realizar la evaluación mencionada en el primer párrafo, será necesario contar con un modelo de madurez que no sólo permita evaluar los procesos involucrados en la gestión de la seguridad de la información, sino también aquellos asociados a la gestión de los riesgos vinculados al tratamiento de la información en todas sus fases, ya que de ello depende un adecuado plan de seguridad de la información, así como los asociados a la implementación del plan/programa de seguridad.

El presente trabajo entonces, encarará la selección de un modelo de madurez para la evaluación de la gestión de riesgos, de la gestión de seguridad de la información y del plan/programa de seguridad de la información, integrados en el negocio[1]. Esta selección y la aplicación del modelo en cuestión se basarán en las premisas establecidas por las asociaciones profesionales, autores y estándares internacionales respecto del Sistema de Gestión de Seguridad de la Información, la gestión del riesgo, la integración de las tecnologías de información y las comunicaciones (TIC) en los procesos de negocio, así como la gestión de calidad.

[1] El término negocio se usa aquí en un sentido amplio haciendo referencia tanto a actividades comerciales, industriales como de gobierno.

Palabras Clave

Gestión de riesgos, gestión de seguridad de la información, modelo de madurez, mejora continua, objetivo de control, implementación de controles, formalización de buenas prácticas, integración de procesos de tecnología de la información, procesos de negocio.

Índice

Prólogo

Si bien la presentación de este trabajo culmina un esfuerzo personal importante, creo que no hubiera sido posible sin la formación, los conocimientos y la experiencia aportada, abierta y desinteresadamente, por los docentes que nos guiaron durante estos años de estudio. A ellos mi agradecimiento y en particular al Dr. Raúl Saroka, director de esta tesis.

Vaya también ese agradecimiento a mi esposo Andrés y a mis hijas Verónica y Mariela, quienes pacientemente me acompañaron y me sufrieron; a mis padres, a mi tío Oscar y a mi abuelo Manuel que, si bien ya no están conmigo, fueron los que hicieron todo lo posible por conducir y satisfacer mi sed de conocimientos; a mis compañeros de trabajo que me alentaron y festejaron todos mis logros y a Patricia Prandini, compañera inseparable de los años de estudios y de los que siguieron como docente, .

Introducción

Dada la significativa evolución que durante las pasadas dos décadas tuvo la gestión de la seguridad de la información, así como los marcos[2] de gobierno y riesgos, tanto corporativos como de las tecnologías de la información y las comunicaciones (TIC), se hizo necesario contar con precisiones respecto del modo en que dicha gestión debiera ser llevada a cabo, a fin de asegurar el logro el cumplimiento de los objetivos de negocio.

Es así como han sido desarrollados diversos estándares internacionales y regulaciones nacionales (por ejemplo en el ámbito de la Administración Pública y del Sistema de Entidades Financieras bajo la supervisión del Banco Central de la República Argentina) que definen los principios básicos en algunos casos, y aspectos de control detallados en otros, para lograr una efectiva gestión de la seguridad de la información. Ellos abarcan desde conceptos tan globales como el planteo estratégico de la seguridad de la información hasta cuestiones operativas.

Las organizaciones, que hasta ahora han resuelto básicamente los problemas tecnológicos de la seguridad de la información aplicando algunas recomendaciones sobre buenas prácticas, en este nuevo contexto intentan adecuar su gestión según alguno o varios de los estándares vigentes. Sin embargo, no es suficiente implementar lo que los estándares proponen. Es necesario contar con algún mecanismo que permita evaluar si los procesos involucrados, en función de la manera en que han sido implementados, resultan efectivos en el logro del objetivo para el que fueron diseñados, tienen las condiciones necesarias para que la organización pueda administrarlos y más aún, si facilitan la mejora continua de la gestión.

Hace algunos años atrás, el Software Engineering Institute (SEI), centro de investigación y desarrollo patrocinado por el Departamento de

Defensa de Estados Unidos de América y gestionado por la Universidad Carnegie-Mellon, creó un Modelo de Capacidad y Madurez o Capability Maturity Model (CMM), inicialmente utilizado para evaluar los

[2] Marcos. Este término se usa en lugar del vocablo inglés framework.

procesos relativos al desarrollo de software.

A posteriori, distintos estándares comenzaron a aplicar un modelo de evaluación de procesos de las TIC que denominaron "de madurez", emulando el desarrollado por Carnegie Mellon.

Asimismo, a partir del año 2005 apareció en el contexto normativo el estándar ISO/IEC 27001 [1], hito evolutivo de las precedentes BS7799 e ISO 17799, habiendo en pocos años pasado a ser el estándar por excelencia en sistemas de gestión de seguridad de la información. Por lo tanto, dado que ésta definió los requerimientos del Sistema de Gestión de Seguridad de la Información, parece razonable intentar alcanzar un modelo de madurez relacionado con ella.

Ahora bien, podríamos preguntarnos qué herramienta permite la evaluación de la madurez del mencionado sistema de gestión y cuál sería el alcance. Precisamente, la respuesta a estas preguntas pretende ser el aporte de este trabajo. En consecuencia su objetivo es: seleccionar un modelo para la evaluación de madurez de la gestión de la seguridad de la información integrada en los procesos de negocio, así como los riesgos asociados al uso[3] de la información y los controles definidos para su tratamiento.

Una premisa básica de este objetivo es considerar que los riesgos inherentes al uso de la información no tienen como origen exclusivo los aspectos tecnológicos de la seguridad de la información, sino los múltiples ambientes relacionados con la estrategia de negocio, los procesos y su adecuada definición y formalización, así como la concientización, competencias, habilidades y responsabilidades del capital humano. Por ende, el modelo de madurez a definir tendrá que tener en cuenta estas variables.

En el marco del planteo del problema expuesto, el trabajo analizará los conceptos que dan sustento al objetivo definido y su justificación, a saber:

---

[3] USO - De aquí en adelante se utilizará este término para referirse al almacenamiento o guarda, procesamiento o utilización y transferencia o traslado de la información escrita, digital, electrónica o verbal.

- la necesidad de integrar las TIC y la seguridad de la información en los procesos de negocio;
- la necesidad de integrar la evaluación de riesgos de seguridad de la información en la evaluación de riesgos de negocio y de redefinir el plan de seguridad de la información;
- la necesidad de evaluar los eventos[4] asociados al uso y gestión de la información, y no sólo las amenazas y vulnerabilidades de los activos informáticos, que potencialmente afecten en forma adversa el logro de los objetivos organizacionales (riesgo);
- la necesidad de evaluar los sistemas de gestión y las diferentes herramientas utilizadas para ello;
- la importancia de los procesos, el modelo de madurez como mecanismo de evaluación y de mejora continua, la precisión en su definición y alcance, y la justificación de su uso;
- el alcance de la evaluación. Es decir, a partir del resultado de los conceptos previamente analizados, ¿qué deberíamos evaluar? ¿cuál o cuáles procesos evaluaríamos?

Este enfoque permite poner en contexto la seguridad de la información, temática que es actualmente subvalorada por quienes cumplen roles en la definición de estrategias, el gobierno o gestión de las organizaciones.

Una materia que fue relegada durante muchísimo tiempo a los aspectos tecnológicos cobra hoy una importancia relevante en virtud de que la información se ha transformado en un factor de éxito de los negocios mundiales. Transacciones bancarias, documentos contractuales, situación económica de las organizaciones, fiabilidad de clientes y proveedores, servicios que cruzan los límites físicos de las naciones a velocidades impensables medio siglo atrás, fusiones de empresas, estadísticas, asuntos legales y policiales, etc., etc.

---

[4] Evento - ISO Guide 73:2009 - Gestión de Riesgos - Vocabulario. Definición: Ocurrencia o cambio de un particular conjunto de circunstancias. Notas: puede ser referido algunas veces como incidente o accidente, puede ocurrir una o varias veces, puede tener varias causas y puede consistir en algo que no pasa.

Un elemento imprescindible para lograr la sustentabilidad de esta gran arquitectura mundial de la información es una adecuada seguridad de la información a partir de la evaluación de riesgos de negocio.

Creemos que este trabajo aportará una mirada más amplia para el análisis de la temática que nos ocupa y una herramienta enfocada en el negocio permitiendo así reducir la brecha entre los responsables técnicos y aquellos que deben lograr los objetivos estratégicos planteados por las organizaciones y que requieren el soporte total o parcial de la tecnología y los sistemas de información.

Capítulo I - Una breve reseña histórica

El concepto de seguridad de la información es tan viejo como el hombre mismo. En la época de la transmisión oral de la información, ésta no debía ser transmitida a cualquiera, sino a los que les estaba permitido poseerla (confidencialidad). Luego, con la aparición de los Reinos y su Defensa Militar, fue aún más importante. Pensemos en las guerras medievales cuando los reyes enviaban papel con el sello de su anillo para conservar la confidencialidad (el sello no debía estar dañado al llegar) y la autenticidad (no repudio) y definían una ruta diseñada para permitir el cambio de caballos, utilizando expertos jinetes para llegar a tiempo, cumpliendo así con la disponibilidad. Años más tarde, en siglos más cercanos, aparecen las contraseñas y el cifrado de mensajes para la comunicación entre las tropas.

Si nos remitimos a las primeras organizaciones, cuando la información se encontraba sólo en papel, los mandos medios eran responsables de su cuidado y ellos implementaban medidas de seguridad como armarios con llaves, puertas con doble llave, custodios, etc. El caso más palpable aún hoy es el del papel dinero, información muy crítica que tiene medidas de seguridad extremas, sin relación alguna con las tecnologías de información.

Es decir, el concepto del valor de la información y su necesidad de protección está claramente arraigado en el hombre, en la sociedad y en las organizaciones. Sin embargo, cuando la información se digitaliza y pasa a estar contenida en soportes que se encuentran en un lugar diferente al de trabajo habitual, el personal comienza a desprenderse de la responsabilidad de proteger la información organizacional. Es por ello, que dicha responsabilidad se transfiere al área de TI, cuando ésta sólo tiene responsabilidad sobre su protección en los procesos de TI, en virtud de lo establecido por los procesos de negocio.

Si analizamos lo antedicho, vemos que la digitalización ha provocado una involución en ciertos criterios organizacionales. Pero luego de la aparición de marcos de trabajo, como por ejemplo los desarrollados por el

Committee of Sponsoring Organizations de la Treadway Commission (COSO) en materia de controles y riesgos, vemos claramente la necesidad de integrar nuevamente los conceptos. Lamentablemente esta vuelta a los criterios originales ha tomado cerca de cincuenta años.

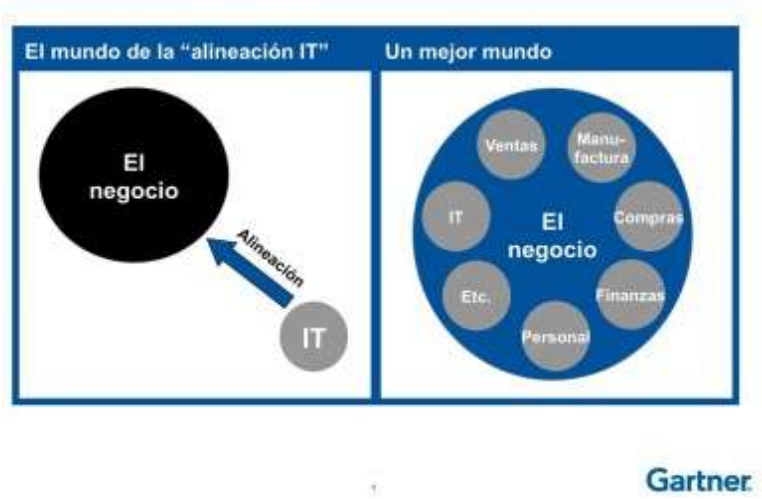
En esos viejos tiempos, los soportes de la información fueron la piedra y luego el papel. La información era visible al ojo del hombre y palpable por sus manos. A medida que la tecnología fue avanzando, la información se fue alejando del origen de producción del dato y por la complejidad de los nuevos soportes, sólo accesible por expertos. Esta situación generó en quienes conducen los negocios, la sensación de que la responsabilidad sobre la información fue transferida hacia las áreas tecnológicas. Ahora tomamos conciencia de que los responsables siguen siendo quienes desempeñan los diferentes roles de negocio, si bien son los técnicos los que deben hacerse responsables de la seguridad en los nuevos soportes, así como del procesamiento y transferencia de dicha información.

Capítulo II – La integración como parte de la nueva visión

La creciente dependencia que los negocios, así como las actividades científicas, académicas, etc. tienen respecto de las tecnologías de información y las telecomunicaciones (TIC), ha incrementado la necesidad de contar con una efectiva gestión de las mismas.

Debemos recordar que la incorporación de las TIC en las organizaciones comenzó a partir de la adquisición de equipamiento para procesar grandes volúmenes de información a mayor velocidad. A tal efecto se incorporó personal experto en la materia que rápidamente fue creando un muro a su alrededor a partir de un lenguaje propio y del concepto de autosuficiencia para lograr una solución a la problemática; situación que llevó a una especie de aislamiento o de independencia de las áreas TIC.

Como reacción a este contexto la academia, las asociaciones profesionales, las consultoras y los grupos de investigación comenzaron a hablar de la necesidad de alinear las TIC con los objetivos de negocio, avanzando recientemente en dicho concepto, para comenzar a hablar de integración [2] de las TIC con el negocio.



Ahora bien, ¿cómo se fue desarrollando el camino hacia dicha integración?

En la segunda mitad de los años 60, varios profesionales que se encontraban trabajando en una auditoría de controles de los sistemas de

información en diferentes compañías de EEUU perciben las dificultades que presentaban las nuevas herramientas para realizar un efectivo control. Es así como se funda la Information Systems Audit and Control Association (ISACA), la cual fue la primera organización que vislumbró la criticidad que tenían las TIC en el logro de los objetivos organizacionales. Asimismo, con el objetivo de investigar estos temas, se establece en 1998 el IT Governance Institute (ITGI), siendo el que utiliza por primera vez el concepto de **gobierno** en el marco de las TIC (Ver Ref. ITGI)

Veamos entonces las definiciones:

> *"El gobierno de la empresa es un conjunto de responsabilidades y prácticas ejercidas por la dirección y los gerentes ejecutivos con el objetivo de proveer dirección estratégica, asegurando que los objetivos son alcanzados, que los riesgos son tratados apropiadamente y verificando que los recursos son usados con responsabilidad."* [3]

> *"El gobierno de las TI es responsabilidad de la dirección y de los gerentes ejecutivos. Es parte del gobierno empresarial y se conforma por el liderazgo, las estructuras organizacionales y los procesos que aseguran que las TI dan soporte a los objetivos y estrategias de la organización."*[5] [4]

Es decir que el ITGI integra el gobierno de las TIC con el gobierno corporativo.

Hasta ahora nos hemos referido a la integración y gobierno de las TIC, pero nuestro objetivo es tratar la seguridad de la información. En consecuencia, introducimos a continuación esta temática.

La seguridad de la información en sus comienzos tuvo un abordaje netamente tecnológico, porque éste era el enfoque que prevalecía respecto del uso de la información, tal como analizamos al comienzo del capítulo. A pesar de las regulaciones y normas emitidas respecto de la necesidad de contar con políticas, programas, procesos de evaluación de riesgos, las organizaciones no han logrado un control eficaz de los diferentes

[5] La traducción es obra de la autora.

escenarios[6] que son objeto de tratamiento por parte de la gestión de seguridad de la información. Por supuesto que esta realidad es consecuencia, en primera instancia, de la falta de cumplimiento de dichas reglamentaciones, pero un concepto que fue apareciendo a medida que crecía la complejidad en el uso de la información, es el de la falta de conciencia y compromiso de la alta dirección.

Como premisa para mejorar esta situación, el ITGI establece en su publicación sobre gobierno de la seguridad de la información que *"El gobierno de la seguridad de la información es responsabilidad de la dirección y los gerentes ejecutivos. Debe ser una* ***parte integral***[7] *y transparente del gobierno de la empresa y estar alineada con el marco de gobierno de TI."*[8] [5].

En función de este premisa señala que los resultados esperados del gobierno de la seguridad de la información son: alineación estratégica, gestión del riesgo, gestión de recursos, medición del desempeño y entrega de valor; y entiende que un avance en la mitigación de las posibles "brechas (gaps)" en los que podrían filtrase amenazas sería la integración de procesos de aseguramiento en relación con los procesos de seguridad (Ver Ref. GobSI). Este concepto es el núcleo de la idea de "convergencia" [6], desarrollada en otra publicación del ITGI orientada a la conducción gerencial, la cual refuerza lo antedicho alertando sobre la posible existencia de riesgos no identificados, al no considerar todos los procesos de seguridad en conjunto (Ver Ref. Cvg). Y agrega, en consonancia con la guía para el consejo de dirección:

> *"… la seguridad de la información concierne a todos los procesos de la información, física y electrónica, independientemente de si involucran gente y tecnología o relaciones con socios comerciales, clientes y terceras partes. […] a todos los aspectos de la información y*

---

[6] Se utiliza el vocablo escenario para identificar de manera genérica el conjunto de activos de la información y los eventos relacionados.

[7] El formato "negrita" no corresponde a la obra original. Ha sido utilizado por la autora para destacar la frase.

[8] La traducción y el destacado de los términos son obra de la autora.

a la protección total en todos los puntos dentro del ciclo de vida de la información utilizada en la organización.[…] trata con todos los aspectos de la información, ya sea hablada, escrita, impresa, electrónica o en cualquier medio e independientemente de si es creada, vista, transportada, almacenada o destruida. Esto contrasta con la seguridad de TI, la cual tiene que ver con la seguridad de la información dentro de los límites del dominio tecnológico. […] la información confidencial divulgada durante una conversación en un ascensor o enviada por servicio postal está fuera del alcance de la seguridad de TI. Sin embargo, desde la perspectiva de la seguridad de información, la naturaleza o tipo de compromiso no es importante, lo que es importante es que se ha filtrado información.

Específicamente, la seguridad de la información refiere a la protección de los activos de la información respecto del riesgo de pérdida, discontinuidad operacional, mal uso, divulgación no autorizada, falta de disponibilidad o daño. También tiene relación con el incremento potencial de la responsabilidad civil o legal que las organizaciones enfrentan como resultado de información inexacta y pérdida o ausencia del debido cuidado en su protección.

Este documento trata la necesidad de una adecuada alineación de las actividades del programa de seguridad de la información para reforzar el entendimiento de que la información es un activo organizacional crítico y que los enfoques ad-hoc del pasado no sirven para tratar las situaciones actuales y emergentes. Como cualquier otra actividad crítica, las actividades del programa de seguridad de la información deben ser rigurosamente planificadas, efectivamente ejecutadas y constantemente monitoreadas al máximo nivel de la organización."[9] [7]

En abril de 2004 la Corporate Governance Task Force, publica un reporte, en el que define que la seguridad de la información no es sólo un tema técnico sino también un desafío para el negocio y su gobernabilidad

[9] La traducción es obra de la autora.

(Ver Ref. CGTF).

Esta publicación alienta al sector privado a incorporar el gobierno de la seguridad de la información en el gobierno corporativo y define un marco para el gobierno de la seguridad de la información, cuya adopción recomienda para incluir efectivamente la ciberseguridad en sus procesos de gobierno corporativo.

En el ítem 7 – Programa de seguridad de las unidades organizacionales, del marco referenciado, se establece que "Cada unidad organizacional independiente debe desarrollar, documentar e implementar un programa de seguridad de la información, consistente con una guía de prácticas de seguridad aceptada como por ejemplo, la ISO/IEC 17799, para proveer seguridad para la información y los sistemas de información que dan soporte a las operaciones y activos de la unidad organizacional, incluyendo aquéllos provistos o gestionados por otra unidad organizacional, contratista u otra fuente." [8]

Sin compartir necesariamente la metodología de descentralización planteada, sobre todo en el aspecto del desarrollo ya que el programa de seguridad de la información dejaría de ser integral, el concepto es muy interesante porque plantea la responsabilidad de cada unidad organizativa.

Por su parte *COBIT® 5 for Information Security*, última versión de esta publicación, la cual toma los conceptos de *Business Model for Information Security (BMIS)* [9] y las ya referidas publicaciones del ITGI, entre otras de la misma fuente, asume que la seguridad de la información es un concepto extendido a través de toda la empresa, con intervención en cada actividad y proceso que se ejecuta.

También el CERT® Coordination Center perteneciente al Carnegie Mellon Software Engineering Institute expresa "*Gobernar para la seguridad de la empresa significa entender que la adecuada seguridad es un requerimiento del que no se puede prescindir para hacer negocios. Si la dirección de una organización no establece y no refuerza la necesidad que tienen los negocios de una efectiva seguridad de la empresa, el estado deseado de seguridad no será articulado, alcanzado ni sostenido en el tiempo. Para alcanzar una capacidad sustentable las organizaciones deben*

hacer responsable de la seguridad empresarial a líderes del nivel de gobierno, no a otros roles organizacionales que carecen de autoridad, responsabilidad y recursos para actuar y hacer cumplir las regulaciones."[10] [10]

Éstas son solamente algunas de las publicaciones sobre la materia, que permiten mostrar que en este siglo se ha desarrollado una corriente muy importante hacia la necesidad de integrar la seguridad de la información en los procesos de negocio.

Para concluir este capítulo, transcribiremos el resumen de la publicación *Integración Balanceada de la Seguridad de la Información en la Gestión de Negocios* [11], fundamentalmente por el enfoque de procesos al que alude, ya que éste es un pilar fundamental de este trabajo.

> *"La información es un bloque básico de la construcción de nuestra sociedad moderna y necesita ser protegida. Este artículo, enfoca la cuestión de la seguridad de la información desde el punto de vista de la gestión del negocio. La seguridad de la información no es una entidad separada, aislada del resto de las prácticas de negocio; por el contrario, constituye una parte integral de sistema moderno de gestión de negocios y asiste a la organización para lograr y mantener un margen competitivo sobre sus rivales de negocio. El objetivo para el desempeño del negocio, incluyendo la seguridad de la información, es superioridad sobre los competidores. Cumpliendo sólo el mínimo de los requerimientos o logrando mediocridad no es suficiente.*
>
> *Desde que los negocios modernos están basados en un enfoque de procesos,* ***también la seguridad de la información está integrada en la gestión de los procesos de negocio.***"[11]

A partir de nuestra experiencia en la gestión, compartimos los conceptos señalados en los párrafos precedentes y podríamos dar cuenta de los esfuerzos requeridos para transformar la visión tecnológica en una visión

---

[10] La traducción es obra de la autora.

[11] El formato "negrita" no corresponde a la obra original. Ha sido utilizado por la autora para destacar la frase.

integral.

En un orden más práctico, si se quiere, dentro de las tareas que corresponden al desarrollo de un programa de seguridad de la información, ISACA menciona en su *Manual de Preparación para el examen de Certificación en Gestión de la Seguridad de la Información (CISM)*, las de:

- Integrar los requerimientos de seguridad de la información en los procesos de la organización (por ej. control de cambios, fusiones y adquisiciones)
- Integrar los controles de seguridad de la información en los contratos (por ej. de emprendimientos conjuntos (*joint ventures*), proveedores externos, socios comerciales)

Asimismo, la propia norma ISO/IEC 27001 en su introducción define "*Es importante que el sistema de gestión de seguridad de la información sea parte de y esté integrado en los procesos organizacionales y en la estructura global, y que sea considerado en el diseño de los procesos, los sistemas de información y los controles*."

Para terminar, debemos tener en cuenta que la seguridad de la información alcanza a todo tipo y envergadura de organizaciones y no es proporcional al tamaño de las mismas, sino que tiene relación con la criticidad y sensibilidad de la información y de los procesos que maneja, así como cuán avanzadas se encuentran en el uso de las TIC. Por ello y por la necesidad de adecuarla a la dinámica de los negocios, donde los procesos se modifican y mutan permanentemente, se hace necesaria su integración.

La confiabilidad de la información, un concepto básico en los negocios, depende de su seguridad.

Capítulo III – Del plan de seguridad hacia el plan de tratamiento de riesgos

Históricamente, en la gestión corporativa y también en la de las TIC, se desarrollaron en primera instancia los mecanismos de control como medio para asegurar el logro de los objetivos de negocio. Recordemos lo relatado en el capítulo anterior respecto de los comienzos de ISACA.

En el ámbito corporativo, el Committee of Sponsoring Organizations de la Treadway Commission (Grupo COSO) [12], el cual comienza sus actividades en el año 1985, publica en 1992 el Marco de Control Interno, precisamente como un avance hacia la evaluación del sistema de control interno y sus mecanismos de mejora.

También en el ámbito de la seguridad de la información, el British Standards Institution (BSI) más un grupo de empresas y de organizaciones del gobierno británico desarrollaron inicialmente una serie de buenas prácticas (controles). Éstos comienzan a ser definidos por la serie BS7799 (1995) y luego por la ISO17799 (2000).

Ahora bien, los acontecimientos de fines del siglo pasado y principios de éste (Ej.: Enron, Worldcom, la burbuja puntocom) movilizaron nuevamente a los especialistas, dado que los mecanismos implementados a esa fecha no habían dado los resultados esperados.

El grupo COSO, que sólo había referenciado el concepto de evaluación de riesgo en su primer informe, comienza a desarrollarlo en profundidad a partir del 2001 y publica en el año 2004, un marco integrado para la gestión de riesgos corporativos, que dio en llamarse *Enterprise Risk Management Integrated Framework* o *ERM Integrated Framework* [13], el cual introduce los principales conceptos y define la metodología a utilizar.

Es así como los marcos ya referidos introducen los conceptos de riesgo y control, los cuales han evolucionado hasta el paradigma actual de gobierno, riesgo y cumplimiento (GRC).

A través de la penetración de las tecnologías de información a partir de lo que se conoce como Sociedad de la Información, a finales del siglo XX,

los marcos, modelos, metodologías que se gestan a nivel corporativo son luego incorporados por la gestión de las mencionadas tecnologías. Lo cual es razonable teniendo en cuenta que, de la adecuada gestión de los procesos asociados a las tecnologías de información depende el logro de los objetivos de negocio, tal como lo analizamos en el Capítulo II - LA INTEGRACIÓN COMO PARTE DE LA NUEVA VISIÓN. En consecuencia, cada uno de esos procesos debe también adoptar los principios de riesgo, control y cumplimiento ya mencionados. Siendo la seguridad de la información uno de esos procesos, es natural entonces que los incorpore.

En virtud de este nuevo paradigma, surgen las normas ISO/IEC 27001 y 27002 [14] **incorporando el concepto de sistema de gestión de la seguridad de la información a partir de la evaluación de riesgos**. Ambas consideran que los controles a aplicar (plan de tratamiento del riesgo) deben ser definidos en virtud del resultado de la evaluación de riesgos, ya que diferentes organizaciones no sólo pueden enfrentar distintos riesgos, sino también contar con criterios y umbrales de aceptación propios.

Tomando estos principios, el estándar ISO/IEC 27001 define los requerimientos de un Sistema de Gestión de Seguridad de la Información (SGSI) indicando que "*la organización debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado en el* ***contexto global de las actividades de negocio y de los riesgos que enfrenta una organización"***[12]**.**

Uno de los requerimientos para establecer el sistema es seleccionar los objetivos de control para el tratamiento de los riesgos. Para lo cual dirige hacia su Anexo A, el cual contiene una exhaustiva lista de controles a implementar. El contenido de dicha lista es posteriormente detallado por el estándar ISO/IEC 27002.

También ISACA, en su *Manual de Preparación para el examen de Certificación en Gestión de la Seguridad de la Información (CISM)* expresa que "*La gestión de riesgos y el desarrollo de las evaluaciones y los análisis*

[12] El formato "negrita" no corresponde a la obra original. Ha sido utilizado por la autora para destacar la frase.

de impacto al negocio son requerimientos previos fundamentales para desarrollar una estrategia de seguridad significativa. Las organizaciones que desarrollan un programa de gobierno de la seguridad de la información incluirán, por necesidad, las gestión de riesgos como una parte integral del programa en su conjunto."

Posteriormente, en junio del año 2008 se publica la ISO/IEC 27005 [15], que cuenta con una revisión del año 2011.

La ISO/IEC 27005 provee guías para la gestión de riesgos, basada en el marco establecido por COSO ERM y recomienda fuertemente tomar en cuenta todas las situaciones en las que pueda existir riesgo de seguridad de la información, brindando sólo algunos ejemplos.

La experiencia en la implementación de estas normas nos permite afirmar que no están claramente asociados en ellas, el control con el riesgo a mitigar. Ésta es una práctica que debe realizar cada organización, tal como establecen las normas en cuestión: contar con un sistema de evaluación de riesgos para implementar controles costo-efectivos y adecuados a la naturaleza de la organización.

Es por ello, que las organizaciones deben definir su programa de seguridad de la información a partir del plan de tratamiento de los riesgos que enfrenta la información que da sustento a sus procesos de negocio.

La información debe ser categorizada desde el punto de vista de sus requerimientos de seguridad (confidencialidad, integridad, disponibilidad) más criticidad, sensibilidad, secreto o privacidad, en conjunto con las regulaciones vigentes, sean éstas definidas por el Estado, la industria o la organización misma. Asimismo, los procesos de negocio deben ser categorizados en virtud del tipo de información que manejan, se concreten éstos a partir de aplicaciones informáticas o no.

Las actividades a desarrollar para cumplimentar este requerimiento pueden llevar un tiempo considerable, pero a partir de estas definiciones será posible adecuar los controles en función de los riesgos a enfrentar. Este análisis es el que hará la diferencia en el sistema a utilizar, haciéndolo tan riguroso como sea necesario.

Se podría pensar que esta metodología sólo es aplicable en organizaciones de gran tamaño. Sin embargo, si bien para las organizaciones de tamaño medio podría implicar un costo considerable de implementación, debido a que en general carecen de la formalidad necesaria para llevar a cabo estas actividades, evitarían gastos en la implementación de controles posiblemente innecesarios y obtendrían los beneficios de la efectividad al no omitir controles necesarios.

Es decir, que esta metodología permite implementar seguridad de la información donde realmente se justifica, ya que su ausencia pondría a la organización en una situación de riesgo cuya materialización podría provocar un impacto económico negativo.

A continuación reproduciremos un relato de una obra de Westerman y Hunter [16] que muestra claramente el impacto de los riesgos de TI en el negocio, pero que también permite ver las consecuencias que acarrea el accionar de los hombres de negocio que no ejercen su responsabilidad respecto de las decisiones tomadas por el personal de las TIC. Asimismo, traduciremos algunos párrafos que describen claramente la problemática.

La mencionada obra cuenta el caso de Comair, una subsidiaria de U$S 780 millones de Delta Air Lines que no pudo operar desde el 24 al 29 de diciembre de 2004 cuando falló el sistema de planificación de la tripulación. Este sistema es crítico debido a las regulaciones de la Federal Aviation Administration que dispone un límite de número de horas que cada miembro de la tripulación puede trabajar en un período de veinticuatro horas. El sistema mencionado es el que asegura el cumplimiento de dicha norma y si ese sistema no funciona, la aerolínea no vuela.

En el período de tiempo referido, debido a la necesidad de las aerolíneas de cancelar vuelos o replanificarlos por inusual mal tiempo, hubo muchísimo más trabajo que en otros años, de por sí más atareados por la fecha de la que se trataba.

Ninguno en Comair sabía que el sistema sólo podía administrar 32.000 cambios por mes. Al entrar un cambio más a la cifra indicada el sistema dejó de funcionar y fue necesario recargarlo nuevamente.

Por supuesto esto generó complicaciones importantes para los pasajeros, sobre todo en esa fecha, que las cámaras de televisión se encargaron de difundir al pueblo Norteamericano.

La compañía perdió U$S 20 millones sobre los u$s 25,7 millones de ganancias operativas del trimestre anterior.

Este incidente versa sobre la disponibilidad y se produjo a causa de un pequeño detalle en una aplicación informática. Un pequeño detalle que debió haber sido tomado en cuenta por las gerencias operativas, ya que son ellas las que realizan, o al menos debieran hacerlo, el análisis estadístico de sus operaciones.

Sin embargo, en esta desviación de su responsabilidad a la que hemos hecho referencia en el Capítulo I - UNA BREVE RESEÑA HISTÓRICA, en muchas ocasiones las gerencias operacionales dependen del personal de desarrollo para obtener la información que debiera ser de preocupación permanente de su gestión. Los analistas encargados de determinadas aplicaciones suelen conocer más sobre el comportamiento de los números operativos que los propios gerentes de esas áreas.

Es de destacar que, en este caso, un factor no relacionado con la seguridad de la información produjo un incidente de seguridad como es la falta de disponibilidad.

Vemos a partir de este ejemplo, cuán amplio es el espectro de los riesgos que debemos identificar. Y una vez más, podemos observar que la causa se encuentra en el negocio.

Westerman y Hunter explican:

> *"Los ejecutivos que, inteligentemente, invirtieron en TI como un arma estratégica simultáneamente incrementaron el riesgo de TI en sus empresas. Al depender más de TI para sus procesos críticos, su eficiencia competitiva y sus vínculos con clientes y proveedores, ellos incrementaron la dependencia de sus firmas del correcto funcionamiento de sus sistemas informáticos, así como también sus vulnerabilidades frente a amenazas externas.*
>
> *Muchos ejecutivos aún no han entendido la totalidad de las*

implicancias que esta situación genera. Para decirlo sin rodeos, la administración de riesgos de TI no puede seguir el ritmo de la realidad de los riesgos de TI. Éstos son aún manejados como una cuestión técnica y son ignorados por los ejecutivos de negocio. Aún cuando éstos entienden la importancia estratégica de TI para sus empresas, ellos aún no han podido o deseado asumir el fuerte compromiso necesario para administrar TI con efectividad."[13] [17]

Compartimos plenamente los conceptos de este trabajo ya que logra establecer claramente la importancia que tiene el involucramiento de los ejecutivos de negocio en las incumbencias de TI.

En otro de sus párrafos dice que muchos de los factores de riesgo corresponden a un inadecuado gobierno de TI, como por ejemplo:

1. Las actividades de TI de muchas organizaciones están motivadas, a través de las líneas de reportes y responsabilidades, a ser bien cercanas al negocio que sirven y responder a los requerimientos tan rápido como sea posible, en vez de pensar con visión empresarial sobre las decisiones de TI.
2. Sin la participación del negocio, los gerentes de TI pueden asumir incorrectamente cuáles son los riesgos que más preocupan al mismo.

A modo de conclusión expone:

"Tener un excelente personal de TI no es suficiente para controlar los riesgos de TI. Administrar los riesgos de TI requiere que todo el mundo involucrado piense de manera diferente. El CIO debe poner en claro a los ejecutivos de negocio cuáles son las consecuencias para el negocio y proveer un ambiente de toma de decisiones en el cual dichos ejecutivos puedan discutir y tomar decisiones sobre los riesgos de TI en términos del negocio. Los ejecutivos de negocio deben asegurar que el CIO haya implementado la administración de riesgos y debe participar activamente en las duras decisiones y cambios culturales que la administración de riesgos de TI

[13] La traducción es obra de la autora.

conlleva."

Y agrega:

"Porque el riesgo de TI ahora es el riesgo del negocio, con consecuencias para éste, las empresas deben cambiar la manera de gestionar dicho riesgo. Los negocios no pueden seguir pensando que los riesgos de TI van a estar contenidos entre las paredes del departamento de TI, o incluso dentro de la empresa. ***Ellos deben reemplazar los enfoques tecnológicos y puntos de vista fragmentados de los riesgos de TI por una visión integradora que comienza con el entendimiento de los riesgos de negocio y sus consecuencias que se derivan de las decisiones de TI."***[14] [18]

Este mismo concepto se aplica para los riesgos de la seguridad de la información. ISACA, en los contenidos que maneja la bibliografía propuesta en su certificación para la gestión de la seguridad de la información (CISM, por sus siglas en inglés), establece claramente que los riesgos de seguridad de la información deben ser integrados a la evaluación de riesgos del negocio en todo su alcance, es decir, desde los estratégicos hasta los operativos.

En resumen este capítulo ha mostrado el giro que realizó el enfoque de seguridad de la información. Mientras que en un principio se refería a la "aplicación de controles", actualmente define que éstos se aplicarán en función de la evaluación de riesgos que, además, debe estar integrada en la evaluación de riesgos del negocio.

[14] La traducción es obra de la autora. El formato "negrita" no corresponde a la obra original. Ha sido utilizado por la autora para destacar la frase.

Capítulo IV – ¿Cuál debiera ser el enfoque de los riesgos de seguridad de la información?

Como vimos en el capítulo anterior, la evolución de la gestión de la seguridad de la información siguió el mismo camino que la evolución de la gestión de negocios; comenzando con la formalización de controles a aplicar (buenas prácticas y el concepto de Control Interno) y posteriormente estableciendo la necesidad de generar e implementar dichos controles a partir de la evaluación de riesgos.

También vimos cómo la serie de normas ISO/IEC 27000[15] reflejaron estos principios.

Por su parte ISACA, en el marco del Gobierno Corporativo, hace referencia al Gobierno de la Seguridad de la información y al Gobierno de TI, todos los cuales involucran la gestión de riesgos.

Por lo tanto, el Gobierno de Seguridad de la Información es una disciplina enmarcada en el Gobierno Corporativo, y sus riesgos son evaluados en el marco de la Gestión de Riesgos del negocio, uno de cuyos aspectos serán los riesgos de seguridad de los activos tecnológicos. Es decir, que el enfoque excede el ámbito de las TIC.

Esta visión en conjunto con la desarrollada en el Capítulo II – LA INTEGRACIÓN COMO PARTE DE LA NUEVA VISIÓN, justifica la necesidad de que la gestión de seguridad de la información sea independiente de la gestión de las TIC, ya que su alcance es el tratamiento de la información en todos los procesos de negocio.

Ahora bien, veamos la definición de gestión de riesgo corporativo efectuada por el grupo COSO en su *Enterprise Risk Management* y el cubo que representa sus componentes, ya que éste es el punto de partida para el resto de marcos y normas sobre la materia.

---

[15] Así se denomina al conjunto de normas ISO/IEC que contiene las normas 27001, 27002, 27005 y otras.

La **Gestión del Riesgo Corporativo** es un proceso, efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, aplicado tanto en la definición de la estrategia como a través de toda la empresa, diseñado para identificar ***eventos potenciales*** que pueden afectar a la entidad y para gestionar el riesgo con el fin de mantenerlo dentro de su apetito de riesgo, para proporcionar un grado de seguridad razonable en cuando a la consecución de objetivos de la entidad.

Creemos que es clave el componente resaltado en la imagen, pues éste marca la diferencia entre el concepto tecnológico de la evaluación de riesgos sostenido históricamente por la seguridad de la información y el concepto más amplio y orientado al negocio que se pretende en la actualidad. Lamentablemente, el estándar ISO Guide 73:2009 [19], conserva una redacción confusa al respecto, afirmación que justificamos en los párrafos siguientes. A continuación la definición contenida en la guía.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Nota 1 - Un efecto es una desviación de lo esperado – positiva o negativa.

Nota 2 - Los objetivos pueden ser de diferentes aspectos (tales como financieros, salud, seguridad informática y ambientales) y pueden aplicar en diferentes niveles (tales como estratégico, transversales a la organización, proyectos, productos y procesos).

Nota 3-El riesgo es caracterizado en referencia a **potenciales eventos** y **consecuencias** o una combinación de ellos.

Nota 4- El riesgo de seguridad de la información es habitualmente

expresado en términos de una combinación de consecuencias de un **evento** de seguridad de la información y su posibilidad (likelihood) asociada de ocurrencia.

Nota 5- Incertidumbre es el estado, incluso parcial, de la deficiencia de información relativa a, entendimiento o conocimiento de un evento, sus consecuencias o posibilidad de ocurrencia.

Nota 6– El riesgo de seguridad de la información está asociado con la posibilidad de que una amenaza puede explotar una vulnerabilidad de un bien o grupo de bienes informáticos y, en consecuencia causar daño a la organización.

Como podemos observar, si bien en la Nota 4 considera para el riesgo de seguridad de la información la existencia de eventos, en la Nota 6 parece restringir el mencionado riesgo a la "posibilidad de que una amenaza puede explotar una vulnerabilidad de un bien o grupo de bienes informáticos y, en consecuencia causar daño a la organización". Definición ésta ampliamente usada en las prácticas de gestión de seguridad de la información y extendida exclusivamente al ámbito de las TIC.

Sin embargo, el estándar ISO/IEC 27005 hace referencia a la ocurrencia de eventos en el desarrollo del proceso, aunque no siempre utilice dicho término. Por ejemplo:

- Refiriéndose al propósito de la identificación de riesgo, punto 8.2.1.1., expresa que se debe determinar qué puede pasar para que suceda una pérdida, profundizando el cómo, dónde y porqué.
- En el punto 8.2.1.3., refiriéndose a la identificación de amenazas, indica la necesidad de obtener información sobre ellas, a partir de la revisión de incidentes (recordemos que este término se relaciona con evento).
- En el punto 8.2.1.5., cuando refiriéndose a la identificación de vulnerabilidades de los bienes/activos[16], expresa que pueden ser identificadas en las siguientes áreas: la organización, procesos y procedimientos, rutinas de gestión, personal, entorno físico, configuración

[16] Traducción de "asset".

de los sistemas, hardware, software y equipamiento de comunicaciones y la dependencia de partes externas.

Más aún, cuando se refiere a la necesidad de que la organización defina el alcance y límites de la gestión de riesgos de seguridad de la información, formula que se debe considerar entre otros, las políticas, las estrategias y los objetivos de negocio de la organización, los procesos de negocio, las estructuras y funciones de la organización, los requerimientos legales, regulatorios y contractuales aplicables a la organización, la política de seguridad, el enfoque general de la gestión de riesgos de la organización y los bienes/activos informáticos. Cuestiones todas que distan mucho de ser "tecnológicas".

Además, el estándar define que un bien/activo es cualquier cosa que tiene valor para la organización y que, en consecuencia, requiere protección. **Y agrega que, para la identificación de dichos bienes se debe tener en mente que un sistema de información consiste en algo más que hardware y software.**

Por lo tanto, queda claro que el estándar extiende la gestión de riesgos de seguridad de la información a la identificación de potenciales eventos en el ámbito de toda la organización.

Paulatinamente y sobre todo en las últimas dos décadas, la visión tecnológica ha ido mutando a la visión organizacional.

Un claro ejemplo de la evolución en la evaluación de riesgos desde las TIC hacia el negocio, es el proceso de DRP, siglas de los términos en inglés de la Recuperación ante Desastres (Disaster Recovery Plan), el cual terminó conformando en conjunto con otros procesos, el de Continuidad del Negocio, ya que no solamente se encuentran involucradas las TIC sino toda la organización.

Éste es un concepto en el que se hace mucho foco debido a que las mayores pérdidas son ocasionadas por la materialización del riesgo de “discontinuidad operativa”. Es justamente ésta la razón por la cual es necesario evaluar los riesgos en todos los procesos. Tomemos como ejemplo el caso de la compañía Comair presentado en el capítulo anterior, en el que se produjo un incidente de discontinuidad por causas que nada

tienen que ver con un ciberataque o una amenaza a la seguridad física de un centro de procesamiento.

Ejemplos sobre falta de control, definición errónea de procesos, etc. pueden encontrarse muchos: "*… una oficina de Ernst & Young envió un paquete conteniendo un dispositivo flash que almacenaba información sobre los planes de retiro de 401k empleados. La información, que incluía nombres y números del seguro social estaba cifrada, pero la oficina envió la clave de cifrado en el mismo sobre…*". [20] El paquete fue robado. Es incuestionable que el error no tiene nada que ver con lo tecnológico, sino con el diseño de procesos y la falta de capacitación del personal. Sin embargo, generó un incidente de seguridad de la información.

Por otro lado, existen otros hechos que pueden generar un gran volumen de pérdidas, como por ejemplo el fraude en el ámbito bancario, el cual tiene que ver fundamentalmente con la adecuada definición, construcción y prueba de las aplicaciones informáticas, así como con los permisos que se otorgan y el proceder de las personas, en especial en los ataques de ingeniería social.

En un documento [21] muy interesante se presenta un ejercicio realizado entre directores de varias compañías donde se plantea cinco áreas de riesgo entre las que se considera, entre otros más cercanos a la operatoria de las TIC, los riesgos de la información. En este caso, indican los autores con ironía luego de estudiar los resultados, que los directores están satisfechos sólo con contar con políticas de privacidad apropiadas, acordes con la ley y, lo más importante, con un oficial de privacidad que tenga el suficiente tiempo, conocimiento y autoridad para llevar adelante esas políticas destinadas a prevenir las brechas o sus catastróficas consecuencias. Mostrando así la falta de conciencia de estos responsables respecto de las verdaderas causas de los riesgos de la información.

El mismo documento expone las cuantiosas pérdidas ocasionadas por brechas en la seguridad de la información: "*… subraya la importancia de las inversiones en IT, señalando que las compañías norteamericanas gastan tanto en tecnología de la información cada año como en sus oficinas, depósitos, y fábricas. Como resultado de estas importantes inversiones, las*

consecuencias de cualquier desastre son propensas a ser profundas y duraderas." En otro apartado indica "*… las firmas que experimentaron infracciones de seguridad de Internet, subsecuentemente perdieron un promedio de 2,1% de su valor de mercado en dos días, resultando en una pérdida de capitalización bursátil de más de 1,6 billones de dólares cada una. TJX vio una caída inicial a corto plazo de 1,7% en el precio de sus acciones el día 30 de Enero (2007), 12 días después de que sus infracciones de seguridad fueran anunciadas. Sus acciones experimentaron una caída de 3,6% dos días después en respuesta a una demanda promovida por una clase de acciones y un llamado a la Comisión Federal de Comercio para investigar a TJX por posible negligencia. Mientras que el valor de sus acciones eventualmente se recuperó, y ha llegado a superar al de sus competidores, esto sólo ocurrió luego de una extensa y costosa campaña publicitaria que consumió tiempo y atención de la Gerencia, que pudo haber sido utilizada en mejorar el curso del negocio.*"

De lo antedicho es posible inferir que, si bien las mayores pérdidas se producirán frente a la discontinuidad de las operaciones, una organización puede sufrir cuantiosas pérdidas por brechas de seguridad de la información sin que ello afecte la continuidad del negocio.

También se deduce que no sólo la identificación de las amenazas y vulnerabilidades de los activos tecnológicos permiten identificar, evaluar y posteriormente tratar los riesgos de seguridad de la información. Debemos incluir en dicha evaluación todos los procesos además del accionar humano, eslabón más débil de la cadena.

De hecho, el alcance de los controles establecidos por el estándar ISO/IEC 27002 excede lo tecnológico ya que existen capítulos referidos a la organización, los recursos humanos, el cumplimiento de regulaciones, etc.

El estándar NIST SP800-30 revisión 1 [22], actualización publicada en 2012, es mucho más clara aún y presenta una visión muy diferente a la del estándar original, utilizando el enfoque de eventos y los aspectos organizacionales. Mientras que en su versión original definía la amenaza como la posibilidad de que una fuente de amenaza explotara accidental o intencionalmente una vulnerabilidad específica, en la revisión la define como

cualquier circunstancia o evento con la posibilidad de impactar adversamente en las operaciones organizacionales y bienes, individuos, otras organizaciones o la Nación a través de sistemas de información mediante accesos no autorizados, destrucción, revelación o modificación de información, así como también la denegación de servicios.

Respecto de las vulnerabilidades establece que no sólo se encuentran en los sistemas de información ya que viendo estos sistemas en un contexto más amplio, las vulnerabilidades pueden encontrarse en las estructuras del gobierno organizacional (ej. la falta de efectivas estrategias de gestión de riesgos y de adecuados marcos de riesgos, pobre comunicación entre agencias, decisiones inconsistentes sobre la prioridad relativa de funciones de negocio). También pueden encontrarse en relaciones externas (ej. dependencia de fuentes de energía particulares, cadena de suministros, tecnologías de información y proveedores de telecomunicaciones); en procesos de negocio (ej. procesos pobremente definidos o que no tienen en cuenta el riesgo); y arquitecturas de seguridad de la organización/información (ej. pobres decisiones sobre la arquitectura resultando en falta de resiliencia de los sistemas de información organizacionales). Es posible consultar las definiciones completas en Ref. NIST.

Asimismo, más allá de lo económico, existen los riesgos de incumplimiento de las regulaciones y pérdida de reputación e imagen, entre otros. Los requerimientos de la Ley SOX[17] han obligado a las organizaciones que deben cumplir con ella, a enormes esfuerzos de adaptación de sus procesos.

Es importante señalar en este punto, que la demora en el desarrollo de este trabajo (comenzó a fines de 2011), debido a circunstancias que no viene al caso enumerar, ha derivado en una disminución de su característica

[17] Sarbanes-Oxley Act of 2002, 30 de julio de 2002. Es una ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. Nace con el fin de monitorear a las empresas que cotizan en la bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor. Más allá del ámbito nacional, involucra a todas las empresas que cotizan en la Bolsa de Valores de Nueva York, así como a sus filiales.

innovadora, ya que los estándares de manera natural devinieron en nuestros dichos.

Para mostrar esta situación, a continuación incluimos parte de un trabajo del BSI [23] donde se realiza una comparación entre la primera versión del estándar ISO/IEC 27001 y su revisión de 2013.

Concepto nuevo o actualizado	**Explicación**
Evaluación de riesgos	La identificación de activos, amenazas y vulnerabilidad ya no son un prerrequisito para la identificación de riesgos de seguridad de la información(*)
Dueño del riesgo	Reemplaza al dueño del activo
Plan de tratamiento del riesgo	Se considera más importante la eficacia del plan de tratamiento de riesgos que la eficacia de los controles
Controles	Son determinados durante el proceso de tratamiento de riesgo, en vez de ser seleccionados del Anexo A

(*) Esto es precisamente lo que nosotros sostenemos en este trabajo. Debemos remitirnos a las definiciones del marco COSO ERM, referenciadas por el estándar ISO 31:000 [23].

El autor del libro sobre el que está basada esta guía, David Brewer, PhD, FBCS, fue uno de los desarrolladores del estándar SGSI original, el BS7799-2:2002.

Brewer también señala que el estándar ISO/IEC 27005 se encuentra en proceso de revisión y cabe destacar que el estándar ISO/IEC 27001:2013 en su contenido y respecto de riesgos, sólo referencia el estándar ISO 31000:2009 [24].

Capítulo V – Mecanismos/Herramientas utilizados en la Evaluación de un Sistema de Gestión

Sin lugar a dudas, las organizaciones comprendieron la necesidad de contar con herramientas que les permitieran medir el desempeño en el logro de sus objetivos, habiendo comenzado a dar forma a las mismas durante el último cuarto del siglo pasado.

Visualizando el tema desde la óptica de la organización como un todo, es posible ver que desde finales de la década del 70, las organizaciones han avanzado en el uso de indicadores diferentes a los financieros para medir el resultado de su estrategia y/o gestión. Así es como han sido desarrollados métodos que tienden a lograr un conjunto de indicadores que permiten evaluar otros componentes de las organizaciones, tales como la satisfacción del cliente, el cumplimiento de los proveedores, los procesos internos, el cumplimiento de regulaciones, etc. El profesor Robert S. Kaplan de la Harvard Business School y Dr. David P. Norton del Nolan Norton Institute desarrollaron un proyecto de investigación que dio lugar a uno de los instrumentos de mayor interés en la década del ’90: el balanced scorecard o cuadro de mando integral. [25]

Gráfica del cuadro de mando integral

Otra corriente de pensamiento se orientó hacia la calidad de procesos estableciendo los principios que luego de varias revisiones han definido los modelos que rigen en nuestros días. A continuación analizaremos algunos de ellos.

Serie de estándares ISO 9000

Después de la II Guerra Mundial las inspecciones y controles desarrollados por el Reino Unido durante la misma en virtud de las necesidades que surgieron, forman parte del incipiente concepto de "calidad". "*Para entonces el término "calidad" se asocia a "conformidad" más que a "mejora" – o sea por inspección se verifica la conformidad contra los controles y requerimientos.*".

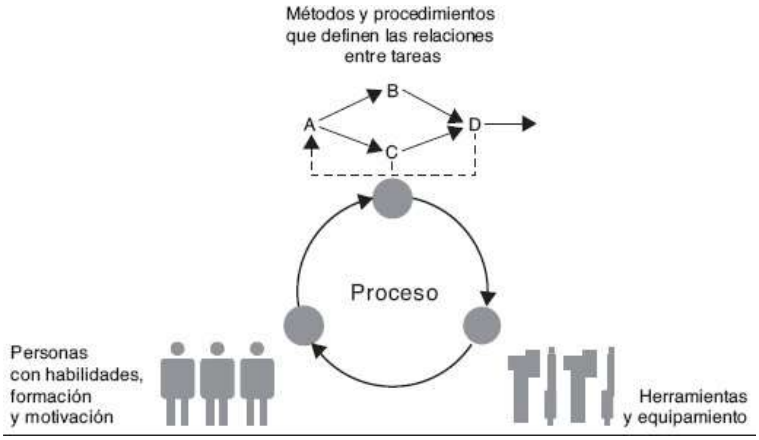
Posteriormente se avanza en conceptos de "sistemas" y "procesos" hasta llegar al de "aseguramiento de la calidad". También comienzan a participar diferentes sectores como el de energía y a extenderse por otros países como USA, Canadá y de Europa. En 1974 se publicó una normativa para Aseguramiento de la Calidad (Guías): BS5179 y en 1979, producto de un acuerdo, se publica en el Reino Unido, la BS5750 (precursora de ISO 9000). [26]

En 1987 se publicó la serie ISO 9000 y fue evolucionando hasta la ISO 9000:2000, las cuales "*son reestructuradas según un modelo de proceso de negocios que representa de forma más precisa el modo en el que las organizaciones operan realmente, en comparación con la anterior estructura lineal de 20 requisitos de las normas de 1994. La base de esta nueva estructura está compuesta por cuatro nuevas cláusulas principales: Responsabilidad de la Dirección, Gestión de los Recursos, Realización del Producto y Medición, Análisis y Mejora; la definición del ciclo PLANEAR-HACER-VERIFICAR-ACTUAR como parte integral y la definición de "Calidad" como cumplir con las necesidades y expectativas del cliente.*" [27]

Modelo de Capacidad y Madurez

Según el Software Engineering Institute (SEI), existen tres dimensiones críticas en las que las organizaciones se focalizan: las

personas, los procedimientos y los métodos, y las herramientas y equipamiento. Sin embargo, afirma que lo que sustenta todo el conjunto son los procesos, ya que ellos son los que permiten alinear las actividades proporcionando la infraestructura necesaria para hacer frente a un mundo en constante evolución, maximizar la productividad de las personas y utilizar la tecnología para crecer en competitividad [28].



Tres dimensiones críticas – Fuente: Software Engineering Institute (SEI)

"¿Que es lo que mantiene a todo unido? Los procesos usados en la organización. Los procesos permiten alinear la manera en la que se hacen los negocios. Permiten escalar y proveer una manera de incorporar conocimiento, de optimizar los recursos y de examinar las tendencias del negocio. Esto no significa que las personas y la tecnología no son importantes. Vivimos en un mundo donde la tecnología está cambiando a una velocidad increíble. Asimismo, la gente trabaja en muchas compañías durante sus carreras. Vivimos en un mundo dinámico. Focalizarse en los procesos provee la infraestructura y estabilidad necesarias para tratar con el siempre cambiante mundo, maximizar la productividad de la gente y el uso de la tecnología para ser competitivo" [29]

Del lado de la calidad encontramos los conceptos desarrollados por Phillip Crosby [1979], W. Edwards Deming [1986], Joseph Juran [1988] y Watts Humphrey[1989] (éste último para el SEI),los que se resumen en el siguiente principio: "*la calidad de un sistema o de un producto está muy influenciada por la calidad del proceso empleado para desarrollarlo y mantenerlo*". Basado en estos principios, el SEI (a partir de 1986) desarrolla

los Modelos de Capacidad y Madurez *(CMM- Capacity Maturity Model)*, luego devenidos en *CMMI - Capacity Maturity Model Integration*, los cuales se integran definitivamente en la versión 1.3. (2010). (Ver Anexo II – ALGUNOS MODELOS)

Los CMMI proponen dos caminos para la mejora de procesos: el modelo de capacidad, y el modelo de madurez.

La diferencia más importante entre ambos es que el **modelo de capacidad** puede ser usado para la mejora de un área de proceso[18] individual o un conjunto de ellas. La organización puede seleccionar la que desea mejorar y sólo estará limitada por la interdependencia con otras áreas de proceso.

Mientras tanto, el **modelo de madurez** define que cada nivel será alcanzado cuando se mejoren las áreas de proceso pertenecientes a un subconjunto previamente establecido para ese nivel.

El **modelo de madurez** usa los niveles para caracterizar el estado general de los procesos organizacionales como un todo, mientras que el de capacidad usa los niveles para caracterizar el estado de los procesos organizacionales relativos a un área de proceso o un grupo de ellas.

Es por ello que el modelo de capacidad no es adecuado para comparar la madurez de organizaciones diferentes, dentro de las actividades previstas por el modelo, respecto de la mejora de procesos.

Estándar ISO/IEC 15504

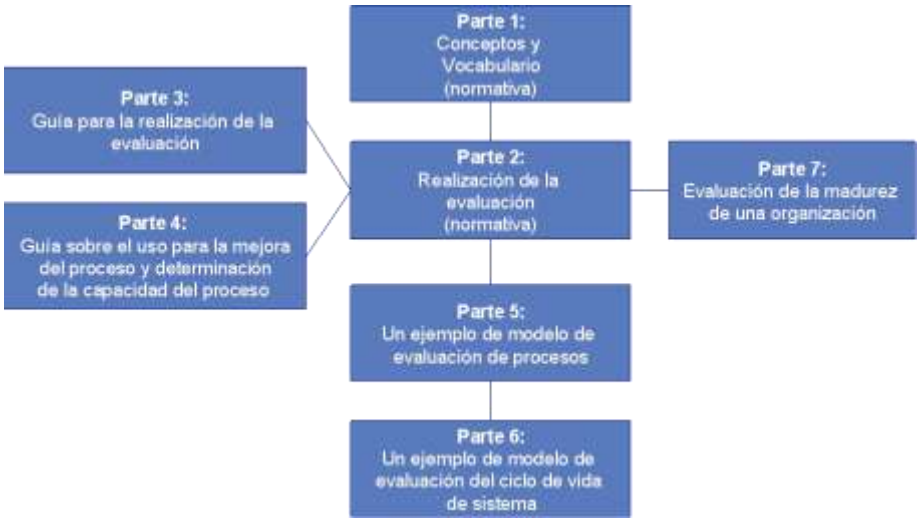
En virtud de las consultas realizadas en la Web, se ha podido apreciar que el método de evaluación de los modelos de la mejora de procesos referentes en el mercado son: el *Standard CMMI Appraisal Method for Process Improvement (SCAMPI)*, método oficial usado para evaluar los procesos organizacionales y proveer calificación, e ISO/IEC 15504 [30], también conocido por la abreviatura *SPICE (Software Process Improvement*

[18] "Área de proceso": conjunto de prácticas relacionadas en un área (no se utiliza el término como funcional) tal que, cuando son implementadas colectivamente, satisfacen un conjunto de metas consideradas importantes para mejorar dicha área. Se podría interpretar que el área de proceso es un proceso transversal en el que pueden encontrarse involucradas varias áreas funcionales.

Capability Determination) o Determinación de la Capacidad de Mejora del Proceso de Software, en castellano, el cual es el título de la parte 2 del estándar. El primero es un estándar de facto y está más difundido, pero el segundo tiene la ventaja de ser un estándar internacional. Cabe señalar que la ISO/IEC 15504, fue enmendada en el año 2004 reemplazando el concepto de "proceso de software" por el de "tecnología de información", extendiendo así su alcance.

Es posible encontrar comparaciones entre estos dos modelos, si bien no son expuestas aquí porque no constituyen un objetivo de este trabajo.

"*A diferencia del estándar ISO/IEC 15504 que hasta el momento sólo evaluaba los procesos, o niveles de capacidad, el modelo CMMI incorpora desde hace tiempo la evaluación por niveles de madurez, permitiendo dar una "puntuación" a la organización. Pero como consecuencia de la necesidad transmitida por la industria del software en la mejora de la calidad basada en niveles de madurez y con el fin de crear una certificación internacional a nivel de organización, ISO ha desarrollado la parte 7 - Evaluación de Madurez de una Organización, la cual ha sido publicada en 2008.*" [31]



Fuente: Kybele Consulting - Estructura de la ISO 15504

Cabe señalar que el estándar de referencia ha incorporado 3 partes adicionales, que están orientadas a temas específicos.

Hasta aquí hemos hecho referencia a modelos genéricos que pueden

ser aplicados a la gestión de cualquier tipo de organización y proceso.

A continuación mostraremos los relacionados a la gestión de la seguridad de la información.

Estándar ISO/IEC 21827:2008

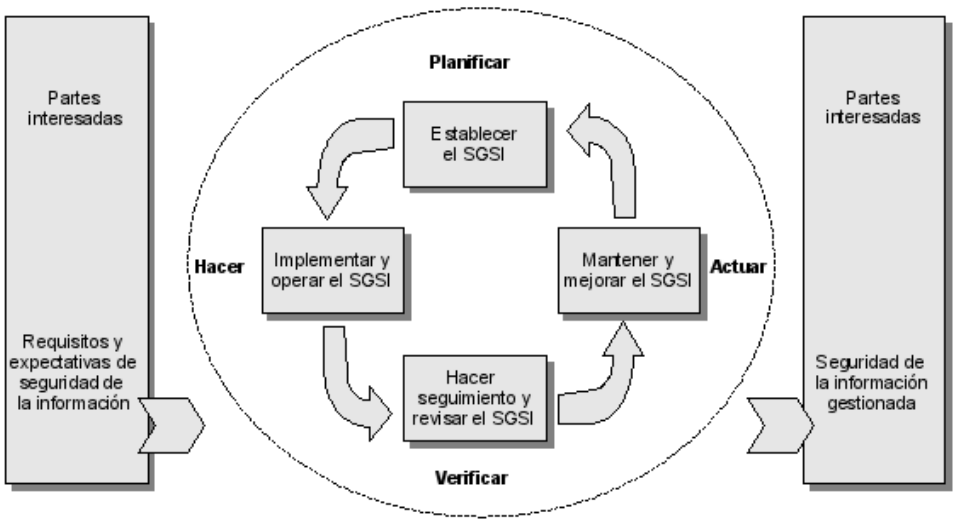
Formaliza el *Systems Security Engineering - Capability Maturity Model® (SSE-CMM)* como estándar internacional.

Claramente este modelo es de capacidad, confirmándolo al ofrecer un cuadro donde muestra su alineación con el estándar ISO/IEC 15504-2.

El SSE-CMM no está totalmente integrado con los CMMI, ya que fue diseñado previamente a la integración. Por otra parte, está orientado específicamente a los aspectos técnicos, incluyendo áreas de procesos de ingeniería. (Ver Anexo II – ALGUNOS MODELOS).

Estándar ISO/IEC 27001

En octubre de 2005 a través del estándar ISO/IEC 27001, actualizada en 2013, se presenta el Sistema de Gestión de Seguridad de la Información construido también con un enfoque de procesos y con el criterio de mejora continua utilizando el ciclo PLANIFICAR-HACER-VERIFICAR-ACTUAR (PDCA).



Cabe señalar que si bien la versión 2013 no especifica que el modelo es PDCA, como consecuencia de la necesidad de mantener homogeneidad

con otros sistemas de gestión normados por ISO, el desarrollo del proceso normado sigue este modelo. Basta para demostrarlo, decir que algunos de sus capítulos son: 6. Planificación, 8. Operación, 9. Monitoreo y revisión y 10. Mejora.

Relación entre los estándares ISO/IEC 27001, ISO 9001 y el modelo CMMI

El estándar ISO/IEC 27001 está alineado con el estándar ISO 9001, *Quality management systems - Requirements*, al igual que con el estándar ISO 14001:2004, *Environmental management systems – Requirements*, "*… con el fin de dar soporte consistente y permitir una implementación y operación integrada con estándares de gestión relacionados*" [32]. Es decir, está pensada como un modelo de mejora continua de gestión de la calidad de los procesos. Es importante señalar que el estándar ISO 9001 no propone un mecanismo para la medición de la madurez de los procesos sino que establece, bajo el título "Mejora continua" que "*La organización debe mejorar continuamente la eficacia del sistema de gestión de la calidad mediante el uso de la política de la calidad, los objetivos de la calidad, los resultados de las auditorías, el análisis de los datos, las acciones correctivas y preventivas y la revisión por la dirección.*" [33]

Si bien el modelo CMMI se desarrolla sobre los principios enunciados por los maestros en gestión de la calidad y su mejora continua, los cuales también dan soporte teórico al estándar ISO 9001, agrega una serie de metas y prácticas asociadas a una escala de valores que indica los diferentes niveles que los procesos y la organización deben cumplimentar, para mejorar la calidad y conseguir efectividad en el logro de sus objetivos. Es decir que establece una guía para determinar la calidad del proceso.

Algunos autores consideran como desventaja del estándar ISO 9001:2000 su característica de modelo genérico, a causa de lo cual hay pocas directrices para su implementación en algunas industrias o campos específicos En tanto otros estiman que el modelo CMMI es de dificultosa implementación para algunas organizaciones por ser riguroso y detallado [34].

Cabe señalar que ambos modelos hacen la salvedad respecto a la necesidad de adaptar los principios a la estructura y dimensión de la organización en la que se van a implementar.

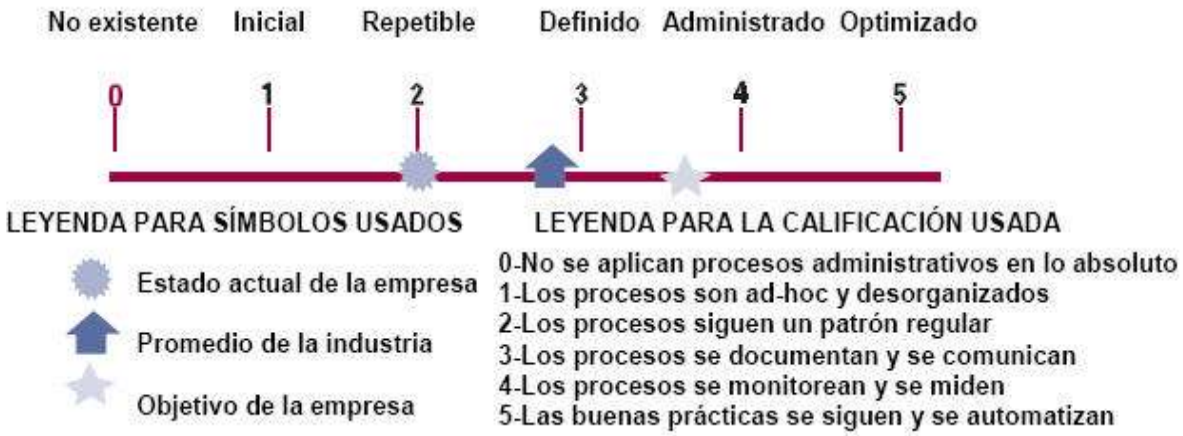
En este capítulo hemos tratado de mostrar los esfuerzos realizados para definir mecanismos de evaluación de los sistemas de gestión. Como conclusión, podemos apreciar que desde múltiples visiones, se avanzó sobre el desarrollo de herramientas o mecanismos que permitieran que directivos y partes interesadas (stakeholders) pudieran conocer el estado de situación, ya sea de los procesos o de la organización toda.

Dado que, tal como mostramos en los capítulos precedentes, la seguridad de la información se plantea como un sistema de gestión, es necesario aplicar para su evaluación alguno de los mecanismos expuestos. En el capítulo siguiente desarrollamos esta idea y seleccionamos el modelo a utilizar.

Capítulo VI – ¿Qué es EL “modelo de madurez” y por qué usarlo?

La escala de valores asociada a los modelos CMMI fue rápidamente aplicada por las organizaciones, asociaciones profesionales y consultoras para la evaluación de la gestión de cualquier proceso u organización, estableciendo los requerimientos que creyeron necesarios para cumplimentar cada nivel. También en conjunto con esta escala se popularizó el uso de la expresión “modelo de madurez” para referirse a la misma.

Por ejemplo, CobiT utiliza hasta la versión 4.1 la siguiente guía de evaluación de procesos de tecnologías de información, que denomina **modelo de madurez**, si bien se asemeja más al **modelo de capacidad** del SEI ya que mide cada proceso.



Una curiosidad a señalar es que la escala de 0-5 no existe para el CMMI. Éste utiliza la escala del 1-5 para el modelo de madurez, y la de 0-3 para el modelo de capacidad. Lo más significativo es que no utiliza el nivel 0 en su escala de madurez, y explica claramente la razón por la cual no debe ser usado. En cambio, como podemos ver en este ejemplo, el nivel 0 es usado como parte de la escala de madurez. Como se puede observar, Cobit adaptó el modelo según su propia iniciativa.

Otro ejemplo que podemos tomar es el de Gartner[19], que utiliza un

[19] Gartner, Inc. es una compañía internacional abocada a la investigación y consultoría en tecnologías de información.

modelo de madurez ad-hoc para evaluar la madurez de la organizaciones respecto del programa de seguridad de la información definiendo los consabidos seis niveles (0-5) utilizados por la mayoría, tal como se muestra a continuación [35].

Descripción de los niveles de madurez

Nivel 0 – *Inexistente*: No existen actividades de seguridad formalizadas. Lo controles implementados son ad hoc. Las tareas se realizan informalmente y sin coordinación alguna, los procesos no están definidos y los cambios de personal producen fallas.

Nivel 1 – *Inicial*: Los procesos de seguridad son ad hoc, desconectados entre si y desorganizados. Existen algunos individuos dedicados, pero no existen programas formales. Existe una limitada, aunque creciente, concientización y la aceptación a través de la organización de la necesidad de un programa formal.

Nivel 2 – *En desarrollo*: Se encuentra definida una visión y se asegura por medio de un programa formal. Se evalúan los requerimientos, se asignan las responsabilidades y se inicia la implementación del plan. Se identifican las brechas y los programas de comunicación y educación se desarrollan a través de toda la organización.

Nivel 3 – *Definido*: Las metas, prácticas y métricas de desempeño están totalmente definidas; los procesos han sido estandarizados, integrados, documentados e implementados y un modelo de gobierno y cumplimiento se está llevando a cabo.

Nivel 4 – *Gestionado*: El programa es parte de la cultura y es un parte integral e inseparable de las operaciones y las decisiones. El desempeño es fuertemente predecible.

Nivel 5 – *Optimizado*: **Los procesos son completamente maduros**. **Todas las inversiones y decisiones están relacionadas**. Los comentarios o sugerencias de los interesados son usados para ajustar y mejorar continuamente los procesos a medida que los requerimientos de la gente, la tecnología y los negocios van cambiando y aparecen las oportunidades.

Nuevamente encontramos definiciones generalistas muy difíciles de evaluar. ¿Cómo se lleva a la práctica las premisas enunciadas por Gartner? ¿Qué quiere decir que “todos los procesos son completamente maduros”, o

que "todas las inversiones están relacionadas con las decisiones”?. Son expresiones muy interesantes para un manifiesto, tal vez incluso para redactar políticas. Pero ¿cuáles son las acciones que debe encarar un gerente para concretarlas? Seguramente detrás de estos enunciados existen documentos con mayores precisiones y cursos de entrenamiento así como horas de consultoría en apoyo a su implementación.

En conclusión, analizando los modelos tomados como ejemplo entre tantos otros que es posible encontrar, podemos apreciar que se han utilizado algunos términos y características de los modelos CMMI, pero de una manera absolutamente discrecional y con muy poca, más precisamente casi ninguna, rigurosidad. Podríamos decir sin equivocarnos que dichos modelos sólo fueron una fuente inspiradora para una escala de medición.

Con este criterio, para definir un modelo de madurez basta con describir formalmente los procesos y las condiciones que deben cumplir para transitar los 6 niveles.

Con esta misma actitud de arbitrariedad, han utilizado indistintamente los conceptos madurez y capacidad, cuando para los CMMI estos son dos modelos claramente diferentes y la evaluación de los mismos tiene directivas muy precisas, tal vez hasta rígidas.

Para mostrar cuánto de cierto hay en lo expresado previamente, podemos decir que cuando ISACA presenta el marco COBIT5, finalmente decide usar el estándar ISO/IEC 15504 parte 2. O sea, en principio blanquea que el modelo que usa es de capacidad y no de madurez, como expresaba en su versión 4.1; y por otro lado, se aleja de los requerimientos generalistas planteados según su criterio discrecional, para tomar rigurosas premisas de una norma de aplicación internacional.

Entonces, teniendo en cuenta este análisis, conviene dar una mirada a los modelos CMMI. El estudio profundo de los mismos permite entender su alcance tanto respecto de la definición de los niveles (de capacidad por un lado y de madurez por otro) como de su estructura, compuesta por áreas de proceso, metas y prácticas genéricas y metas y prácticas específicas. (Ver Anexo III – BREVE DESCRIPCIÓN DE LOS CMMI, SUS COMPONENTES Y CARACTERÍSTICAS).

Los modelos CMMI son sumamente minuciosos y estructurados y, además, aportan una guía práctica con ejemplos muy valiosos. Asimismo, si los mencionados alcance y estructura son adaptados según el criterio de la organización, es posible aplicarlos en cualquier ámbito.

Es pertinente recordar, como ya dijimos en el Capítulo V – MECANISMOS/HERRAMIENTAS UTILIZADOS EN LA EVALUACIÓN DE UN SISTEMA DE GESTIÓN, que estos modelos rescatan el valor de los procesos como el elemento que hace de integrador de las dimensiones críticas de una organización (procesos, personas y tecnología), según el SEI.

En este sentido y teniendo en cuenta el documento de Gartner mencionado previamente es importante destacar un trabajo llevado a cabo en el encuentro denominado *"The Gartner Security Summit"* in Washington D.C. en 2008, donde los participantes evaluaron la madurez de sus programas con una herramienta provista por la consultora. Dicha herramienta permitía evaluar nueve (9) dominios del programa de seguridad, siendo uno de ellos la Gestión de los Procesos de Seguridad. En el análisis de los resultados, la consultora resalta que entre los dominios evaluados, algunos de los cuales lograron niveles de 2,5, llama la atención el bajo nivel que mostró el mencionado dominio, ya que sólo alcanzó el valor 1. Dice Scholtz que es impactante el bajo desempeño de la gestión de procesos. Y agrega: la madurez del programa de seguridad es esencialmente una función de la madurez de los procesos sobre los que se soporta; ignorar la madurez de los procesos, tratando de mejorar la madurez del programa es un atajo que no funciona.

Desafortunadamente, continúa Scholtz, muchas organizaciones han implementado principalmente controles tecnológicos, así como contratado los recursos humanos necesarios para manejarlos, pero ignoran los aspectos humanos de la seguridad, y **no entienden los requerimientos del negocio sobre la gestión de la seguridad**.

Compartimos plenamente los conceptos expresados por Scholtz y consideramos que la implementación del SGSI según el estándar ISO/IEC 27001 es una parte del camino a recorrer, pero que dado que utiliza

conceptos muy genéricos puede ser interpretada de muchas maneras. Por lo cual, más allá de que una organización pueda certificar procesos específicos bajo el estándar, ello no permite medirla como un todo respecto de la seguridad de la información.

En este orden de cosas, y teniendo en cuenta su valor estratégico surge como requerimiento muy importante definir un criterio para realizar dicha medición. Estableciendo dicho criterio y un método de evaluación, no sólo podremos afirmar que una organización es madura según esas variables, sino también comparar varias organizaciones respecto de las mismas.

Hemos encontrado criterios enfocados hacia el concepto de que la madurez se consigue a través de la implementación de las buenas prácticas "in crescendo". Por ejemplo, el artículo "*¿Cómo Puede Medirse la Seguridad?*" [36], expresa que la madurez está dada por la existencia de todos los controles del estándar ISO/IEC 27002 aplicados cada vez en un porcentaje mayor.

Claramente este criterio no tiene en cuenta la evaluación de riesgos ni el enfoque de procesos, previstos por las normas y además, en función de los análisis previos, podría no ser aplicable la totalidad de los controles.

Volviendo al documento de Gartner previamente mencionado, es interesante analizar el criterio que utiliza para establecer la madurez del programa de seguridad de la información, enmarcado en el programa de riesgos de las TIC. Éste establece que una vez alcanzado el nivel 3, "Definido" (ver la definición más arriba), la organización puede comenzar su programa estratégico de seguridad de la información "*(algunas veces referido como la implementación de un sistema de gestión de seguridad de la información, tal como el definido en el estándar ISO/IEC 27001)*".

Para que una organización pueda evaluar el programa de seguridad de información que está llevando a cabo, Gartner propone utilizar la guía que se detalla a continuación, a partir de una serie de preguntas de selección múltiple que realiza por cada punto.

- Gobierno

- Planeamiento estratégico
- Planeamiento táctico y presupuesto
- Organización
- Marco de controles
- Arquitectura de seguridad
- Gestión de procesos de seguridad
- Comunicación y concientización
- Respuesta a incidentes

Las preguntas concernientes al ítem gestión de procesos de seguridad, que es el tópico en el cual las empresas alcanzaron un nivel 1, son:

1. ¿Hay un catálogo de procesos documentado de los procesos estratégicos y tácticos relacionados con el programa (de seguridad de la información), asociado a sus dueños?
2. Los procesos relacionados con el programa, ¿están en su lugar, totalmente documentados y soportando las metas del programa de gestión de riesgos?
3. ¿Han conducido un análisis de brecha (gap) para determinar la madurez de los procesos relacionados con el programa? En este caso, brinda como una de las respuestas a seleccionar, su propio marco de evaluación de madurez o CMMI.
4. ¿Tienen un método de formalización de procesos estándar, incluyendo la creación, modificación y “retiro del servicio” (inhabilitación, quitar de vigencia) un proceso?
5. ¿Han definido un conjunto de métricas que es reportado a la gerencia para validar adherencia a los sus controles?

Si las leemos atentamente veremos que el alcance de la gestión de procesos es muy amplio, pero para nuestro propósito la pregunta 3 es clave. En lo que se refiere a madurez del proceso, Gartner propone como opción usar su modelo ad-hoc de evaluación de madurez o los CMMI. Es decir, que nos lleva a la fuente: CMMI.

Sin embargo, medir la madurez de los procesos sería adoptar el "modelo de capacidad" según el enfoque de los CMMI, mientras que el modelo de madurez provee una manera de evaluar el desempeño de una organización en su conjunto.

Para ello, los modelos CMMI definen las prácticas genéricas y las específicas relacionadas, que debieran ser implementadas para un subconjunto de áreas de proceso por cada nivel, ya que según expresan, la experiencia ha demostrado que las organizaciones dan lo mejor de ellas cuando focalizan sus esfuerzos de mejora de procesos en un número manejable de áreas de proceso por vez[20].

Una organización podría mejorar sus áreas de proceso en el orden que desee, tal como fue expuesto en el capítulo anterior respecto del modelo de capacidad, pero sólo tendrá un nivel de madurez específico si las áreas de proceso establecidas por el modelo para ese nivel, han sido desarrolladas de acuerdo con sus pautas.

Es importante considerar también que, además de que los modelos CMMI conforman la base sobre la que se construyó el resto, tal como ya hemos visto, son de acceso público.

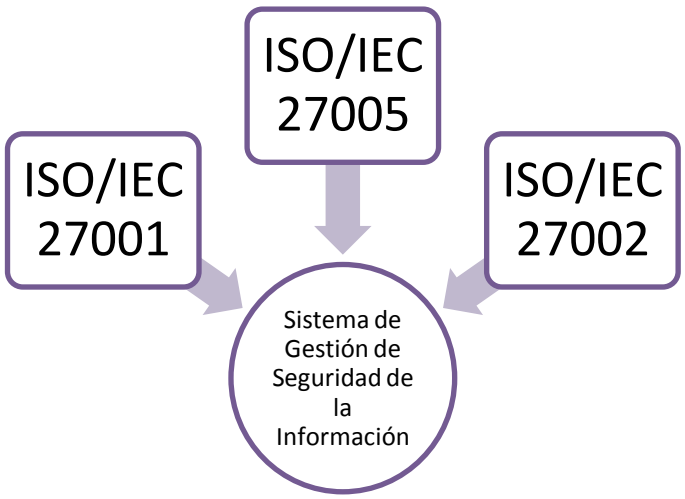
En conclusión, nosotros creemos que debemos medir la madurez de la organización respecto de la seguridad de la información utilizando el "modelo de madurez" establecido por los modelos CMMI, considerando la seguridad de la información integrada en todos los procesos de negocio.

[20] Los niveles del modelo de madurez y las áreas de proceso que deben ser implementadas para cumplimentar el nivel se muestran en la tabla de págs. 47 a 51.

CAPITULO VII - Pero…. ¿Qué debemos evaluar? Y ¿Con qué herramienta?

El estándar ISO/IEC 27001 en su ítem 4.2.1 - Establecer el SGSI, dispone que la organización debe definir un enfoque de evaluación de riesgos (4.2.1.c a 4.2.1.f) y seleccionar los objetivos de control y los controles para el tratamiento del riesgo, de su Anexo A (4.2.1.g). Asimismo, en su ítem 4.2.2 - Implementar y operar el SGSI, define la necesidad de formular el plan de tratamiento de riesgos para gestionar los riesgos de seguridad de la información e implementar dicho plan con el objetivo de alcanzar los objetivos de control seleccionados, lo cual implica implementar los controles para dichos objetivos de control.[21] Cumplir estos requerimientos significa implementar los procesos involucrados en los controles definidos por el estándar ISO/IEC 27002 (18 dominios) y los procesos explicitados por el estándar ISO/IEC 27005 para la gestión de riesgos.

Es decir, que debemos articular como mínimo[22] tres estándares para establecer, implementar, mantener y mejorar el SGSI.



Ahora bien, como ya dijimos, el estándar ISO/IEC 27001 define los

[21] Los ítems mencionados en estas frases corresponden a la versión de el estándar ISO/IEC 27001:2005, los cuales fueron resumidos por la versión 2013 en sus capítulos 4 y 6.
[22] Recordar que fueron publicadas otras, como por ej. la de métricas.

macro-procesos necesarios para gestionar la seguridad de la información incluyendo acciones muy amplias que podrían ser implementadas de varias maneras. La cuestión que se plantea es ¿cómo saber si la implementación seleccionada es la correcta y es un paso hacia la madurez? ¿Cómo saber que los objetivos se cumplen? Necesariamente debemos descender un escalón para definir subprocesos y procedimientos que permitan completar dichas acciones, lo cual implica la necesidad de definir procesos en detalle. Algo semejante ocurre con el estándar ISO/IEC 27005.

Por otro lado, para que la aplicación de los controles y buenas prácticas contenidas en el estándar ISO/IEC 27002 sea efectiva, deben ser considerados en el marco de procesos formalizados, primer paso para asegurar su cumplimiento, en virtud de la definición de procesos tomada en cuenta por la mejora continua y el modelo de madurez. Cabe señalar que también el estándar hace referencia a la necesidad de formalizar las medidas que propone, lo cual nos lleva entonces a la necesidad de definir esos procesos, subprocesos, procedimientos y normativa interna de la organización.

Es más, el estándar ISO/IEC 27002 incorpora la necesidad y el valor de los procesos. Ello se manifiesta porque además de pedir la formalización de las buenas prácticas, aboga por las métricas, por ejemplo en el ítem 12.6 – GESTIÓN DE VULNERABILIDADES TÉCNICAS; y también por la mejora continua, por ejemplo cuando la sugiere para el proceso de GESTIÓN DE INCIDENTES en el dominio 16. En este caso en particular va más allá de lo establecido por el estándar ISO/IEC 27001, ya que ésta plantea la mejora continua del proceso de seguridad, mientras que el estándar ISO/IEC 27002 plantea la mejora continua de un subproceso.

En conclusión y en respuesta a la pregunta ¿Qué debemos evaluar?: Para efectivizar el SGSI es necesario implementar todos los procesos y subprocesos definidos por las tres normas. Lo cual significa también que para evaluar la madurez de la organización respecto del SGSI, debemos evaluar la madurez de la organización respecto de esos procesos. Es decir la gestión de la seguridad de la información, la gestión de riesgos, y los procesos relacionados con su tratamiento (plan de seguridad) o, lo que

es lo mismo, los involucrados en la implementación de los controles establecidos por la ISO/IEC 27002.

Respecto de la pregunta ¿Con qué herramienta? Tal como hemos planteado en el capítulo anterior, creemos que corresponde utilizar el modelo de madurez del CMMI, ya que el modelo PDCA utilizado por el estándar ISO/IEC 27001 es perfectamente compatible con el criterio de los CMMI, tal como fuera expuesto en los capítulos precedentes. Cabe señalar que, tanto el estándar ISO/IEC 27005, como aquellas que surgieron a partir de la expansión de procesos del estándar ISO/IEC 27002, también responden al modelo PDCA[23], siendo entonces también compatibles.

A modo de ejercicio se propone utilizar los criterios del CMMI-SVC, orientado a la gestión de servicios ya que podríamos considerar la seguridad de la información como un servicio de soporte a la organización.

A continuación se incluye una tabla que muestra el paralelismo entre el modelo CMMI-SVC y el estándar ISO/IEC 27001 (en su versión 2005 ya que en su versión 2013 se han reubicado los conceptos), alineando los ítems que conforman esta última con las áreas de proceso del modelo. En ella es posible ver las coincidencias ya que tanto el modelo como el estándar están basados en el criterio de la calidad de procesos y su mejora continua.

[23] Por ejemplo, el capítulo 16 derivó en el estándar ISO/IEC 27035:2011: Estándar para la Gestión de Incidentes de Seguridad de la Información y el capítulo 17 en la ISO / IEC 27031:2011 - Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de las TIC para la Continuidad del Negocio

Tabla de comparación en el modelo CMMI-SVC y los requerimientos del SGSI planteado por ISO/IEC 27001

Área de Proceso	**CMMI-SVC - Propósito**	**CMMI-SVC Nivel de madurez**	**Nivel de madurez para Seguridad**	**SGSI -27001**	**Comentarios**
Gestión de la Configuración (CM)	Establecer y mantener la integridad de los productos[24] usando identificación, control, contabilización del estado y auditoría de la configuración.	2	2	4.2.2. f-h)	
Medición y Análisis(MA)	Desarrollar y mantener una capacidad de medición suficiente para dar soporte a la necesidad de información de la gestión.	2	2	4.2.2. d)-4.2.3.c)	También el estándar ISO/IEC 27002 sugiere medir, por ejemplo, las vulnerabilidades técnicas.
Aseguramiento de la Calidad de Procesos y Productos (PPQA)	Proveer al staff y la gestión con una mirada objetiva (interna) del proceso y los productos asociados.	2	2	4.2.2.e) y 6 – Aseguramiento/Auditoría Interna	
Gestión de Acuerdos con el Proveedor (SAM)	Gestionar la adquisición de productos y servicios de un proveedor (pueden ser componentes de nuestro producto o consumibles).	2	2		Aplicable a la provisión de activos informáticos que hacen a la seguridad, proveedores de servicios de desarrollo, de asesoramiento o validaciones como “penetración de la red”
Despacho de Servicios (SD)	Despachar servicios de acuerdo con los acuerdos de servicios.	2	2		El estándar ISO/IEC 27001 no hace mención a este concepto, pero sin duda es un mecanismo de la calidad del servicio.

[24] El modelo CMMI-SVC cubre las actividades requeridas para establecer, distribuir y gestionar los servicios. Como se define en el contexto CMMI, un servicio es un producto intangible que no requiere almacenamiento. El modelo CMMI-SVC ha sido desarrollado para ser compatible con esta amplia definición.

Área de Proceso	CMMI-SVC - Propósito	CMMI-SVC Nivel de madurez	Nivel de madurez para Seguridad	SGSI -27001	Comentarios
Gestión de Requerimientos (REQM)	Gestionar los requerimientos de productos y sus componentes y de asegurar el alineamiento entre esos requerimientos y los planes de trabajo y los productos.	2	2	Gestionar las medidas de seguridad : 4.2.2 b-c)	Los grupos de seguridad reciben requerimientos tecnológicos y no tecnológicos que no están planificados. Por ej. incorporación de un nuevo proceso.
Monitoreo y Control del Trabajo (WMC)	Proporcionar una visión del trabajo en ejecución de manera tal que puedan ser aplicadas apropiadas acciones correctivas cuando el desempeño se desvía significativamente del plan.	2	2	Todo 4.2.3, excepto d) - 7 y también 5.1. Ver: GP 2.7 GP 2.8 GP 2.10	
Planeamiento del Trabajo (WP)	Establecer y mantener planes que definan las actividades del trabajo.	2	2	4.2.2.a)Plan de tratamiento del riesgo. Ver: GP 2.2 – GP 2.3 - GP 2.4 - GP 2.5 - GP 2.7	
Gestión de Riesgos (RSKM)	Identificar problemas potenciales antes de que ocurran de manera tal que el tratamiento del riesgo pueda ser planificado e invocado cada vez que sea necesario a través de la vida del producto o trabajo para mitigar impactos adversos en la consecución de los objetivos.	3	Es necesario realizar un análisis específico	4.2.1. c-d-e-f-g-h	Proceso regulado por el estándar ISO/IEC 27005.
Gestión de la Capacidad y Disponibilidad (CAM)	Asegurar un efectivo desempeño del sistema de servicio y que los recursos son provistos y usados efectivamente para dar soporte a los requerimientos del servicio. Tanto la capacidad como la disponibilidad son medidas de calidad. Capacidad es el grado en que una cosa puede soportar, sostener, procesar o producir otra cosa. En el contexto de los servicios, la capacidad puede referirse a la cantidad máxima de entrega del servicio o el máximo número de pedidos de servicio que un sistema puede manejar satisfactoriamente en un período de tiempo. Disponibilidad es el grado en el cual algo es accesible y utilizable cuando se necesita. En el contexto de servicios, la disponibilidad puede referirse al conjunto de tiempos, lugares y otras circunstancias en las cuales los servicios deben ser entregados, los pedidos deben ser cumplidos o cualquier otro aspecto del acuerdo de servicio debe ser logrado.	3	3	4.2.2 g) y 5.2.1.	Proceso que asegura la existencia, mantenimiento, capacidad y disponibilidad de todos los activos informáticos que dan soporte a las funciones de seguridad de la información (Seguridad física, lógica, procesamiento y transferencia de información. En procesamiento se incluye capacidad para logs, información cifrada, existencia de back-ups, capacidad/disponibilidad de las redes, de los dispositivos específicos de seguridad como firewalls, IPS, comunicaciones cifradas, etc.).

Área de Proceso	CMMI-SVC - Propósito	CMMI-SVC Nivel de madurez	Nivel de madurez para Seguridad	SGSI -27001	Comentarios
Análisis de Posibles Decisiones y su Resolución (DAR)	Analizar posibles soluciones usando un proceso de evaluación formal que evalúa alternativas identificadas en comparación con el criterio establecido.	3	3		
Resolución y Prevención de Incidentes (IRP)	Asegurar la oportuna y efectiva resolución de incidentes en el servicio y su adecuada prevención.	3	3	4.2.2 h) 4.2.3.a) y 7	Proceso que da soporte al dominio 16 del estándar ISO/IEC 27002.
Gestión Integrada del Trabajo (IWM)	Establecer y gestionar el trabajo y la participación de los interesados relevantes de acuerdo con un proceso integrado y definido que es personalizado (tailored) a partir del conjunto de procedimientos estándar de la organización.	3	3	4.2.4. c) Ver: GP 2.7 GP 3.1 GP 3.2	Organización de la Seguridad/Compromiso gerencial/ - Cumplimiento de aspectos legales o contractuales, de regulaciones y de requerimientos de seguridad
Definición del Proceso Organizacional (OPD)	Establecer y mantener un conjunto utilizable de activos de procesos organizacionales, estándares de entorno de trabajo, y reglas y guías para los equipos.	3	3		
Focalización en el Proceso Organizacional (OPF)	Planificar, implementar y distribuir mejoras de los procesos organizacionales basados un riguroso entendimiento de las fortalezas y debilidades de los procesos y los activos de procesos organizacionales.	3	3		
Entrenamiento Organizacional (OT)	Desarrollar habilidades y conocimientos de la gente de manera que ellos puedan cumplir sus roles efectiva y eficientemente.	3	3	4.2.2. e) y 5.2.2	"La gente", en el caso de la seguridad, no son sólo los técnicos, sino todos los empleados. Por lo tanto es extensible al concepto de concientización.
Continuidad del Servicio (SCON)	Establecer y mantener planes para asegurar la continuidad de los servicios durante y después de cualquier interrupción significativa de las operaciones normales.	3	3		Proceso que da soporte al dominio 17

Área de Proceso	CMMI-SVC - Propósito	CMMI-SVC Nivel de madurez	Nivel de madurez para Seguridad	SGSI -27001	Comentarios
Transición del Sistema de Servicio (SST)	Distribuir nuevos o significativos cambios de los componentes del sistema de servicio mientras se gestionan sus efectos sobre la ejecución de los servicios en producción.	3	3		
Gestión de la Estrategia de Servicio (STSM)	Establecer y mantener los estándares de servicio acorde a las necesidades estratégicas y planes.	3	3	4.2.1.a) - Alcance y límites	Fijar necesidades y planes estratégicos para los servicios estándar. Las "necesidades estratégicas" son condiciones u objetivos de la organización que a menudo son direccionadas por el entorno. Una organización puede necesitar incrementar sus ganancias o impuestos. Los clientes pueden necesitar un nuevo conjunto de servicios o esperan una oferta de servicios diferentes basados en los que ofrece la competencia.
Desempeño del Proceso Organizacional (OPP)	Establecer y mantener un entendimiento cuantitativo de la realización de procesos seleccionados en el conjunto de procesos estándar de la organización para dar soporte a los objetivos de calidad y desempeño de los procesos y para proveer datos de dicho desempeño, líneas de base y modelos para gestionar cuantitativamente el trabajo organizacional.	4	4	4.2.4 y 8.	
Gestión Cuantitativa del Trabajo (QWM)	Gestionar cuantitativamente el trabajo para alcanzar los objetivos de calidad y desempeño de los procesos establecidos para el trabajo.	4	4	4.2.4 y 8.	
Análisis Causal y su Resolución (CAR)	Identificar las causas de resultados seleccionados y ejercer acciones para mejorar el desempeño de los procesos.	5	5	4.2.4 y 8.	
Gestión del Desempeño Organizacional (OPM)	Gestionar proactivamente el desempeño de los procesos para alcanzar los objetivos de negocio.	5	5	4.2.4 y 8.	

Área de Proceso	CMMI-SVC - Propósito	CMMI-SVC Nivel de madurez	Nivel de madurez para Seguridad	SGSI -27001	Comentarios
	Sería necesario definir un área de proceso que incluya la evaluación de las políticas.			4.2.1.b) Política (Se debe tener en cuenta que es un super set de la política de seguridad de la información). Ver: GP 2.1(*)	No existe como área de proceso en los modelos CMMI, se muestra para indicar que están todos los ítems de la ISO/IEC 27001, aunque algunos correspondan a las metas y prácticas genéricas. (*) Las siglas GG y GP corresponden a los términos metas genéricas (Generic Goals) y prácticas genéricas (Generic Practices). Una explicación sobre las mismas se encuentra a continuación y en el Anexo III – BREVE DESCRIPCIÓN DE LOS CMMI, SUS COMPONENTES Y CARACTERÍSTICAS

A partir de las someras definiciones del propósito de cada área de proceso en la tabla anterior, no es posible percibir la rigurosidad del modelo. Para apreciarla, conviene consultar el Anexo III – BREVE DESCRIPCIÓN DE LOS CMMI, SUS COMPONENTES Y CARACTERÍSTICAS, donde además de su estructura, es posible conocer las trece prácticas genéricas, agrupadas en tres metas genéricas y las 170 prácticas y metas específicas agrupadas en 23 áreas de proceso, que lo conforman.

Como cierre de este capítulo consideramos necesario señalar que, sólo es posible asegurar que los procesos cuya madurez estamos analizando cumplen con los objetivos requeridos, si alcanzan el nivel 2.

Teniendo en cuenta lo antedicho y que los modelos CMMI parten de la premisa que los procesos conforman el hilo conductor de una gestión madura, sin lugar a dudas, ellos son el camino a seguir para lograr la madurez de la gestión de la seguridad de la información[25], integrada en los procesos de negocio. Lo cual comprende además, lograr la madurez del proceso de gestión de riesgos y de los procesos involucrados en la gestión de los controles a aplicar, en función del plan de tratamiento de riesgos/plan de seguridad.

[25] Tal vez el lector se pregunte a esta altura del desarrollo del trabajo, porqué no utilizar el modelo CMM-SSE. Cabe recordar entonces que éste no forma parte de los modelos CMMI, y que está orientado a los aspectos técnicos y empresas ingenieriles según lo ya explicado en el Capítulo V – MECANISMOS/HERRAMIENTAS UTILIZADOS EN LA EVALUACIÓN DE GESTIÓN, razón por la cual no es utilizable en este contexto.

CAPITULO VIII – Y ahora... ¿Cómo lo implementamos?

Del análisis de la bibliografía y de los estándares efectuado en los capítulos previos, así como de la aplicación de la tríada normativa descrita en el capítulo anterior, resulta el esquema plasmado en el siguiente gráfico.

Nota: El SGSI abarca la gestión de riesgos y del programa de seguridad de la información.

El punto de partida de este esquema es que la organización diseña "procesos de negocio" orientados a lograr el cumplimiento de sus objetivos. El proceso de gestión de riesgos evalúa los riesgos de negocio y debe incluir en dicha evaluación la correspondiente a los riesgos de seguridad de la información, lo cual permite generar el plan de tratamiento de riesgos/plan de seguridad de la información. Es decir:

En virtud de que la seguridad de la información está integrada en el negocio, en el marco de la evaluación de riesgos del negocio se debe evaluar en todos los procesos, los eventos[26] asociados al uso y gestión de la información, que potencialmente afecten en forma adversa el logro de los objetivos organizacionales; el plan de tratamiento resultante conformará el plan/programa de seguridad de la información y éste debe ser implementado a través de procesos perfectamente definidos que abarquen aspectos y áreas tecnológicas y no tecnológicas.

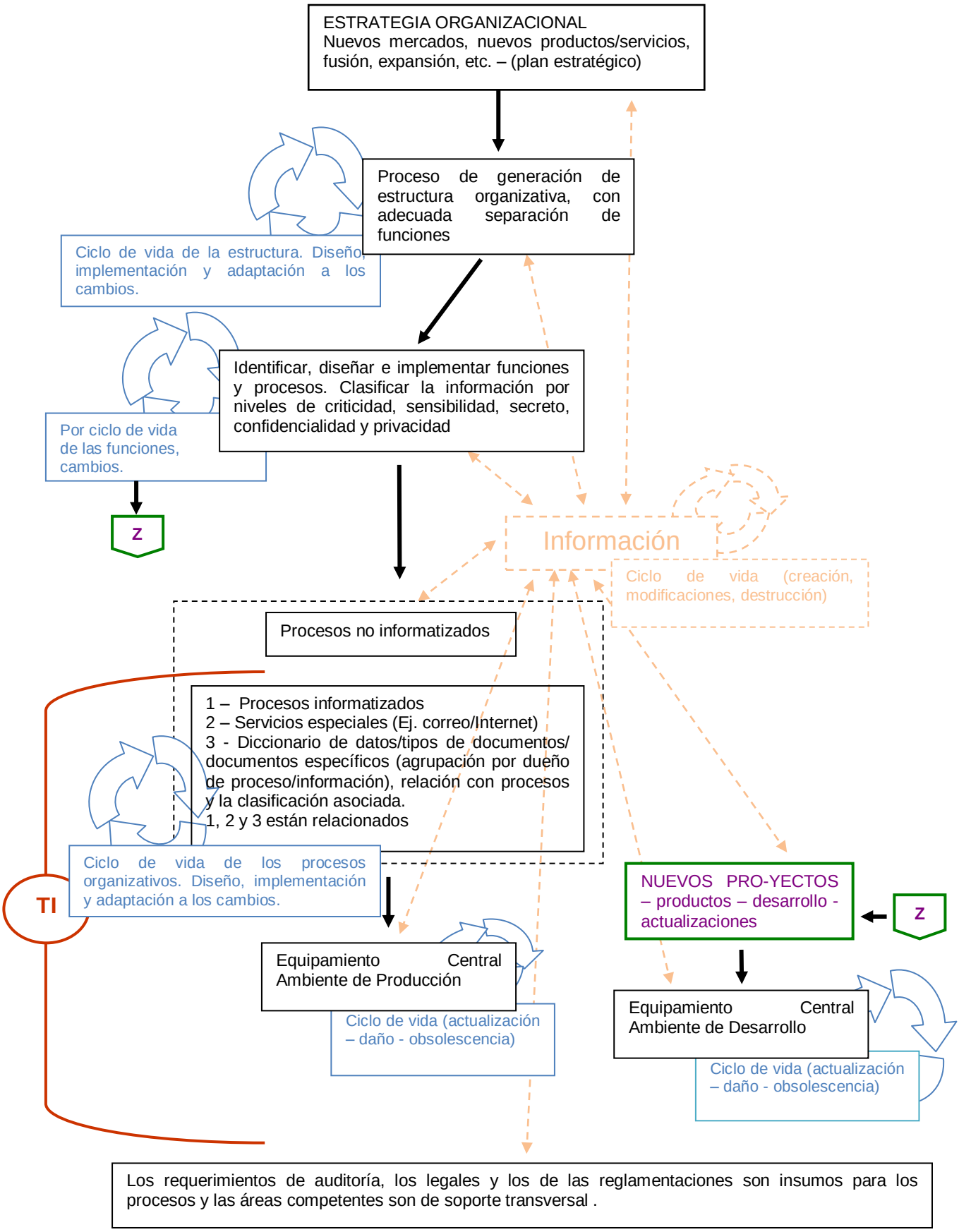
[26] Idem 4.

El modelo de madurez se aplicará a todos los procesos involucrados en este esquema.

Queda claro en la especificación precedente que debemos focalizarnos en los procesos. Por lo tanto, para plantearla de una manera práctica y concreta, representaremos la organización y su relación con la información mediante el gráfico de la página siguiente. En él se caracteriza los procesos organizacionales mediante bloques, colocando la información en el centro de la escena y simbolizando su expansión hacia todos los rincones de la organización. También se representa el dinamismo del sistema organizacional ya que éste cambia permanentemente en función de sus objetivos y del entorno en el que se desarrolla. Es por ello que, además de la relación entre procesos, en cada bloque se ha tomado en cuenta su ciclo de vida, el cual puede dar origen también, a situaciones que podrían modificar los procesos.

Para interpretarlo, se debe pensar en cada bloque como el resultado de la cascada de bloques que lo preceden. Por lo tanto, queda claro que la dimensión tecnológica es resultado de la cascada de procesos organizacionales (principio desarrollado por COBIT 5).

También se ha separado en el sector correspondiente a TI, los procesos en producción de aquéllos que se encuentran en desarrollo. Estos últimos surgen como resultado de los cambios que se originan en cualquiera de los bloques que van desde la definición de la estrategia hasta el de funciones/procesos, así como en cada uno de sus ciclos de vida. Por lo tanto, requieren procesos específicos.


ESTRATEGIA ORGANIZACIONAL
Nuevos mercados, nuevos productos/servicios, fusión, expansión, etc. – (plan estratégico)
Proceso de generación de estructura organizativa, con adecuada separación de funciones
Ciclo de vida de la estructura. Diseño, implementación y adaptación a los cambios.
Identificar, diseñar e implementar funciones y procesos. Clasificar la información por niveles de criticidad, sensibilidad, secreto, confidencialidad y privacidad
Por ciclo de vida de las funciones, cambios.
Z
Información
Ciclo de vida (creación, modificaciones, destrucción)
Procesos no informatizados
1 – Procesos informatizados
2 – Servicios especiales (Ej. correo/Internet)
3 - Diccionario de datos/tipos de documentos/ documentos específicos (agrupación por dueño de proceso/información), relación con procesos y la clasificación asociada.
1, 2 y 3 están relacionados
Ciclo de vida de los procesos organizativos. Diseño, implementación y adaptación a los cambios.
TI
NUEVOS PRO-YECTOS – productos – desarrollo - actualizaciones
Z
Equipamiento Central Ambiente de Producción
Ciclo de vida (actualización – daño - obsolescencia)
Equipamiento Central Ambiente de Desarrollo
Ciclo de vida (actualización – daño - obsolescencia)
Los requerimientos de auditoría, los legales y los de las reglamentaciones son insumos para los procesos y las áreas competentes son de soporte transversal .

Ahora bien, mirando el gráfico anterior, se puede observar que de las tres dimensiones críticas en las que las organizaciones se focalizan (procesos, tecnología y personas), falta considerar esta última.

En el gráfico que incorporamos a continuación vamos a incluir el proceso relacionado con las personas, también denominadas, sin entrar en consideraciones sobre la adecuación de los términos, recursos humanos o capital humano.

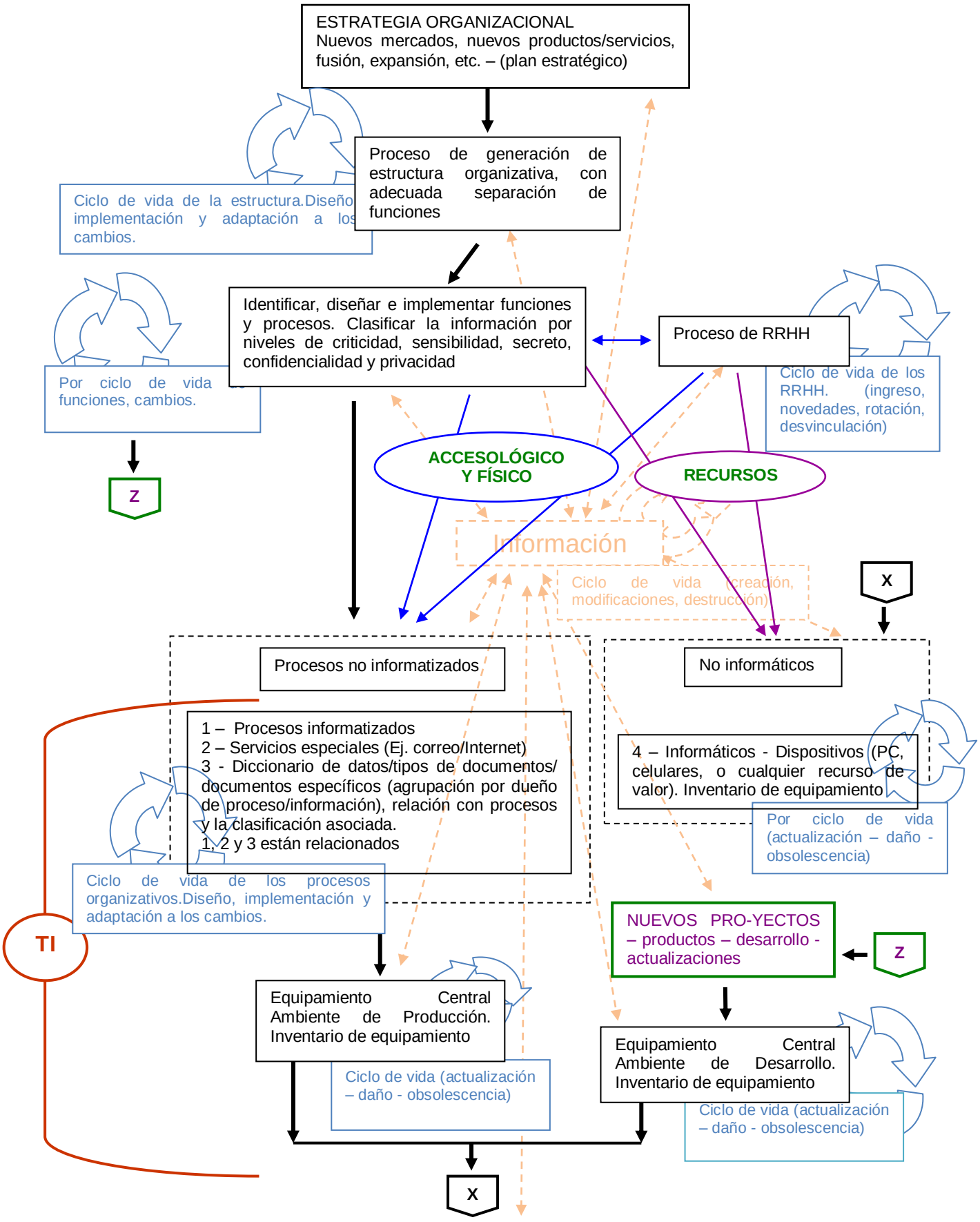
Las personas serán convocadas según los puestos de trabajo creados a partir de las funciones, sin perder de vista la cascada de la cual provienen, y en función de los puestos que desempeñen se les asignarán accesos físicos y lógicos a procesos, áreas e información (en cualquiera de sus presentaciones) y a recursos informáticos y no informáticos (recordar que en algunos puestos un auto puede ser la herramienta asignada). Desde el punto de vista informático estas características conformarán el perfil del puesto.

La relación mencionada se representa mediante conectores de color, diferenciando los dos tipos de asignaciones.

Nótese que mediante el conector "X" se señala que el equipamiento central de producción y desarrollo, así como los recursos conforman el inventario de equipamiento (señalado en cada cuadro) que, a su vez, forma parte del inventario general.

Las personas y sus relaciones con el resto de los componentes agregan nuevos elementos en su relación con la información.

En el gráfico a continuación, podemos ver entonces el mapa completo de las tres dimensiones críticas, procesos, personas y tecnología, y sus relaciones con la información.



Los requerimientos de auditoría, los legales y los de las reglamentaciones son insumos para los procesos y las áreas competentes. Son de soporte transversal .

En la representación gráfica que hemos desarrollado, se puede ver claramente que, estando la información presente en todos y cada uno de los componentes y relaciones organizacionales, surge la necesidad de evaluar los riesgos de seguridad de la información en todo el conjunto, así como en cada ciclo de vida, incluyendo el de la información.

Esta representación nos permite distinguir también, que la asignación de perfiles y recursos a las personas, depende de los procesos organizacionales y que la información que manejan los procesos tecnológicos es generada por y es propiedad de, los procesos organizacionales. Por lo tanto, éstos conforman el centro de la escena, y es por esta razón que la gestión de seguridad y de riesgos se integra en ellos.

Por otro lado, en una rápida visualización del gráfico, se observa que los riesgos de TI son sólo una parte del contexto general de riesgos de seguridad de la información.

Hasta aquí el desarrollo de una de las premisas de nuestra especificación inicial. **"En virtud de que la seguridad de la información está integrada en el negocio, en el marco de la evaluación de riesgos del negocio se debe evaluar en todos los procesos, los eventos asociados al uso y gestión de la información, que potencialmente afecten en forma adversa el logro de los objetivos organizacionales".**

Un aspecto muy importante en este contexto es el de la revisión (con frecuencia dada y ante cambios) de los procesos, una de las etapas de la mejora continua plasmada por el modelo PDCA. En el caso de la gestión de riesgos es fundamental, porque allí se detectarán las nuevas necesidades de seguridad. No sólo se deberá monitorizar/revisar el comportamiento del SGSI (recordar que incluye riesgos) sino también los cambios internos y externos que pueden generar nuevos riesgos: cambios en la legislación, regulaciones, contratos, proveedores, sistemas, procesos y nuevas amenazas, etc. Para ello se deberá contar con adecuados procesos de investigación y seguimiento de todo tipo de eventos. Una organización con nivel de madurez alto puede cambiarlo sorpresivamente al ponerse en vigencia una ley, adquirir otra organización, cambiar a otra plataforma o simplemente por reemplazar un especialista de alta preparación a uno de

menor formación o capacidad.

Se podría considerar como ejemplo, los procesos de transferencia de datos personales. Previamente a la puesta en vigencia de la Ley de Habeas Data éstos se transferían sin control alguno. A posteriori, comenzaron a constituir un riesgo legal. O bien que, a partir del uso de nuevas tecnologías de desarrollo de aplicaciones en ambiente abierto y en la Web, se generaron nuevos riesgos de seguridad para la información.

La segunda parte de la especificación inicial enuncia: **"...el plan de tratamiento resultante conformará el plan/programa de seguridad de la información y éste debe ser implementado a través de procesos perfectamente definidos que abarquen aspectos y áreas tecnológicas y no tecnológicas.**"

En realidad, el estándar ISO/IEC 27001, considera que los riegos, en todos los casos posibles, serán tratados mediante los controles previstos en el estándar ISO/IEC 27002, que además están listados en su Anexo A. Por otro lado, éstos pueden ser complementados por los planteados en el estándar ISO/IEC 27005 y los que surgen de la experiencia profesional y de otras organizaciones. Asimismo, la implementación del plan de tratamiento de riesgos (plan/programa de seguridad de la información) quedará atado a los criterios que la organización ha adoptado respecto de la aceptación del riesgo y a su evaluación y priorización, lo cual podría justificar que algunos controles no fueran aplicados.

Ahora bien, ¿qué significa implementar los controles? ¿Son piezas tecnológicas, prácticas procedimentales que de manera puntual se aplican para determinados casos? No. Con seguridad no lo son. Los controles forman parte de un sistema de control interno y como tal, deben ser considerados en procesos organizacionales que harán uso tanto de procedimientos manuales como automatizados. Es decir, la implementación de los controles especificados por el estándar ISO/IEC 27002 deberá ser realizada a través de procesos organizacionales que podrían ser transversales a toda la organización. A esta conclusión nos lleva el propio estándar al haber transformado, a lo largo de los años, algunos de sus capítulos en procesos específicos y, consecuentemente, haber desarrollado

estándares para ellos. En este orden de cosas entonces, se debería pensar en la implementación de los siguientes procesos (nótese que los capítulos del estándar son asociados a la gestión de un proceso específico):

- Gestión de las políticas de seguridad (dominio 5)
- Gestión de estructura y funciones (dominio 6 y 12)
- Gestión de RRHH (dominios 7 y 9). Habitualmente se conoce, desde los aspectos tecnológicos, como gestión de identidades y accesos. Según nuestra visión es necesario agregarle los aspectos no tecnológicos. Asimismo debiera relacionarse con los procesos de gestión de estructura, funciones y activos, tal como se indica en el gráfico de la página 57.
- Gestión de activos (dominios 8 y 12). Inventario de activos informáticos (definidos en la 27005) y catálogo de procesos. Pertenencia y clasificación.
- Gestión de Seguridad Física (dominio 11). Si analizamos en profundidad este dominio del estándar ISO/IEC 27002, veremos que la seguridad física está relacionada con la seguridad edilicia, ambiental, del trabajo, etc. Lo cual nos lleva a la idea de convergencia vista en capítulos anteriores.
- Gestión de comunicaciones, operaciones, control de accesos y aplicaciones de negocio (dominios 9, 12, 13 y 14).
- Gestión de Incidentes (dominio 16) - En la actualidad involucra cumplir con el estándar ISO/IEC 27035:2011 - *Estándar para la Gestión de Incidentes de Seguridad de la Información.*
- Aspectos de Seguridad de la Gestión de la Continuidad del Negocio (dominio 17). Aquí es importante mencionar que el estándar sugiere integrar los requerimientos de la seguridad de la información con otros requerimientos de continuidad relacionados con aspectos tales como operaciones, recursos humanos, materiales, transporte e instalaciones. Actualmente contenidos en el estándar ISO / IEC 27031:2011 - *Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de las TIC para la Continuidad del Negocio*.

- Gestión del cumplimiento (dominio 18). Relacionado con la gestión legal, análisis de nueva legislación, gestión de regulaciones, contratos, normas, así como los relacionados con la verificación del cumplimiento y la auditoría.
- Gestión del intercambio de información con terceras partes (dominio 13), que deberán incluir la gestión de acuerdos de servicio y convenios donde se establezca las responsabilidades sobre la seguridad de la información. Algunos de los aspectos tratados en el dominio 13 - SEGURIDAD DE LAS COMUNICACIONES, pueden ser parte de los temas de Gobierno.

Cabe aclarar que la guía anterior no es de cumplimiento obligatorio si no se desea certificar ISO/IEC 27001, pero sería deseable que lo enunciado en la misma sea tenido en cuenta por el SGSI de la organización.

El gerenciamiento del accionar diario de un área de seguridad de la información, nos permite detectar situaciones específicas que enriquecen nuestro conocimiento. Es por ello que se ha agregado, en el Anexo IV – PROCESOS A GESTIONAR, algunas de las metas relacionadas con la seguridad de la información, obtenidas en base a la experiencia.

Es decir, que para llevar a la práctica los requerimientos fijados por las distintas normas deberemos implementa procesos PDCA que pueden ser transversales a la organización y también contenidos unos en otros. En consecuencia, para conocer la madurez de la gestión de la seguridad de la información integrada en los procesos de negocio debemos aplicar a la gestión de los procesos involucrados, los requerimientos establecidos por el modelo de madurez CMMI, descritos en el Capítulo VII - PERO...¿QUÉ DEBEMOS EVALUAR? Y ¿CON QUÉ HERRAMIENTA?

Queda claro entonces, que la evaluación de madurez tendrá un alcance igual al alcance de la implementación del sistema de gestión de que se trate.

De hecho, los certificadores de ISO/IEC 27001 son muy enfáticos en este tema y recomiendan delimitar muy bien el alcance, ya que si éste es "toda la organización", todos los requerimientos de seguridad deberán ser implementados en ese entorno. Lo cual nos llevaría, en este caso, a implementar también el modelo de madurez con ese alcance.

Otro ejemplo práctico lo da COBIT 5 que, aunque evalúa con el modelo de capacidad utilizando la norma ISO/IEC 15504 parte 2, abarca en su alcance "todos" los procesos comprendidos en el marco.

A continuación presentamos algunas situaciones reales, que dan cuenta de escenarios de riesgo de seguridad de la información en procesos organizacionales y definimos algunos de los requerimientos a concretar desde la visión integradora.

Caso 1 - Decisiones estratégicas. Las de un importante grupo económico del país dedicado a la comercialización masiva (retailers), que ha adquirido varias empresas del rubro. Si bien tecnológicamente las empresas adquiridas se adaptan en un plazo razonable, generalmente pasa hasta un año, antes de ajustar los perfiles de los empleados de dichas empresas. En general, lo logran cuando llega el momento de integrarlos en SAP ERP[27]. Durante ese período de tiempo podrían ocurrir incidentes de seguridad que incluso podrían pasar inadvertidos si no se ha implementado una efectiva gestión de incidentes.

Requerimientos de la gestión integrada

1. La evaluación de riesgos respecto de la decisión estratégica de adquirir una compañía (desde ahora denominada "B") debería incluir en su alcance, la evaluación de riesgos de seguridad de la información (desde ahora se identificará como RSI) de dicha compañía. Tanto tecnológicos como no tecnológicos.

   Debemos tener en cuenta que el enunciado del caso dice que la adaptación al SGSI central es más rápida en sus aspectos tecnológicos. Por lo tanto, será necesario focalizarse en los que no lo son. Por ejemplo, la gestión de identidades enfocada desde el criterio de SAP ERP.
2. Se deberá analizar si B tiene implementado un proceso de gestión de riesgos y si éste alcanza a los RSI.

[27] SAP ERP - Systeme, Anwendungenund Produkte in der Datenverarbeitung (Sistemas, Aplicaciones y Productos en Procesamiento de Datos) - Enterprise Resource Planning (Sistemas de Planificación de Recursos Empresariales)

3. Se deberá analizar si B cuenta con un plan de tratamiento de RSI/plan de seguridad de la información y si éste se encuentra totalmente implementado a través de todos los sistemas de gestión descritos por el estándar ISO/IEC 27002.
4. Si además, se desea conocer el nivel de madurez de B, deberían ser evaluados los criterios del modelo de madurez de CMMI. Sería ideal analizar si el nivel de madurez de B es mayor o menor al de la organización adquirente.

Caso 2 - Proceso operativo en un organismo del Estado. Un área que debía enviar información personal a los beneficiarios, para hacerlo en un tiempo más corto eligió el correo electrónico como instrumento de envío. Estaban convencidos que el procedimiento era correcto dado que habían pensado en todos los controles. Sin embargo, estaban utilizando un medio altamente inseguro para enviar datos personales, los cuales se hallan protegidos por la ley de Habeas Data.

Requerimientos de la gestión integrada

1. En la evaluación de riesgos del proceso de negocio, se debería evaluar el riesgo de seguridad de la información en la entrega de información protegida por la ley. Sea dicha entrega realizada a los titulares del dato o a terceros.
2. En el caso de terceros existen cuestiones accesorias a considerar respecto del consentimiento, las cuales probablemente deban ser evaluadas por las áreas jurídicas.
3. En el caso de los titulares, debiera ser considerada la posibilidad de que la información enviada sea sustraída. El correo electrónico es una herramienta vulnerable y si su uso se descarta, también sería necesario considerar las vulnerabilidades de cualquier otra herramienta propuesta.

Caso 3 - Proceso de distribución, entrega e instalación de PC, notebooks, dispositivos móviles, etc. En un organismo del Estado se detectó la entrega de equipamiento a empleados sin la correspondiente

documentación ni registro del movimiento, lo cual impacta directamente sobre la Gestión de Activos.

Requerimientos de la gestión integrada

1. La evaluación de riesgos del proceso de gestión de recursos humanos (Ver Anexo IV - Procesos a gestionar, pág. 99 y el proceso de RRHH en el gráfico de la pág. 57) debe incluir la evaluación de riesgos de seguridad de la información involucrando en ella la entrega de activos informáticos físicos.
2. En el proceso en análisis deben estar definidos el alcance y responsabilidad de las acciones de los empleados intervinientes. Deben existir las instancias de autorización, recepción y devolución. ¿Qué debe hacer un técnico cuando retira un disco? ¿En cuánto tiempo debe llevarlo al stock o al taller? ¿Qué debe suceder en las instalaciones descentralizadas? ¿Cómo se realiza la gestión si el mantenimiento es un servicio tercerizado? ¿Cómo impedir la instalación de equipamiento propio en las bocas de redes, o cómo minimizar los riesgos si se permite?, etc.

Caso 4 - Conexión directa a Internet en un área operativa. Detectado durante una auditoría al Área de Comunicaciones en un organismo público.

Requerimientos de la gestión integrada

1. El proceso de creación de áreas en la estructura organizativa, además de justificar su creación y definir su función primaria y sus actividades, debe definir los puestos de trabajo y los recursos necesarios de toda índole.
2. La evaluación de riesgos de la definición de áreas en la estructura organizativa debe incluir la evaluación de riesgos de seguridad de la información. Véase en el gráfico de pág. 57, que el bloque de identificación, diseño e implementación de funciones y procesos está ligado al proceso de RRHH y a las relaciones "Acceso Lógico y Físico" y "Recursos". Estos accesos y recursos debieran involucrar el acceso y conexión a Internet.

3. En el caso que nos ocupa, se debió haber analizado si el área debía tener un acceso más amplio y mayor velocidad y haberlo resuelto a través de contrataciones y/o configuraciones específicas pero siempre controladas por las áreas técnicas correspondientes.

Caso 5 - Procedimientos de excepción. Dícese así de los procedimientos que involucran la carga (incorporación, modificación) manual de datos, por parte de los operadores del centro de procesamiento, en bases de datos de producción. Ello es necesario generalmente, porque los aplicativos no permiten la corrección de errores o carecen de alguna funcionalidad, que podría ser efectuada por supervisores autorizados.

La falta de un procedimiento definido y controlado, atenta contra la integridad de la información ya que, los operadores involucrados tendrían permisos de acceso a las bases de datos de producción.

Requerimientos de la gestión integrada

1. En la evaluación de riesgos de seguridad de la información que se realice en los proyectos de desarrollo de aplicaciones, debería contemplarse esta situación y definir los controles para su tratamiento.
2. Dichos controles deberían ser diseñados acorde a las directivas de la Dirección Nacional de Protección de Datos Personales, en caso que los datos involucrados fueran personales.
3. El procedimiento de excepción debería ser justificado y autorizado, así como ser utilizado como disparador de un alerta a las áreas responsables de desarrollo a los efectos de que produzcan la corrección en el aplicativo correspondiente.
4. Nótese que el procedimiento no sólo involucra las áreas técnicas, sino también las usuarias que realizan los requerimientos de desarrollo de aplicaciones.

Caso 5 - Gestión de cambios. Al realizar un cambio de infraestructura en una compañía, olvidaron un punto de acceso (access point) con seguridad

WEP en la red de servidores. Lo crakearon desde la cafetería de la empresa[28].

Requerimientos de la gestión integrada

En principio debemos señalar que la gestión de cambios es un proceso suficientemente complejo para que en pocas líneas podamos reflejar sus necesidades. Se debe recordar que la Gestión de Cambios es uno de los Servicios de Gestión de TI desarrollados por la Information Technology Infrastructure Library (ITIL).

En consecuencia sólo vamos a agregar que este mal llamado "olvido" indica que la gestión de cambios entrega un servicio defectuoso, lo cual implica que la gestión de cambios no es efectiva (por lo menos a nivel tecnológico y de seguridad). Por lo tanto, esta compañía no ha llegado ni siquiera nivel 2 de madurez para el proceso de gestión de cambios, que es el nivel donde efectivamente se logran los objetivos del proceso.

Evaluación de madurez. En los ejemplos precedentes hemos mostrado una visión integradora de eventos puntuales, que debieron haber sido tratados en el marco de un proceso organizacional predefinido. Ahora bien, para poder afirmar que el SGSI[29] alcanza un determinado nivel de madurez, debiera cumplir con los **criterios del modelo de madurez de CMMI** en cada uno de los procesos integradores expuestos, a saber:

1. El proceso integrador existe y es efectivo desde la óptica del SGSI, la gestión de riesgos y la implantación de controles. Es decir debe cumplir con todos los requerimientos del nivel 2 enunciados en la tabla de págs. 47 a 51. Por ejemplo, debe ser planificado y monitoreado, debe cumplir con los acuerdos de servicio, debe cumplir con los requerimientos de calidad, debe tener capacidad de medición, etc.
2. Una vez logrado el nivel 2, con el que se asegura que el proceso cumple su objetivo, es necesario avanzar sobre el resto de los niveles descritos

[28] XI Seminario Anual de CYBSEC – Tendencias de Seguridad 2012 - Exposición sobre "Administración segura de dispositivos móviles".

[29] Recordar que éste está conformado por la gestión de riesgos y de controles, según la articulación de los tres estándares ya explicada en capítulos precedentes.

en la tabla ya mencionada.

Para ello y en primera instancia, se debe implementar las áreas de proceso que componen el nivel 3, el cual conforma el primer paso hacia la madurez.

Nuevamente observando la tabla de págs. 47 a 51 podemos ver que, respecto del SGSI[30], se debiera cumplir con la gestión de capacidad y disponibilidad. Es decir, la gestión de riesgos de seguridad de la información y la gestión de los controles a implantar debiera tener la capacidad suficiente para encarar los procesos integradores y debiera estar disponible cada vez que fuera necesario.

Además, debiera buscar soluciones mediante un proceso de evaluación formal, resolver incidentes (del proceso en sí), encarar el trabajo a partir del conjunto de procedimientos estándar de la organización, desarrollar habilidades y conocimientos del personal participante, tratar los cambios, etc.

Para que sea más sencillo asociar estas definiciones con los procesos integradores descritos más arriba, desarrollaremos de manera resumida los criterios de nivel 3 para el caso de la evaluación estratégica de la adquisición de una empresa por parte de otra (Caso 1).

a) La empresa adquirente deberá contar en el equipo evaluador con un representante del área de riesgos que evalúe los riesgos de la información y cuáles debieran ser los controles a aplicar para lo cual tendrá que disponer también, de un representante del área de seguridad de la información y probablemente, alguno de las áreas tecnológicas.

b) Ello implica que estos requerimientos deben estar implementados con procedimientos institucionalizados, las áreas competentes deberán contar con la capacidad y disponibilidad suficiente para estar presente en cada oportunidad en que la organización se disponga a realizar una evaluación estratégica, los cual significa contar con una gestión

[30] Recordar que éste está conformado por la gestión de riesgos y de controles, según la articulación de los tres estándares ya explicada en capítulos precedentes.

de cambios y por supuesto, el personal deberá estar capacitado en el trabajo a realizar.

Este camino debe ser encarado para todos los procesos organizacionales, si tenemos en cuenta el gráfico de pág. 57.

Conclusiones

El título de este trabajo " Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio" involucra varios conceptos que entendimos era necesario explicar y justificar. De allí la inclusión de citas y referencias de diferentes autores, sobre cuyas estudios y conclusiones construimos esta propuesta.

Al realizar el análisis de dichos conceptos hemos utilizado, de alguna manera, una perspectiva histórica, al mostrar en cada caso, la evolución de los conceptos aplicados en la seguridad de la información, a partir de la evolución de aquéllos aplicados en el ámbito organizacional. Este paralelismo sirve también para acreditar el cambio que se da en la materia que nos ocupa, virando desde una visión tecnológica hacia una organizacional. Es muy importante destacar esta situación, pues aquellos que no han transitado esta transformación, como por ejemplo los profesionales que se formaron en la administración de organizaciones y luego pasaron a la gestión de la seguridad de la información, pueden considerar trivial lo expuesto en esta obra.

En consecuencia, transitaremos en estas conclusiones el mismo camino que recorrimos en la Introducción para dar sustento al objetivo definido y su justificación: "seleccionar un modelo para la evaluación de madurez de la gestión de la seguridad de la información integrada en los procesos de negocio, así como los riesgos asociados al uso[31] de la información y los controles definidos para su tratamiento".

Es así entonces, que en el Capítulo II - LA INTEGRACIÓN COMO PARTE DE LA NUEVA VISIÓN, mostramos el cambio de enfoque al pasar de la alineación de las TIC con el negocio, a su integración con él, a lo cual también se sumó la seguridad de la información. En él hemos hecho referencia a las aseveraciones de destacadas instituciones mundiales que han avanzado primero hacia el gobierno de las TIC y que actualmente coinciden en señalar que un adecuado gobierno de la seguridad de la

[31] Idem 3.

información es imprescindible para hacer negocios. Con lo cual, hemos mostrado la tendencia mundial de considerar la integración de la seguridad de la información en los procesos de negocio.

Otro de los conceptos que enunciamos como necesario es la integración de la evaluación de riesgos de seguridad de la información en la evaluación de riesgos de negocio, así como de redefinir el plan de seguridad de la información. Es así como en el Capítulo III - DEL PLAN DE SEGURIDAD HACIA EL PLAN DE TRATAMIENTO DE RIESGOS, mostramos este decisivo cambio de visión que plantea el estándar ISO/IEC 27001 [37], como resultado del hito histórico de la aparición del Marco Integrado de Gestión de Riesgos publicado por el Grupo COSO, luego de un viraje de visión desde el control hacia el riesgo. Además, discurrimos también sobre varias posturas internacionales que afirman que la gestión de riesgos de seguridad de la información debe estar integrada en la gestión de riesgos del negocio.

La disquisición desarrollada en el Capítulo IV - ¿CUÁL DEBIERA SER EL ENFOQUE DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN?, es central desde el punto de vista de nuestro trabajo. En él se explica el camino que siguió la evolución de la gestión de riesgos en seguridad de la información, pasando de un enfoque eminentemente tecnológico a uno organizacional. Llegando incluso a definir la necesidad de revisión del estándar ISO/IEC 27005 [38] para orientarlo hacia la visión del estándar ISO 31000 [39]. Esta nueva postura de los estándares no hace más que convalidar nuestra posición al inicio de este trabajo, de trabajar sobre los eventos y no sobre amenazas y vulnerabilidades; lo cual brinda una visión más abarcativa y permite pensar en términos del negocio.

Las premisas desarrolladas en los capítulos previamente mencionados, nos permiten fundamentar la posición que plasmamos en el capítulo final:

"En virtud de que la seguridad de la información está integrada en el negocio, en el marco de la evaluación de riesgos del negocio se

debe evaluar en todos los procesos, los eventos[32] asociados al uso y gestión de la información, que potencialmente afecten en forma adversa el logro de los objetivos organizacionales; el plan de tratamiento resultante conformará el plan/programa de seguridad de la información y éste debe ser implementado a través de procesos perfectamente definidos que abarquen aspectos y áreas tecnológicas y no tecnológicas."

Pero el título de este trabajo hace referencia a un modelo de madurez, razón por la cual planteamos en principio, la necesidad de evaluar los sistemas de gestión y las diferentes herramientas utilizadas para ello. Es así, que decidimos desarrollar el Capítulo V - MECANISMOS/HERRAMIENTAS UTILIZADOS EN LA EVALUACIÓN DE UN SISTEMA DE GESTIÓN, mostrando que las mismas permiten que directivos y partes interesadas (stakeholders) conozcan el estado de situación de la organización. En nuestro recorrido destacamos la posición de los modelos CMMI [40] por ser los que rescatan el valor de los procesos, teniendo en cuenta que los estándares ISO/IEC 27001, 27002 [41] y 27005 definen cada sistema de gestión como un proceso PDCA[33]. También diferenciamos el modelo de capacidad del de madurez, explicando que para comparar organizaciones diferentes y para evaluar la organización como un todo, es necesario utilizar el modelo de madurez.

Ahora bien, como resultado del análisis de diferentes modelos de madurez, llegamos a la conclusión, en el Capítulo VI - ¿QUÉ ES EL "MODELO DE MADUREZ" Y POR QUÉ USARLO?, que la generalidad de ellos habían tomado la tabla de evaluación de los modelos CMMI, aunque distorsionada, y luego habían desarrollado arbitrariamente y con muy poca rigurosidad algunas condiciones para alcanzar dichos valores. Pero lo que es más significativo aún es que llamaron modelo de madurez a un modelo de capacidad. Esta aseveración queda demostrada cuando el marco COBIT5 decide usar para la evaluación, el estándar ISOIEC 15504 parte 2

---

[32] Idem 4.

[33] Modelo de procesos definido por la teoría de calidad total: PLANIFICAR-HACER-VERIFICAR-ACTUAR.

[42] que corresponde a la evaluación de un modelo de capacidad, tal como se explica en el capítulo. En él también se destaca un trabajo de investigación de Gartner [43] cuya conclusión es, para la mayoría de las empresas analizadas, que la gestión de los procesos de seguridad de la información mostraban serias deficiencias. En este sentido es muy reveladora la síntesis que realiza la consultora al afirmar que muchas organizaciones han implementado principalmente controles tecnológicos, así como contratado los recursos humanos necesarios para manejarlos, pero ignoran los aspectos humanos de la seguridad y no entienden los requerimientos del negocio sobre la gestión de la seguridad. En el documento de Gartner al que estamos haciendo referencia se propone para evaluar dicha gestión, la utilización de un modelo ad-hoc propio o del modelo CMMI. Esta apreciación más nuestros propios análisis ya referenciados, fundamenta la elección del modelo de madurez CMMI.

Si bien el recorrido que hemos realizado a través de los distintos capítulos justifica los diferentes conceptos involucrados en el título del trabajo, entendimos que nos faltaba una cuestión esencial. Y así estructuramos el Capítulo VII - PERO...¿QUÉ DEBEMOS EVALUAR? Y ¿CON QUÉ HERRAMIENTA?, donde mostramos que, si el SGSI definido por el estándar ISO/IEC 27001, se basa en la Gestión de Riesgos definida por el estándar ISO/IEC 27005 para obtener un plan de tratamiento de riesgos que luego derivaría en el plan de seguridad por el cual se implementarían los controles del estándar ISO/IEC 27002, es necesario articular e implementar los tres estándares para lograr la implementación del SGSI. Asimismo, como cada uno de ellos conforma uno o varios procesos, se debería evaluar la madurez de cada uno de ellos.

A los efectos de mostrar que es posible utilizar el modelo de madurez CMMI para evaluar el SGSI, se construyó una tabla de comparación entre el modelo CMMI-SVC y el estándar ISO/IEC 27001, expuesta en las págs. 47 a 51 señalando que dicho modelo, también puede ser aplicado a la gestión de riesgos y cualquier otro de los procesos necesario para llevar a cabo la implementación del estándar ISO/IEC 27002.

Por último, en el Capítulo VIII - Y AHORA... ¿CÓMO LO

IMPLEMENTAMOS?, se desarrolla la construcción en el ámbito organizacional, de los conceptos explicados hasta el momento. Aquí se muestra en sendos gráficos los procesos de negocio, tecnológicos y no tecnológicos, y la penetración de la información en cada uno de ellos, pudiéndose ver claramente que los tecnológicos conforman sólo una pequeña parte del total. También, mediante otro gráfico de círculos concéntricos, se muestra la secuencia de la integración de la gestión de riesgos de seguridad en la gestión de riesgos de los procesos de negocio, lo cual se logra a través de la evaluación de los eventos relacionados con el uso y gestión de la información en todos los procesos de negocios. Dicha secuencia, implica que finalmente también el plan de seguridad se integra en los procesos de negocio.

Se concluye entonces a partir de esa secuencia que, para evaluar la madurez de la organización, es necesario evaluar la madurez de todos los procesos relacionados con la implementación de los tres estándares ya mencionados, situación ejemplificada a través del desarrollo de varias situaciones reales.

ANEXO I – Conceptos complementarios

Ref. ITGI*: "El IT Governance Institute (ITGI) fue establecido en 1998 en virtud de la creciente criticidad de las tecnologías de la información en el éxito de la empresa. En muchas organizaciones, el éxito depende de la habilidad de las TI para permitir el logro de las metas organizacionales. En tales entornos, el gobierno de las TI es una disciplina tan crítica para la dirección y el gerenciamiento como el gobierno corporativo o empresarial. Un efectivo gobierno de las TI ayuda a asegurar que las TI dan soporte a los objetivos de negocio, maximiza las inversiones y maneja adecuadamente las oportunidades y los riesgos." [44]*

Ref. GobSI*: "Los cinco resultados que se esperan del gobierno de la seguridad de la información son:*

1. *Alineación estratégica de la seguridad de la información para dar soporte a los objetivos organizacionales.*
2. *Gestión del riesgo a través de la ejecución de adecuadas medidas para gestionar y mitigar los riesgos y reducir potenciales impactos sobre los recursos de información a un nivel aceptable.*
3. *Gestión de recursos utilizando los conocimientos de seguridad de la información y la infraestructura eficiente y efectivamente.*
4. *Medición del desempeño midiendo, monitoreando y reportando métricas del gobierno de la seguridad de la información para asegurar que los objetivos organizacionales son alcanzados.*
5. *Entrega de valor optimizando la inversión de la seguridad de la información en soporte a los objetivos organizacionales.*" [45]

"Un concepto promisorio (promising/promissory-que encierra en sí promesa-que a futuro se ve como bueno), conducido en gran parte por la creciente tendencia en segmentar la seguridad en funciones separadas pero relacionadas, se focaliza en la integración de un proceso de aseguramiento de la gestión de una organización en relación con los procesos de seguridad. Esto puede servir para mejorar la seguridad general y la eficiencia operativa.

……

Evaluar los procesos de gestión desde el comienzo al final, en conjunto con sus controles, puede mitigar la tendencia a que existan "espacios" (gaps) entre varias funciones." [46]

Ref. Cvg: Integración de los procesos de aseguramiento (Convergencia)

"Un área emergente de interés conceptual relacionada al resultado sugerido de gobierno de seguridad de la información es el aseguramiento de los procesos de negocio o la integración del aseguramiento.

La mayoría de las organizaciones utilizan numerosos procesos de aseguramiento, cada uno en "silos" no integrados. Estas actividades están a menudo relacionadas a la seguridad de la información pero operan más o menos independientemente. Esta falta de integración demostrable e innecesaria crea a menudo un número de riesgos no identificados que deben ser tratados. Un enfoque para el gobierno de la seguridad de la información que incluye un esfuerzo para integrar estas funciones de aseguramiento debe ser considerado para asegurar que los procesos operan como se espera desde el comienzo al fin, o sea, minimizando riesgos escondidos." [47]

Ref. CGTF*: "La seguridad de la información no es sólo un tema técnico sino también un desafío para el negocio y la gobernabilidad que involucra la gestión de riesgos, generación de informes y rendición de cuentas.*

Una seguridad efectiva requiere el compromiso activo de la dirección ejecutiva para evaluar nuevas amenazas y proveer un fuerte liderazgo sobre la ciberseguridad. El término para describir el compromiso escrito de la dirección ejecutiva es gobierno corporativo. Éste consiste en un conjunto de políticas y controles internos mediante los cuales la organización, independientemente de su tamaño o forma, es dirigida y gestionada. El gobierno de la seguridad de la información es un subconjunto del programa de gobierno total. La gestión de riesgos, la generación de reportes y la rendición de cuentas son elementos centrales de estas políticas y controles internos". [48]

Ref. NIST: Una *amenaza* es cualquier circunstancia o evento con la posibilidad de impactar adversamente en las operaciones organizacionales y

bienes, individuos, otras organizaciones o la Nación, a través de sistemas de información mediante accesos no autorizados, destrucción, revelación o modificación de información, así como también la denegación de servicios. Los *eventos de amenaza* son causados por fuentes de amenaza. Una *fuente de amenaza* se caracteriza por: (i) la intención y el método destinado a la explotación de una vulnerabilidad, o (ii) una situación y un método que pueden explotar accidentalmente una vulnerabilidad. En general, los tipos de fuentes de amenazas incluyen: (i) ciberataques o ataques físicos hostiles, (ii) errores humanos de omisión o comisión, (iii) las deficiencias estructurales de los recursos controlados de la organización (por ejemplo, hardware, software, control ambiental), y (iv) los desastres naturales y de origen humano, los accidentes y fallas ajenas a la organización.

Vulnerabilidades y Condiciones que las predisponen: Una *vulnerabilidad* es una debilidad en un sistema de información, en los procedimientos de seguridad del sistema, en los controles internos, o en una aplicación que podría ser explotada por una amenaza. La mayoría de las vulnerabilidades de los sistemas de información pueden estar asociadas con los controles de seguridad que, o bien no se han aplicado (ya sea intencionalmente o no), o se han aplicado pero conservan cierta debilidad. Sin embargo, también es importante tener en cuenta la posibilidad de que surjan vulnerabilidades naturalmente, a medida que la misión/función de negocios de la organización evolucionan en el tiempo, los entornos de operación cambian, las nuevas tecnologías proliferan, y nuevas amenazas aparecen. En el contexto de este cambio, los controles de seguridad existentes se vuelvan inadecuados y pueden necesitar ser reevaluados para verificar su eficacia. La tendencia de los controles de seguridad de potencialmente degradar su eficacia con el tiempo refuerza la necesidad de mantener las evaluaciones de riesgos durante todo el ciclo de vida de desarrollo del sistema, así como la importancia de los programas de monitoreo continuo para obtener conocimiento de la situación actual de la seguridad de la organización.

Las vulnerabilidades no sólo se encuentran en los sistemas de información. Viendo estos sistemas en un contexto más amplio, las

vulnerabilidades pueden encontrarse en las estructuras del gobierno organizacional (ej. la falta de efectivas estrategias de gestión de riesgos y de adecuados marcos de riesgos, pobre comunicación entre agencias, decisiones inconsistentes sobre la prioridad relativa de funciones de negocio). También pueden encontrarse en relaciones externas (ej. dependencia de fuentes de energía particulares, cadena de suministros, tecnologías de información y proveedores de telecomunicaciones); en procesos de negocio (ej. procesos pobremente definidos o que no tienen en cuenta el riesgo); y arquitecturas de seguridad de la organización/información (ej. pobres decisiones sobre la arquitectura resultando en falta de resiliencia de los sistemas de información organizacionales).

Una *condición que predispone una vulnerabilidad* es una condición que existe dentro de una organización, un proceso de la misión o de negocios, de arquitectura de la empresa, de un sistema de información, o del entorno operativo, lo que afecta (es decir, aumenta o disminuye) la probabilidad de que los eventos de amenaza, una vez iniciados, resulten en impactos adversos sobre las operaciones de la organización y bienes, las personas, las otras organizaciones, o la Nación. Este tipo de condiciones incluyen, por ejemplo, la ubicación de una instalación en una zona de huracanes o inundable (aumento de la probabilidad de exposición a los huracanes o inundaciones) o un sistema de información independiente sin conexión a la red externa (disminución de la probabilidad de exposición a un ataque cibernético sobre la en red). Las vulnerabilidades resultantes de los factores que las predisponen y que no pueden ser corregidas fácilmente podrían incluir, por ejemplo, deficiencias en los planes de contingencia, el uso de tecnologías obsoletas o debilidades/deficiencias en la copia de seguridad de los sistema de información y mecanismos de recuperación de fallas. En todos los casos, este tipo de vulnerabilidades crean una predisposición a eventos de amenazas que tienen impactos adversos en la organización. Las vulnerabilidades (incluyendo las predispuestas por determinadas condiciones) forman parte de la situación de seguridad global de los sistemas de información de la organización y los entornos de

operación que puede afectar a la probabilidad de ocurrencia de un evento de amenaza.

Anexo II – Algunos modelos

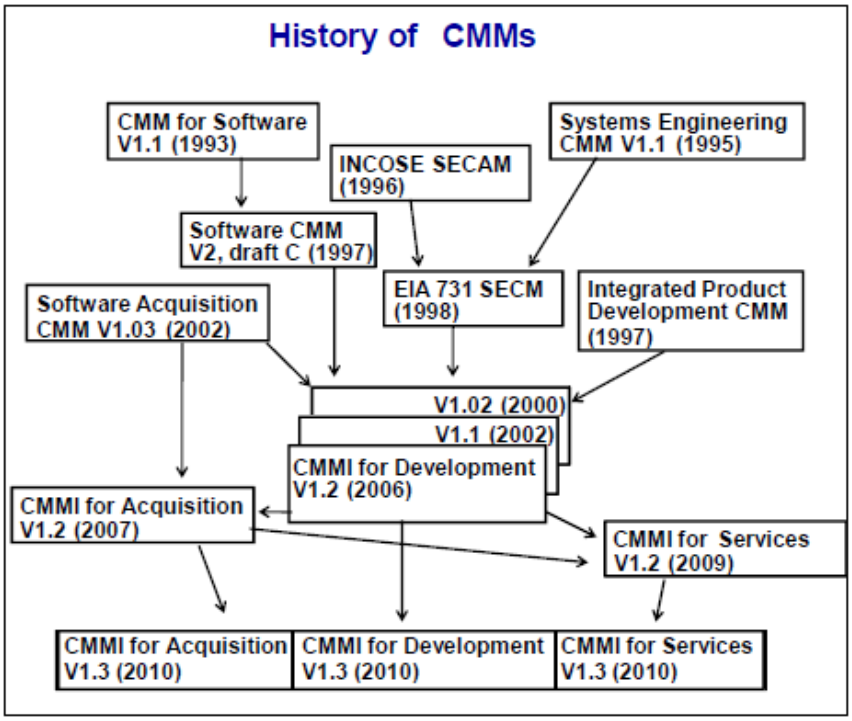
Modelo de Madurez y Capacidad o Capability Maturity Model (CMM)

Es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al software por la Universidad Carnegie-Mellon para el Software Engineering Institute (SEI).

El SEI es un centro de investigación y desarrollo patrocinado por el Departamento de Defensa de los Estados Unidos de América y gestionado por la Universidad Carnegie-Mellon. "CMM" es una marca registrada del SEI.

A partir de noviembre de 1986 el SEI, a requerimiento del Gobierno Federal de los Estados Unidos de América, desarrolló una primera definición de un modelo de madurez de procesos en el desarrollo de software, que se publicó en septiembre de 1987. Este trabajo evolucionó al modelo CMM o SW-CMM (CMM for Software), cuya última versión (v1.1) se publicó en febrero de 1993.

En el año 2000 se presentó el Modelo de Capacidad y Madurez Integrado o Capability Maturity Model Integration (CMMI), el cual fue desarrollado para facilitar y simplificar la adopción de varios modelos de forma simultánea.



Fuente: CMMI for Services – Vs. 1.3 – Introducción – Pág. 6

Systems Security Engineering Capability Maturity Model (SSE-CMM)

Este modelo describe las características esenciales del proceso de ingeniería de los sistemas de seguridad, para asegurar que sea correcto. Es aplicable por organizaciones que desarrollan productos de seguridad, integradoras y las que proveen servicios de seguridad. Fue construido a partir del System Engineering CMM (SE-CMM).

Su mantenimiento es realizado por la International Systems Security Engineering Association (ISSEA) - www.issea.org - una organización sin fines de lucro que fuera constituida en 1999, dedicada al avance de la Ingeniería de los Sistemas de Seguridad como una disciplina definida y mensurable.

Un interesante artículo [49] compara este modelo con varias guías de seguridad (ISO/IEC 13335 - Guidelines for the Management of IT Security or GMITS, NIST Handbook, Canadian Handbook on Information Technology Security) y considera que, si bien tratan los mismos tópicos, las guías, excepto los estándares ISO, son difíciles de transportar a otras culturas o jurisdicciones. En cambio el modelo parte del concepto de que frente a

situaciones similares, el resultado del proceso va a ser mejor y más consistente si aumentamos su nivel de capacidad

Information Security Management Maturity Model (ISM3)

Define un modelo de sistema de gestión de seguridad de la información desde una óptica de negocios considerando la gestión estratégica, táctica y operacional. Es una iniciativa del ISM3 Consortium[34]. Actualmente es impulsado por el Open Group, razón por la cual su sigla es O-ISM3.

Si bien se lo promociona como una manera fácil de implementar la ISO/IEC 27001, no está enfocado en los procesos y más que un modelo es una guía muy detallada y de orden tecnológico de controles a aplicar, con lo cual requiere permanente actualización. Es posible encontrar críticas respecto de su falta de visión de riesgos [50] o de ser sólo un sistema de métricas [51].

[34] Si bien no ha sido posible encontrar la fecha en la que este modelo se publicó por primera vez, existen referencias al mismo desde setiembre de 2004.

Anexo III – Breve descripción de los CMMI, sus componentes y características

Sobre los modelos de capacidad y madurez

Estos modelos se focalizan en el mejoramiento de los procesos en una organización. Ellos contienen los elementos esenciales para los procesos efectivos de una o más disciplinas y describen un camino de evolución de la mejora desde procesos ad-hoc, inmaduros, hasta procesos disciplinados, maduros, con calidad y efectividad mejoradas

"Al igual que otros CMMs, los modelos CMMI proveen una guía para usar al momento de desarrollar procesos. Los modelos CMMI no son procesos o descripción de procesos. Los procesos usados en una organización dependen de muchos factores, los cuales incluyen los dominios de aplicaciones y la estructura y tamaño de la misma. En particular, las áreas de procesos de un modelo CMMI típico no se corresponde uno a uno con los procesos usados en una organización."

Actualmente, CMMI es una aplicación de los principios introducidos más de un siglo atrás en este ciclo continuo de mejora de procesos.

"Todos los modelos CMMI se producen a partir del CMMI Framework (CMF), el cual contiene todas las metas y prácticas que son usadas para obtener los modelos CMMI que pertenecen a las diferentes constelaciones.

Todos los modelos contienen una cantidad definida de áreas de proceso. Éstas cubren conceptos básicos que son fundamentales para la mejora del proceso." [52]

- - - - - - - - -

Un "constelación" se define como una colección de componentes del CMMI que es usada para construir modelos, material de entrenamiento y documentos de evaluación relacionados para un área de interés (ej. adquisición, desarrollo, servicios). El modelo de la "constelación de servicio" se denomina "CMMI para Servicios" o "CMMI-SVC". [53]

"Un área de proceso es un conjunto de prácticas relacionadas en un área tal que, cuando son implementadas colectivamente, satisfacen un conjunto de metas consideradas importantes para mejorar dicha área." [*54*]

- - - - - - - -

Comprendiendo los niveles

En CMMI-SVC los niveles son usados para describir un camino a transitar durante la evolución, recomendado para una organización que quiera mejorar los procesos que utiliza para proveer servicios.

- - - - - - - - - -

CMMI soporta dos caminos de mejora. Uno permite a la organización mejorar incrementalmente los procesos correspondientes a un área de proceso individual (o grupo de áreas de proceso) seleccionada por la organización. El otro, permite mejorar un conjunto de procesos relacionados, mediante la mejora incremental de sucesivos conjuntos de áreas de proceso.

Estos dos caminos de mejora están asociados con dos tipos de niveles: los de capacidad y los de madurez. Estos niveles se corresponden con dos enfoques denominados "representaciones". Las dos representaciones se denominan "continua" y "escalonada o por etapas".

Usando la representación continua se alcanza "niveles de capacidad". Usando la representación escalonada se alcanza "niveles de madurez".

Para alcanzar un nivel particular, una organización debe satisfacer todas las metas de esa área de proceso o de un conjunto de áreas de proceso que han sido elegidos para ser mejorados, independientemente de que sea un nivel de capacidad o madurez.

Ambas representaciones proveen maneras de mejorar los procesos para lograr los objetivos de negocios, y ambas proveen el mismo contenido esencial y usa los mismos componentes del modelo.

A continuación se incluye un gráfico de la estructura de cada representación [55].

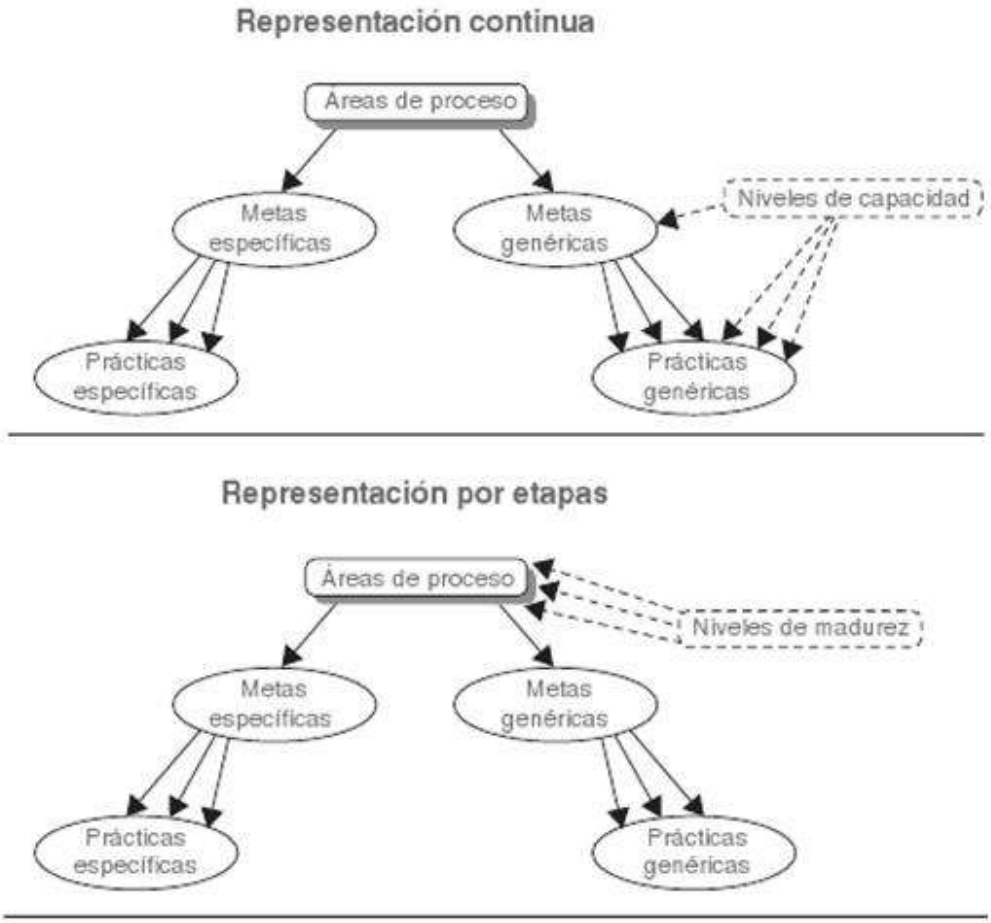


Figura 3.3.1
Tomado de: CMMI® Guía para la integración de procesos y la mejora de productos. Mary Beth Chrissis,

Entendiendo el modelo de capacidad

"Los niveles de capacidad proveen una manera de mejorar los procesos correspondientes a áreas de proceso individuales. Se definen cuatro niveles de capacidad numerados de 0 a 3.

0. Incompleto

1. Realizado

2. Gestionado

3. Definido

Un nivel de capacidad para un área de proceso es alcanzado cuando todas las metas genéricas son satisfechas hasta ese nivel. El hecho de que

los niveles de capacidad 2 y 3 usen los mismos términos que las metas genéricas 2 y 3 es intencional porque cada una de estas metas y prácticas genéricas reflejan el significado de los niveles de capacidad de las metas y las prácticas.

La representación continua implica seleccionar un área de proceso para mejorar y el nivel de capacidad deseado para esa área de proceso. En este contexto, si un proceso está realizado o es incompleto es importante. Por ello se le da el nombre "incompleto" al punto de comienzo del la representación continua."

Entendiendo el modelo de madurez

"Un nivel de madurez consta de prácticas relacionadas específicas y genéricas para un conjunto predefinido de áreas de proceso que mejoran el rendimiento global de la organización. El nivel de madurez de una organización proporciona un camino para predecir el rendimiento en una disciplina dada o en un conjunto de disciplinas.

La experiencia ha mostrado que las organizaciones toman la mejor decisión cuando centran sus esfuerzos de mejora de procesos en un número controlable de áreas de proceso a la vez y que dichas áreas requieren aumentar su complejidad cuando la organización mejora.

Un nivel de madurez es una meseta evolutiva definida para la mejora de procesos de la organización. Cada nivel de madurez madura un subconjunto importante de procesos de la organización, preparándola para pasar al siguiente nivel de madurez. Los niveles de madurez se miden mediante el logro de metas específicas y genéricas asociadas a cada conjunto predefinido de áreas de proceso.

Existen cinco niveles de madurez, siendo cada uno de ellos una capa en la cimentación de la mejora de procesos en curso, denominados por los números 1 a 5.

Los niveles de madurez proveen una manera de mejorar los procesos organizacionales a través de múltiples áreas de proceso. Los cinco niveles de madurez son numerados de 1 a 5.

1. Inicial

2. Gestionado

3. Definido

4. Gestionado cuantitativamente

5. Optimizado

La representación escalonada implica seleccionar múltiples áreas de proceso a mejorar dentro de un nivel de madurez; en consecuencia, si áreas de proceso individuales están realizadas o incompletas no es el enfoque primario. Entonces, se le da el nombre "inicial" al punto de comienzo de la representación escalonada.

Los niveles de madurez son usados para caracterizar la mejora organizacional respecto a un conjunto de áreas de proceso, mientras que los niveles de capacidad caracterizan la mejora organizacional respecto de un área de proceso individual." [56]

Descripción de niveles por modelo

Modelo de Capacidad (Se aplica por área de proceso)

Nivel 0 – *Incompleto*: Una o más de las metas específicas del área de proceso no se cumplen.

Nivel 1 – *Realizado*: El área de proceso cumple con todas las metas específicas. Es decir, se obtiene el producto. Si bien llegar a este nivel implica una mejora, ésta no se mantendrá a través del tiempo. Debe cumplir las metas y prácticas genéricas correspondientes con el nivel (Ver RESUMEN DE METAS Y PRÁCTICAS GENÉRICAS, pág. 90). Es decir, las denominadas G1.

Nivel 2 – *Gestionado*: Además, debe cumplir las metas y prácticas genéricas correspondientes con el nivel (Ver RESUMEN DE METAS Y PRÁCTICAS GENÉRICAS, pág. 90). Es decir, las denominadas G2. Lograr este nivel significa que los procesos son planificados y se ejecutan según las políticas y que las prácticas existentes se mantendrán aún en tiempos de stress.

Nivel 3 – *Definido*: Los estándares, procesos y sus descripciones, del área

de proceso están redactados de una manera más rigurosa y son adecuados al conjunto de estándares utilizados por la organización. Los procesos son manejados proactivamente entendiendo las relaciones entre las actividades y las medidas detalladas del proceso y sus productos. Además, debe cumplir las metas y prácticas genéricas correspondientes con el nivel (Ver RESUMEN DE METAS Y PRÁCTICAS GENÉRICAS, pág. 90). Es decir, las denominadas G3.

Modelo de Madurez (Se aplica para un conjunto predefinido de áreas de proceso)

La tabla que se incluye en págs. 47 a 51 muestra las áreas de procesos agrupadas por los niveles descritos a continuación, a efectos de que sea posible evaluar a la organización en ese nivel de madurez.

Los niveles de madurez son medidos por el logro de las metas y prácticas genéricas y específicas asociadas con cada conjunto predefinido de áreas de proceso.

Nivel 1 – *Inicial*: (No existe el nivel 0) Los procesos son ad hoc y caóticos. Las organizaciones que están en este nivel están caracterizadas por una tendencia a abandonar sus procesos en épocas de crisis y por ser incapaces de repetir sus éxitos.

Nivel 2 – *Gestionado*: Los procesos de este nivel están institucionalizados[35]. El cumplimiento es evaluado y el desempeño compartido con los ejecutivos. La disciplina de los procesos ayuda a asegurar que las prácticas existentes se realizan aún en tiempos de stress. Se aplican las metas genéricas G2 (Ver RESUMEN DE METAS Y PRÁCTICAS GENÉRICAS, pág. 90).

Nivel 3 – *Definido*: Estos procesos están bien especificados y entendidos y están descritos en estándares, procedimientos, herramientas y métodos. Los estándares, procesos y sus descripciones, del área de proceso están redactados de una manera más rigurosa y son adecuados al conjunto de

[35] Institucionalización. Los procesos están arraigados en la manera de hacer negocios, de cumplir con el trabajo. La organización los sigue rutinariamente como parte de la cultura corporativa. Hay compromiso y consistencia en el cumplimiento del proceso.

estándares utilizados por la organización. Los procesos son manejados proactivamente entendiendo las relaciones entre las actividades y las medidas detalladas del proceso y sus productos. Además, debe cumplir las metas y prácticas genéricas correspondientes con el nivel (Ver RESUMEN DE METAS Y PRÁCTICAS GENÉRICAS, pág. 90). Es decir, las denominadas G3.

Un proceso definido provee una base para planificar, cumplir o desempeñar y mejorar las tareas y actividades. Un trabajo puede tener más de un proceso definido (por ej. uno para desarrollar el producto y otro para testearlo). Los procesos de este nivel claramente establecen:

- Propósito
- Entradas
- Criterio de entradas
- Actividades
- Roles
- Métricas
- Pasos de verificación
- Salidas
- Criterios de salidas

Nivel 4 – *Gestionado cuantitativamente*: En este nivel se establecen objetivos cuantitativos para la calidad y el desempeño de los procesos y son usados como criterio para la gestión. Una distinción crítica de este nivel respecto del anterior es que el cumplimiento de estos procesos es predecible. En el nivel 4, el cumplimiento de los procesos es controlado utilizando estadísticas y otras técnicas cuantitativas y las predicciones están en parte basadas en el análisis estadístico de datos muy granulados.

Nivel 5 – *En optimización*: Una diferencia crítica entre este nivel y el anterior es el tema en el que se focalizan. En el nivel 4, la organización y los grupos de trabajo se centran en entender y controlar el desempeño a nivel de los subprocesos y usando los resultados para gestionar el

proyecto. En el nivel 5, la organización se focaliza con el desempeño de toda la organización usando los datos recolectados en múltiples grupos de trabajo. El análisis de estos datos identifica brechas en el desempeño, que son usadas para dirigir la mejora de los procesos organizacionales que genera diferencias medibles.

Las someras descripciones del propósito de cada área de proceso son expandidas en un conjunto de metas y prácticas genéricas (GG y GP por sus siglas en inglés), más un conjunto de metas y prácticas específicas (SG y SP por sus siglas en inglés).

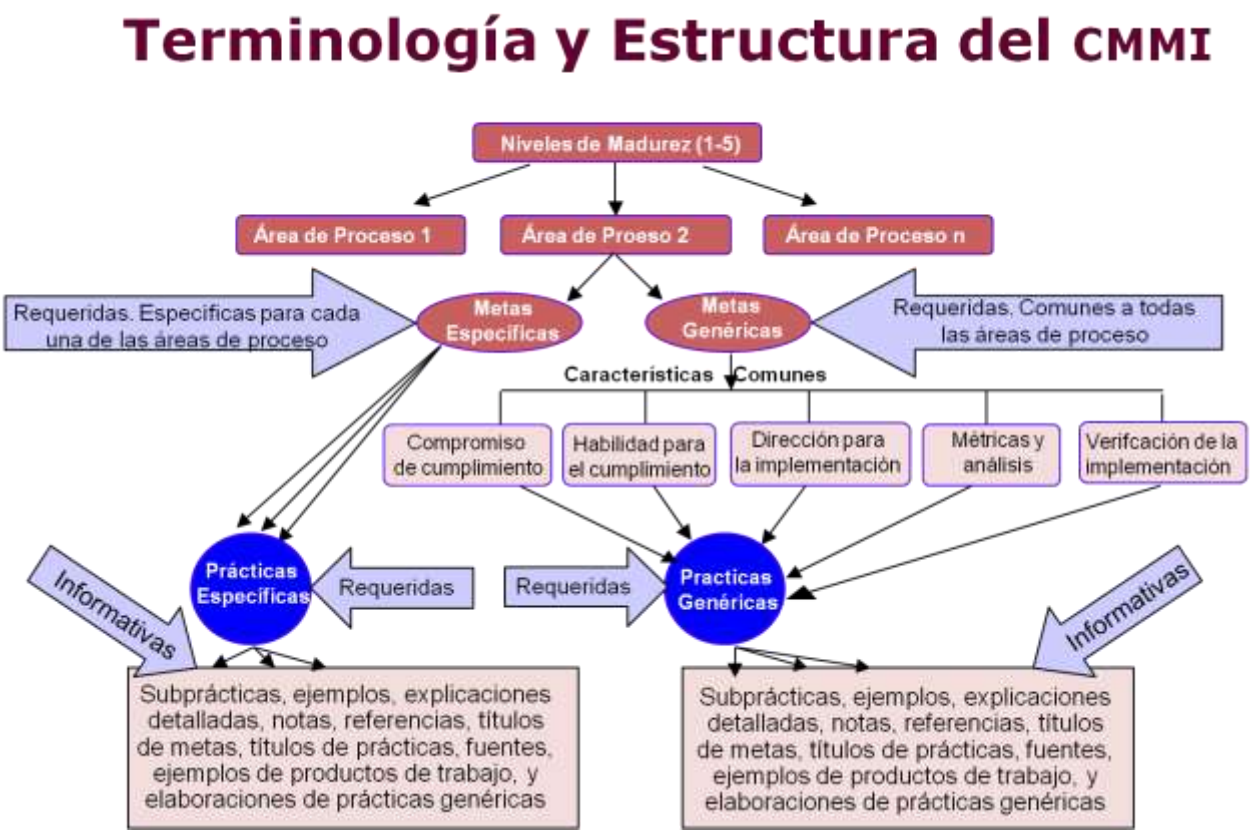
A continuación se muestra una tabla que resume la definición de ambos modelos en función de sus niveles y de los requerimientos de cumplimiento de las metas relacionadas.

	CAPACIDAD **Se trabaja sobre un área de proceso o un grupo cualesquiera de ellas**			**MADUREZ** **Se trabaja sobre todas las áreas de proceso que el modelo indica para un determinado nivel**		
Nivel	**Nombre**	**Metas Específicas**	**Metas Genéricas**	**Nombre**	**Metas Específicas**	**Metas Genéricas**
0	Incompleto	1 o más no se cumplen	No se cumplen			
1	Ejecutado	Se cumplen	No se cumplen	Inicial	Habitualmente se logra el resultado pero heroicamente	
2	Gestionado	Se cumplen	Se cumplen las GG2	Gestionado	Se cumplen	Se cumplen las GG2
3	Definido	Se cumplen	Se cumplen las GG3	Definido	Se cumplen	Se cumplen las GG3
4				Gestionado Cuantitativamente	Todas las áreas de proceso involucradas deben alcanzar el nivel de capacidad 3 (Definido)	
5				En optimización		

Las metas y prácticas genéricas (GG y GP) son componentes que guían a la organización hacia la institucionalización de los procesos

Cabe señalar que la implementación de los modelos **requiere** alcanzar las **metas** genéricas y específicas. Ahora bien, para considerar que dichos requerimientos han sido satisfechos, deben estar presentes en los procesos planeados e implementados, las **prácticas** genéricas y específicas, a pesar de que ambas son descritas sólo como **esperadas**.

Una representación de su estructura es la siguiente:



Fuente: www.cs.njit.edu/~kirova/**ppt/CMMI.ppt**

Resumen de metas y prácticas genéricas

Metas Genéricas	Prácticas Genéricas
GG 1 Lograr las metas específicas	GP 1.1 Realizar las prácticas específicas
GG 2 Institucionalizar un proceso gestionado	GP 2.1 Establecer una política organizativa
	GP 2.2 Planificar el proceso
	GP 2.3 Proporcionar recursos
	GP 2.4 Asignar responsabilidades
	GP 2.5 Capacitar a las personas
	GP 2.6 Controlar los productos de trabajo
	GP 2.7 Identificar e involucrar a las partes interesadas relevantes
	GP 2.8 Monitorizar y controlar el proceso
	GP 2.9 Evaluar el cumplimiento objetivamente

	GP 2.10 Revisar el estado con los niveles de gestión superiores
GG 3 Institucionalizar un proceso definido	GP 3.1 Establecer un proceso definido
	GP 3.2 Recopilar experiencias relacionadas con procesos

Resumen de metas y prácticas específicas por área de proceso.

Metas Específicas	Prácticas Específicas
Gestión de Capacidad y Disponibilidad (CAM)	
SG 1 Preparar la gestión de capacidad y disponibilidad	SP 1.1 Establecer una estrategia de gestión de capacidad y disponibilidad
	SP 1.2 Seleccionar medidas y técnicas de análisis
	SP 1.3 Establecer representaciones del sistema de servicio
SG 2 Monitorizar y analizar la capacidad y disponibilidad	SP 2.1 Monitorizar y analizar la capacidad
	SP 2.2 Monitorizar y analizar la disponibilidad
	SP 2.3 Informar acerca de la gestión de capacidad y disponibilidad
Análisis Causal y Resolución (CAR)	
SG 1 Determinar las causas de los resultados seleccionados	SP 1.1 Seleccionar los resultados a analizar
	SP 1.2 Analizar las causas
SG 2 Abordar las causas de los resultados seleccionados	SP 2.1 Implementar las propuestas de acción
	SP 2.2 Evaluar los efectos de las acciones implementadas
	SP 2.3 Registrar los datos del análisis causal
Gestión de configuración (CM)	
SG 1 Establecer líneas base	SP 1.1 Identificar elementos de configuración
	SP 1.2 Establecer un sistema de gestión de configuración
	SP 1.3 Crear o liberar líneas base
SG 2 Seguir y controlar los cambios	SP 2.1 Seguir las peticiones de cambio
	SP 2.2 Controlar los elementos de configuración
SG 3 Establecer la integridad	SP 3.1 Establecer registros de gestión de configuración
	SP 3.2 Realizar auditorías de configuración
Análisis de Decisiones y Resolución (DAR)	
SG 1 Evaluar Alternativas	SP 1.1 Establecer guías para el análisis de decisiones
	SP 1.2 Establecer criterios de evaluación

Metas Específicas	Prácticas Específicas
	SP 1.3 Identificar soluciones alternativas
	SP 1.4 Seleccionar métodos de evaluación
	SP 1.5 Evaluar soluciones alternativas
	SP 1.6 Seleccionar soluciones
Resolución y prevención de incidencias (IRP)	
SG 1 Preparar la resolución y prevención de incidencias	SP 1.1 Establecer un enfoque para la resolución y prevención de incidencias
	SP 1.2 Establecer un sistema de gestión de incidencias
SG 2 Identificar, controlar, y tratar cada incidencia	SP 2.1 Identificar y registrar incidencias
	SP 2.2 Analizar los datos de cada incidencia
	SP 2.3 Resolver incidencias
	SP 2.4 Monitorizar el estado de las incidencias hasta su cierre
	SP 2.5 Comunicar el estado de las incidencias
SG 3 Analizar y tratar las causas e impactos de las incidencias seleccionadas	SP 3.1 Analizar las incidencias seleccionadas
	SP 3.2 Establecer soluciones para responder a futuras incidencias
	SP 3.3 Establecer y aplicar soluciones para reducir la ocurrencia de incidencias
Gestión integrada de trabajaos (IWM)	
SG 1 Utilizar el proceso definido para el trabajo	SP 1.1 Establecer el proceso definido
	SP 1.2 Utilizar los activos de proceso organizativos para planificar los trabajos
	SP 1.3 Establecer el entorno de trabajo
	SP 1.4 Integrar los planes
	SP 1.5 Gestionar el trabajo utilizando los planes integrados
	SP 1.6 Establecer equipos
	SP 1.7 Contribuir a los activos de proceso organizativos
SG 2 Coordinarse y colaborar con las partes interesadas relevantes	SP 2.1 Gestionar la Involucración de las Partes Interesadas
	SP 2.2 Gestionar las Dependencias
	SP 2.3 Resolver los Problemas de Coordinación
Medición y análisis (MA)	
SG 1 Alinear las actividades de medición y análisis	SP 1.1 Establecer objetivos de medición
	SP 1.2 Especificar medidas
	SP 1.3 Especificar procedimientos de recogida y almacenamiento de datos

Metas Específicas	Prácticas Específicas
	SP 1.4 Establecer procedimientos de análisis
SG 2 Proporcionar resultados de medición	SP 2.1 Obtener mediciones
	SP 2.2 Analizar mediciones
	SP 2.3 Almacenar los datos y los resultados
	SP 2.4 Comunicar los resultados
Definición organizativa de procesos (OPD)	
SG 1 Establecer activos de proceso organizativos	SP 1.1 Establecer procesos estándar
	SP 1.2 Establecer descripciones de modelos de ciclo de vida
	SP 1.3 Establecer criterios y guías de adaptación
	SP 1.4 Establecer el repositorio de mediciones de la organización
	SP 1.5 Establecer la biblioteca de activos de proceso de la organización
	SP 1.6 Establecer estándares de entorno de trabajo
	SP 1.7 Establecer reglas y guías para los equipos
Enfoque organizativo de procesos (OPF)	
SG 1 Determinar oportunidades de mejora de procesos	SP 1.1 Establecer necesidades de procesos organizativas
	SP 1.2 Evaluar los procesos de la organización
	SP 1.3 Identificar las mejoras de proceso de la organización
SG 2 Planificar e implementar acciones de proceso	SP 2.1 Establecer planes de acciones de proceso
	SP 2.2 Implementar planes de acciones de proceso
SG 3 Desplegar activos de proceso organizativos e incorporar experiencias	SP 3.1 Desplegar activos de proceso organizativos
	SP 3.2 Desplegar procesos estándar
	SP 3.3 Monitorizar la implementación
	SP 3.4 Incorporar experiencias a los activos de proceso organizativos
Gestión del Rendimiento organizativo (OPM)	
SG 1 Gestionar el rendimiento de negocio	SP 1.1 Mantener los objetivos de negocio
	SP 1.2 Analizar datos de rendimiento de procesos
	SP 1.3 Identificar áreas de mejora potenciales
SG 2 Seleccionar mejoras	SP 2.1 Recabar mejoras sugeridas
	SP 2.2 Analizar mejoras sugeridas

Metas Específicas	Prácticas Específicas
	SP 2.3 Validar mejoras
	SP 2.4 Seleccionar e implementar mejoras para su despliegue
SG 3 Desplegar mejoras	SP 3.1 Planificar el despliegue
	SP 3.2 Gestionar el despliegue
	SP 3.3 Evaluar los efectos de la mejora
Rendimiento organizativo de procesos (OPP)	
SG 1 Establecer líneas base y modelos de rendimiento	SP 1.1 Establecer objetivos de calidad y rendimiento de procesos
	SP 1.2 Seleccionar procesos
	SP 1.3 Establecer medidas de rendimiento de procesos
	SP 1.4 Analizar el rendimiento y establecer líneas base de rendimiento de procesos
	SP 1.5 Establecer modelos de rendimiento de procesos
Capacitación organizativa (OT)	
SG 1 Establecer una competencia de capacitación organizativa	SP 1.1 Establecer necesidades estratégicas de capacitación
	SP 1.2 Determinar las necesidades de capacitación que son responsabilidad de la organización
	SP 1.3 Establecer un plan táctico organizativo de capacitación
	SP 1.4 Establecer una competencia de capacitación
SG 2 Proporcionar capacitación	SP 2.1 Impartir capacitación
	SP 2.2 Establecer registros de capacitación
	SP 2.3 Evaluar la eficacia de la capacitación
Aseguramiento de calidad de procesos y productos (PPQA)	
SG 1 Evaluar objetivamente los procesos y productos de trabajo	SP 1.1 Evaluar objetivamente los procesos
	SP 1.2 Evaluar objetivamente los productos de trabajo
SG 2 Proporcionar un conocimiento objetivo	SP 2.1 Comunicar y resolver problemas de no conformidad
	SP 2.2 Establecer registros
Gestión cuantitativa de trabajos (QWM)	
SG 1 Preparar la gestión cuantitativa	SP 1.1 Establecer los objetivos del trabajo
	SP 1.2 Componer el proceso definido
	SP 1.3 Seleccionar subprocesos y atributos
	SP 1.4 Seleccionar medidas y técnicas de análisis
SG 2 Gestionar el trabajo cuantitativamente	SP 2.1 Monitorizar el rendimiento de los subprocesos seleccionados

Metas Específicas	Prácticas Específicas
	SP 2.2 Gestionar el rendimiento del trabajo
	SP 2.3 Realizar análisis de causas raíces
Gestión de requisitos (REQM)	
SG 1 Gestionar requisitos	SP 1.1 Entender los requisitos
	SP 1.2 Obtener el compromiso con los requisitos
	SP 1.3 Gestionar los cambios a los requisitos
	SP 1.4 Mantener la trazabilidad bidireccional entre los requisitos
	SP 1.5 Asegurar que los productos de trabajo y los requisitos estén alineados
Gestión de riesgos (RSKM)	
SG 1 Preparar la gestión de riesgos	SP 1.1 Determinar fuentes y categorías de riesgo
	SP 1.2 Definir parámetros de riesgo
	SP 1.3 Establecer una estrategia de gestión de riesgos
SG 2 Identificar y analizar riesgos	SP 2.1 Identificar riesgos
	SP 2.2 Evaluar, categorizar, y priorizar los riesgos
SG 3 Mitigar riesgos	SP 3.1 Desarrollar planes de mitigación de riesgos
	SP 3.2 Implementar planes de mitigación de riesgos
Gestión de acuerdos de suministro (SAM)	
SG 1 Establecer acuerdos de suministro	SP 1.1 Determinar el tipo de adquisición
	SP 1.2 Seleccionar suministradores
	SP 1.3 Establecer acuerdos de suministro
SG 2 Satisfacer los acuerdos de suministro	SP 2.1 Ejecutar el acuerdo de suministro
	SP 2.2 Aceptar el producto adquirido
	SP 2.3 Asegurar la transición de productos
Continuidad del servicio (SCON)	
SG 1 Identificar dependencias esenciales del servicio	SP 1.1 Identificar y priorizar funciones esenciales
	SP 1.2 Identificar y priorizar recursos esenciales
SG 2 Preparar la continuidad del servicio	SP 2.1 Establecer planes de continuidad del servicio
	SP 2.2 Establecer capacitación sobre continuidad del servicio
	SP 2.3 Impartir y evaluar la capacitación sobre continuidad del servicio
SG 3 Verificar y validar el plan de continuidad del servicio	SP 3.1 Preparar la verificación y validación del plan de continuidad del servicio
	SP 3.2 Verificar y validar el plan de continuidad

Metas Específicas	Prácticas Específicas
	del servicio
	SP 3.3 Analizar los resultados de la verificación y validación del plan de continuidad del servicio
Prestación del servicio (SD)	
SG 1 Establecer acuerdos de servicio	SP 1.1 Analizar los acuerdos y datos de servicio existentes
	SP 1.2 Establecer acuerdos de servicio
SG 2 Preparar la prestación de servicios	SP 2.1 Establecer el enfoque de prestación de servicios
	SP 2.2 Preparar las operaciones del sistema de servicio
	SP 2.3 Establecer un sistema de gestión de peticiones
SG 3 Prestar servicios	SP 3.1 Recibir y procesar peticiones de servicio
	SP 3.2 Operar el sistema de servicio
	SP 3.3 Mantener el sistema de servicio
Transición del sistema de servicio (SST)	
SG 1 Preparar la transición del sistema de servicio	SP 1.1 Analizar las necesidades de transición del sistema de servicio
	SP 1.2 Desarrollar planes de transición del sistema de servicio
	SP 1.3 Preparar a las partes interesadas para los cambios
SG 2 Desplegar el sistema de servicio	SP 2.1 Desplegar componentes de sistema de servicio
	SP 2.2 Evaluar y controlar los impactos de la transición
Gestión estratégica de servicios (STSM)	
SG 1 Establecer necesidades y planes estratégicos para los servicios estándar	SP 1.1 Recopilar y analizar datos
	SP 1.2 Establecer planes para servicios estándar
SG 2 Establecer servicios estándar	SP 2.1 Establecer propiedades de servicios estándar y niveles de servicio estándar
	SP 2.2 Establecer descripciones de servicios estándar
Monitorización y control de trabajos (WMC)	
SG 1 Monitorizar el trabajo con respecto al plan	SP 1.1 Monitorizar parámetros de planificación del trabajo
	SP 1.2 Monitorizar compromisos
	SP 1.3 Monitorizar riesgos
	SP 1.4 Monitorizar la gestión de datos
	SP 1.5 Monitorizar la involucración de las partes interesadas
	SP 1.6 Realizar revisiones de progreso

Metas Específicas	Prácticas Específicas
	SP 1.7 Realizar revisiones de hitos
SG 2 Gestionar acciones correctivas hasta su cierre	SP 2.1 Analizar problemas
	SP 2.2 Realizar acciones correctivas
	SP 2.3 Gestionar acciones correctivas
Planificación de trabajos (WP)	
SG 1 Establecer estimaciones	SP 1.1 Establecer la estrategia de servicio
	SP 1.2 Estimar el alcance del trabajo
	SP 1.3 Establecer estimaciones de los atributos de productos de trabajo y tareas
	SP 1.4 Definir fases del ciclo de vida
	SP 1.5 Estimar el esfuerzo y el coste
SG 2 Desarrollar un plan de trabajo	SP 2.1 Establecer el presupuesto y el cronograma
	SP 2.2 Identificar riesgos
	SP 2.3 Planificar la gestión de datos
	SP 2.4 Planificar los recursos
	SP 2.5 Planificar los conocimientos y las habilidades que se necesitan
	SP 2.6 Planificar la involucración de las partes interesadas
	SP 2.7 Establecer el plan de trabajo
SG 3 Obtener el compromiso con el plan	SP 3.1 Revisar los planes que afecten al trabajo
	SP 3.2 Conciliar los niveles de trabajo y de recursos
	SP 3.3 Obtener el compromiso con el plan

Anexo IV – Procesos a Gestionar

Funciones, estructura organizacional, puestos de trabajo, perfiles – ciclo de vida

Metas de seguridad de la información

- Contar con un proceso formalmente definido de creación, revisión con una frecuencia dada y actualización según los cambios que realice la organización, de las funciones organizacionales y por ende de la estructura organizacional que incluya su aprobación por parte de la máxima autoridad de la organización.

  Analizar los riesgos de inadecuada separación de funciones, de autorización inadecuada para el acceso a datos y funcionalidades, o para tomar capacitación, entregar equipamiento o permitir la transferencia de información. (**Atención**: Estos cambios organizacionales pueden pasar personal con nivel de responsabilidad (de conducción) a empleado o al revés. Ello implica que cambian los actores en el proceso de autorización.). Este proceso se da en el marco de decisiones estratégicas, tácticas y operativas preexistentes, pero se alimenta de las fluctuaciones del proceso de estrategia organizacional (nuevos mercados, nuevos productos/servicios, fusión, expansión, etc.).

- Contar con un proceso formalmente definido de creación, revisión con una frecuencia dada y actualización según los cambios que se presenten, de puestos de trabajo. Este proceso permitirá contar con una grilla coincidente con las funciones asignadas en la estructura organizacional. Recordar que el personal debe acceder sólo a la información que necesita para ejecutar sus funciones.

  Dicho proceso debe ser transversal a todas las áreas de la organización. Es decir, cuando se crea una nueva área o una nueva función dentro de un área, se deberá actualizar la grilla de puestos de trabajo según corresponda. Este proceso se da en el marco de una estructura y funciones dadas, pero se alimenta de las fluctuaciones del proceso de gestión de funciones y estructura.

- Contar con un proceso formalmente definido de creación, revisión con una frecuencia dada y actualización según los cambios que acontezcan de perfiles y su asignación a los puestos de trabajo. Los perfiles estarán conformados por las aplicaciones y datos a las que debe acceder, así como los servicios que se le otorgarán (correo electrónico, Internet, etc.), dispositivos (smartphone, laptop, etc.), autenticación (firma digital, etc.), tipo de usuario (administrador, común, etc.), tipo de acceso (local, remoto, etc.), transferencia de archivos, acceso a medios de almacenamiento masivo de información (pen-drive, DVD), tarjeta de acceso al edificio/áreas restringidas y todo aquel activo de información del que deberá hacer uso. La definición de datos sólo podrá ser realizada si previamente se ejecutó la clasificación de información, y también la capacitación que debe recibir. Este proceso se da en el marco de puestos de trabajo dados, pero se alimenta de las fluctuaciones del proceso de gestión de puestos de trabajo.

Recursos Humanos – Ciclo de Vida

Metas de seguridad de la información

- Contar con un proceso, de ingreso de personal formalmente definido, de revisión con una frecuencia dada y de actualización de las condiciones, en función de los cambios producidos en leyes, regulaciones y normas.
  Este proceso deberá al menos considerar:
  - ♦ Riesgo de contratar personal inadecuado - Averiguación de antecedentes [57]
  - ♦ Riesgo de responsabilidad - Una vez incorporado formalmente a la organización (firma de contrato o inclusión formal en la planta de personal) deberá firmar el compromiso de confidencialidad de acuerdo al perfil asignado. (Ver las resoluciones de la Dirección Nacional de Protección de Datos Personales).
  - ♦ Riesgo de falta de conocimiento de seguridad - Realización del Curso de Inducción en seguridad de la información. (Ver proceso de Capacitación).

Sólo podrá hacer uso de los activos de información una vez que haya cumplimentado los pasos descritos previamente.

- Contar con procesos de otorgamiento de vacaciones y licencias, registración de ausencias, rotación de personal entre puestos o áreas y de desvinculación formalmente definidos, de revisión con una frecuencia dada y actualización de las condiciones en función de los cambios organizacionales y regulatorios.

  Estos procesos deberán al menos considerar, en caso que corresponda, riesgo respecto de falta de presencia del empleado, su desvinculación, cambios de puestos de trabajo, etc. Posibles controles:

  - ♦ La inhabilitación durante ausencias, vacaciones y licencias.
  - ♦ El cambio de puesto de trabajo y perfil.
  - ♦ La devolución de equipamiento y dispositivos (notebook, token, smartphone, etc.) o bien la desafectación (por ej. la PC de escritorio)
  - ♦ La baja del usuario en caso de desvinculación. Si ésta es por causa de despido, para evitar represalias, impedir accesos.

  Todas estas consideraciones se potencian cuando el personal realiza funciones críticas como el manejo de dinero, de transferencias financieras, bancarias, etc. y de tecnologías de información.

Capacitación

Metas de seguridad de la información

Contar con un proceso de Capacitación formalmente definido, con una revisión con frecuencia dada y actualización en función de los cambios organizacionales y regulatorios. Deberá considerar:

Curso de Inducción: Armado según evaluación de riesgos del puesto, incluyendo los relacionados con tecnologías de la información. Incluye todo lo que la empresa quiere transmitir en general más lo de seguridad de la información. Entrenamiento en el uso de equipamiento (ej. PC y software entre otros). Evita errores y problemas de seguridad.

Curso regular: sobre seguridad (presencial, e-learning, etc.). Boletines, folletos, juegos, etc.

Frecuencia y cuándo: Según evaluación de riesgos para distribución del personal y otros. Ej.: Cambios de equipo, plataformas, servicios, etc.

Patrimonio, inventario, responsabilidades – ciclo de vida

Metas de seguridad de la información (clasificación de activos)

El proceso de clasificación de activos, debe estar ligado al proceso de inventario de la organización y debe indicar claramente cómo se debe proceder para su clasificación. El control de clasificación de activos se impone por la necesidad de establecer el impacto sobre la organización en caso que los mismos sean robados, destruidos, etc. Como en cualquier otro proceso debe tener responsables, que serán los dueños de los mismos, quienes son los que establecerán en virtud de los riesgos, cuáles son los críticos y no críticos. En el caso de hardware y software es asimilable a los inventarios de bienes de uso y en el de los servicios, igual que otros tipos de servicios como el mantenimiento de equipos fabriles.

Los activos informáticos como hardware y software también son Activos Fijos, por lo tanto, deben estar inventariados. No sólo el equipamiento como un todo, sino también sus partes, por ej. los discos (Es posible reemplazar un disco por uno de menor tamaño o desguazar una PC y quitarle la motherboard. Nos vamos a dar cuenta cuando la PC no funcione. Y esto también tiene valor como Activo Fijo, salvo que se mande a pérdida la PC completa). ITIL nos provee de una metodología, como es la CMDB (Configuration Management Data Base) para hacer este mantenimiento. No todas las organizaciones pueden depender de ITIL. Sin embargo, siempre es posible cargarlos en el Sistema de Inventario de la organización o, en el caso de una muy pequeña, por ej. con 5 máquinas, registrarlas en una planilla de cálculo. Lo que no debe pasar es que estén fuera de inventario.

El resto puede ser más dificultoso de clasificar. Por ej., en el caso de los datos se hace más difícil porque aún no se ha ideado una manera de inventariarlos. Qué habría que registrar, cantidad de bases de datos, cantidad de registros o cantidad de bytes? Y cómo los valorizamos. De hecho actualmente, cuando es necesario valorizar el impacto de la pérdida

de una base de datos, los especialistas no se ponen de acuerdo si debieran tomar lo que cuesta recuperarla medido en horas hombre o el valor intrínseco del dato ya que en algunos casos puede ser imposible recuperarlos. Pensemos por ejemplo si hubiéramos decidido despapelizar y luego destruir la documentación en papel (cuando fuera factible).

Cada vez que se adquiere un bien, su riesgo debe ser evaluado y el bien clasificado.

También se clasifican por criticidad en cuanto a los riesgos de falta de disponibilidad o discontinuidad del negocio para las aplicaciones críticas. Éstos no sólo deben ser evaluados desde las fallas del equipamiento y servicios centrales, sino también desde los problemas en el equipamiento de las sucursales, que podrían impedir la atención en una zona determinada. Por ej. fallas en los equipos de telecomunicaciones/servidores de la sucursal, sus end-points, su provisión de energía, etc. También es necesario considerar la provisión del servicio de telecomunicaciones por parte de la empresa telefónica.

En los casos de criticidad, se analizará el riesgo de no disponer de ellos. Esto se realiza a partir de las aplicaciones o documentación crítica.

Tiene competencia, además del área dueña de la información, las áreas de legales.

Utilización de la información en los procesos organizacionales - tácticos y operativos (diseño y desarrollo de productos, generación de satisfacción de demanda, gestión del cambio interno y externo, gestión de las comunicaciones internas y externas) – Ciclo de vida de la información

Metas de seguridad de la información

Además de clasificar los bienes informáticos en críticos, también es necesario considerar la clasificación en datos sensibles según las normas de Protección de Datos Personales en los países que las posean (Por ej., Argentina, Brasil, Chile, Colombia, México y Uruguay). En nuestro país se debe considerar la Ley de Habeas Data (Ley 25.326), su reglamentación y la normativa de la Dirección Nacional de Protección de Datos Personales. La clasificación de datos y documentación también puede extenderse a

aquéllos que son confidenciales, secretos o privados.

Este requerimiento, al igual que el de confidencialidad, (no necesariamente deberían ser los mismos datos) obviamente va a impactar en el diseño de los sistemas ya que será necesario que cada perfil vea los datos que le correspondan en función de la clasificación.

En la aplicación de la Ley de Habeas Data el negocio muchas veces prefiere ahorrar la correcta identificación del cesionario, así como su consentimiento informado, pensando que en caso de sufrir un juicio, seguramente va a tener que pagar menos que el dinero que pierde de ganar en el tiempo que le toma el correcto procedimiento. Sin embargo, luego de varios juicios, su imagen se verá disminuida y es probable que empiece a tener problemas para conseguir datos de sus clientes. Asimismo, se debe tener en cuenta que el organismo de control puede aplicar sanciones de apercibimiento, suspensión, multa, clausura o cancelación del archivo, registro o banco de datos y que también están previstas sanciones penales. (Hay empresas que compran bases de datos para vender un servicio).

En este marco, también deben ser evaluados los riesgos de transferencia de información a terceros.

En todos los procesos organizacionales se evaluará los riesgos asociados al intercambio de información con organizaciones externas (Pedido, dueño define el qué, sistemas el cómo se obtiene, procesamiento lo procesa y se transfiere (con mecanismos de cifrado). Monitoreo: (pedidos contra transferencia) y entre los distintos procesos internos (uso de correo, Intranet, despapelización).

Cuando se hace referencia al intercambio de información se incluye la transferencia de información entre las áreas de tecnologías de información. Sólo producción puede operar datos reales y es necesario considerar los riesgos de posible fuga de información en los procesos de resguardo de información y transferencia al exterior.

Tiene competencia, además del área dueña de la información, las áreas de legales.

Accesos de terceros (aspectos físicos y lógicos)

Metas de seguridad de la información

Contratación de proveedores de productos y/o servicios, alta de nuevos clientes. Cesión de información a terceros (clientes/proveedores/otras organizaciones, por ej. Auditores externos). Mecanismos de entrega.

Es necesario evaluar el riesgo de estos procesos desde la óptica de la Ley de Habeas Data, por lo cual será necesario el trabajo en equipo con el área de Legales.

Luego será necesario analizar los riesgos de los procesos operativos. ¿Cómo se envía o cómo acceden?

Proveedores técnicos y de proyectos: Usuarios externos sin acceso remoto. Seguridad privada, limpieza, mantenimiento de proveedores.

Uso de correo e Internet

Gestión de autorización

Metas de seguridad de la información

Un circuito anterior al otorgamiento de permisos (accesos y equipamiento) a los perfiles. Deriva a generar la autenticación y autorización en la herramienta de administración de seguridad. Es un control preventivo. Luego, se debe implementar el control detectivo (logs) que responde al monitoreo. Se debe tener en cuenta los cambios en los niveles de conducción de los terceros, ya que ello implica cambios en los autorizantes.

Gestión de seguridad física

Metas de seguridad de la información

Ha crecido la idea de convergencia …

http://www.unisys.com/unisys/inc/countrysites/pdf/Convergencia%20de%20seguridad.pdf La seguridad física no sólo tiene que ver con el equipamiento central, sino con las diferentes áreas que utilizan información crítica, sensible, secreta o privada y tiene que ver con los perfiles de los

recursos humanos y los riesgos vistos desde la higiene y seguridad del trabajo.

Gestión Legal

Metas de seguridad de la información

Investigación en leyes, cumplimiento. Auditoría, Legales, Cumplimiento y Fraude input para los procesos.

Funciones más clasificación

Metas de seguridad de la información

Diseño de sistemas y de información (datos + su elaboración) + flujo de documentación

La constatación de que la información es confiable requiere de una buena seguridad. Porqué? Para que sea confiable tiene que poseer integridad, disponibilidad, confidencialidad. Tener en cuenta que dicha confiabilidad impacta sobre las áreas de reporting a casas matrices, organismo de control de otros países, etc. En estos procesos es necesario tener en cuenta la calidad del dato (integridad) ya que la Ley de Habeas Data establece la necesidad de corregir en x cantidad de días frente al requerimiento del titular. Fraude

Adquisición, desarrollo y mantenimiento de aplicaciones

Metas de seguridad de la información

Las aplicaciones son las herramientas con las que cuenta el negocio para ejecutar las diferentes actividades de cada proceso. En consecuencia, deben considerar todos los controles internos de esos procesos más las consideraciones tecnológicas.

Por ellas se comete fraude. Por ellas podemos quedarnos sin operar. Todos los controles operativos (cantidad de registros, de zonas, de operaciones, tamaño de una tabla, etc.) pueden traer falta de disponibilidad. Sus errores también porque pueden dejar de funcionar.

Gestión de infraestructura edilicia

Metas de seguridad de la información

Mudanzas, reestructuraciones, cambios de infraestructura (tiene que ver con lugares para equipos críticos, cableado, tensión, probable extensión de la red, telefonía IP, etc.)

Gestión de hardware y software

Metas de seguridad de la información

Definición infraestructura de seguridad – Análisis de capacidad (tanto de procesamiento como de almacenamiento), adquisición, puesta en producción. Resultado de falta de capacidad, obsolescencia. También end-points

Gestión del cambio (urgencias - actividades ad-hoc)

Metas de seguridad de la información

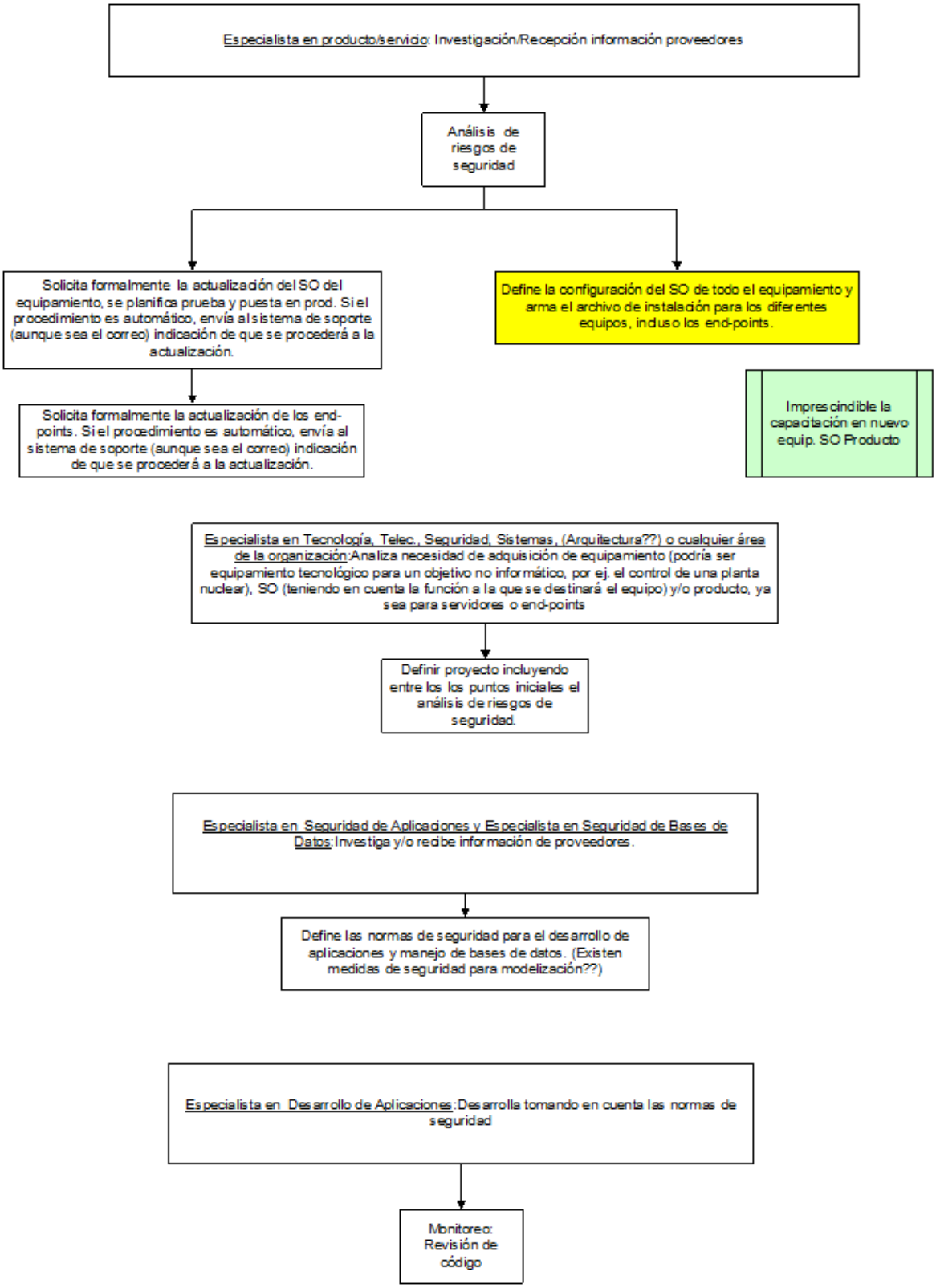
Parte del resto de los procesos.Evaluar riesgos en cambios tecnológicos (Ej. Virtualización, cloudcomputing, cambio de plataforma). En plan estratégico. En layout de oficinas por requerimientos de seguridad física. En cambios de servicios, plataformas, aplicaciones, productos, telefonía, equipamiento, sistemas operativos, metodologías, de arquitectura tecnológica, amenazas y vulnerabilidades. Esto alimenta capacitación y acciones técnicas y/o usuarios. Implica nuevos mecanismos de seguridad.

Necesidad de establecer procesos de investigación

Metas de seguridad de la información

Más allá del aporte de los proveedores, es necesario contar con equipos de investigación en nuevos productos, desarrollo de aplicaciones, aspectos tecnológicos en general.

En la página siguiente se ofrece un esquema respecto de las necesidades en materia de investigación.


Especialista en producto/servicio: Investigación/Recepción información proveedores
Análisis de riesgos de seguridad
Solicita formalmente la actualización del SO del equipamiento, se planifica prueba y puesta en prod. Si el procedimiento es automático, envía al sistema de soporte (aunque sea el correo) indicación de que se procederá a la actualización.
Define la configuración del SO de todo el equipamiento y arma el archivo de instalación para los diferentes equipos, incluso los end-points.
Solicita formalmente la actualización de los end-points. Si el procedimiento es automático, envía al sistema de soporte (aunque sea el correo) indicación de que se procederá a la actualización.
Imprescindible la capacitación en nuevo equip. SO Producto
Especialista en Tecnología, Telec., Seguridad, Sistemas, (Arquitectura??) o cualquier área de la organización: Analiza necesidad de adquisición de equipamiento (podría ser equipamiento tecnológico para un objetivo no informático, por ej. el control de una planta nuclear), SO (teniendo en cuenta la función a la que se destinará el equipo) y/o producto, ya sea para servidores o end-points
Definir proyecto incluyendo entre los los puntos iniciales el análisis de riesgos de seguridad.
Especialista en Seguridad de Aplicaciones y Especialista en Seguridad de Bases de Datos: Investiga y/o recibe información de proveedores.
Define las normas de seguridad para el desarrollo de aplicaciones y manejo de bases de datos. (Existen medidas de seguridad para modelización??)
Especialista en Desarrollo de Aplicaciones: Desarrolla tomando en cuenta las normas de seguridad
Monitoreo: Revisión de código

Bibliografía General

- Corporate Information Security Working Group, Report of the Best Practices and Metrics Teams, Government Reform Committee, United Status House of Representatives, EE.UU, 2004, http://net.educause.edu/ir/library/pdf/CSD3661.pdf, (consultado el 03/07/10)
- Information Technology Governance Institute (ITGI), ISACA, CobiT5, EE.UU
- ISO/IEC 27004:2009 – Information technology – Security techniques – Information security management – Measurement
- Taylor S., Information security maturity assessment, The University of Auckland, Nueva Zelanda, 2005, http://www.security.auckland.ac.nz/InfomationSecurityMaturityAssessment.htm, (consultado el 14/06/10)
- ISACA, Manual de Preparación para el examen de Certificación en Gestión de la Seguridad de la Información (CISM), EE.UU., 2013
- ISM3 Consortium, Information Security Management Maturity Model (ISM3), actualmente es impulsado por el Open Group, razón por la cual su sigla es O-ISM3, 2011
- CMMI® for Acquisition, Version 1.3
- CMMI® for Development, Version 1.3
- Systems Security Engineering Capability Maturity Model (SSE-CMM)

Bibliografía específica

[1] ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements. Actualizada en 2013.

[2] Ione de Almeida, El negocio no es “cliente” de IT, Gartner, 2012, http://www.informationweek.com.mx/columnas/el-negocio-no-es-cliente-de-it/ - (consultado en febrero/2012)

[3] IT Governance Institute (ITGI), Board Briefing on IT Governance, 2nd. Edition, Illinois, 2003, pág. 6

[4] IT Governance Institute (ITGI), Board Briefing on IT Governance, 2nd. Edition, Illinois, 2003, pág. 10

[5] IT Governance Institute (ITGI), Information Security Governance - Guidance for Boards of Directors and Executive Management, 2nd. Edition, Illinois, 2006, pág. 11

[6] IT Governance Institute (ITGI), Information Security Governance - Guidance for Information Security Managers, Illinois, 2008, pág. 25.

También ver http://www.sans.edu/research/security-laboratory/article/convergence-did - (consultado el 15/01/2013)

[7] IT Governance Institute (ITGI), Information Security Governance: Guidance for Information Security Managers, 2nd Edition, Illinois, 2008, pág. 10

[8] Corporate Governance Task Force Report, Information Security Governance – A call to action, 2004, http://www.criminal-justice-careers.com/sites/default/files/resources/InfoSecGov4_04.pdf, (consultado el 26/08/2012)

[9] ISACA, The Business Model for Information Security, Illinois, 2010

[10] CERT - Software Engineering Institute – Carnegie Melon – "Governing for Enterprise Security" –http://www.cert.org/governance/, (consultado el 08/03/2012)

[11] Juhani Anttila Venture Knowledgist Quality Integration Helsinki, Finland www.QualityIntegration.biz [This text was made together with Jorma Kajava and Rauno Varonen of the University of Oulu, Finland and presented as a conference paper at the Euromicro Conference in Rennes, France in September, 2004] http://www.qualityintegration.biz/Rennes2004.html, (consultado el 26/08/2012)

[12] Committe of Sponsoring Organizations of the Treadway Commission (COSO), Los nuevos conceptos de Control Interno, COOPERS & LYBRAND, Madrid, 1997.

[13] Committe of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management Executive Summary, 2004, www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf, (consultado el 16/07/2010)

[14] ISO/IEC 27002:2008 - Information technology — Security techniques — Code of practice for information security controls. Actualizada en 2013

[15] ISO/IEC 27005:2008 – Information technology – Security techniques – Information security risk management. Actualizada en 2011

[16] Westerman, George, Hunter Richard, IT Risk – Turnig Business Threats into Competitive Advantage, Harvard Business School Press, Boston, 2007, págs. 2-7

[17] Westerman, George, Hunter Richard, IT Risk – Turning Business Threats into Competitive Advantage, Harvard Business School Press, Boston, 2007, págs. 6-7

[18] Westerman, George, Hunter Richard, IT Risk – Turnig Business Threats into Competitive Advantage, Harvard Business School Press, Boston, 2007, págs. 10-11. También en http://www.gartner.com/5_about/news/gartner_press/Westerman_intro.pdf, (consultado en agosto 2012)

[19] ISO Guide 73:2009 - Gestión de Riesgos - Vocabulario

[20] Ernst & Young loses 401k information of bank employees - http://www.infosecurity-magazine.com/view/23621/ernst-young-loses-401k-information-of-bank-employees/,2012, (consultado el 22/09/12)

[21] Parent, Michael y Reich, Blaize Horner, Governing Information Technology Risk, Berkeley, University of California, 2009, www.energycollection.us/Board-Charters/Information-Technology/Governing-IT-Risk.pdf, (consultado el 24/09/2012)

[22] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments - Information Security, Maryland, 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf, (consultado el 24/10/2012)

[23] BSI - Migrando de ISO/IEC 27001:2005 hacia ISO/IEC 27001:2013, 2014, http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf - Guía basada en el libro de David Brewer´s "Una introducción sobre ISO/IEC 27001:2013", (consultado el 28/04/2014)

[24] ISO 31000:2009 - Risk management - Principles and guidelines

[25] AMAT Joan M., profesor del Instituto de Empresa de Madrid, autor del prólogo del libro Cuadro de Mando Integral (The Balanced Scorecard), cuyos autores son Kaplan Robert S. y Norton David P., GESTIÓN 2000, España, 1997

[26] Instituto Latinoamericano de la Comunicación Educativa (ILCE), Historia de ISO 9000, http://201.159.130.148/calidadtotal/images/stories/artiso1.pdf, (consultado el 11/08/2012)

[27] Instituto Latinoamericano de la Comunicación Educativa (ILCE), Historia de ISO 9000, http://201.159.130.148/calidadtotal/images/stories/artiso2.pdf, (consultado el 11/08/2012)

[28] Software Engineering Institute (SEI), CMMI for Services, Versión 1.3, Pittsburgh, 2010, págs. 3-4

[29] Software EngineeringInstitute (SEI), CMMI forServices, Versión 1.3, Pittsburgh, 2010, pág. 4

[30] ISO/IEC 15504 - Information technology -- Process assessment

[31] Kybele Consulting, La Certificación por Niveles de Madurez de ISO/IEC 15504 SPICE, http://www.kybeleconsulting.com/articulos/la-certificacion-por-niveles-de-madurez-de-isoiec-15504-spice/, (consultado el 11/08/12)

[32] ISO/IEC 27001:2005 - Information security management systems - Requeriments

[33] ISO/IEC 9001:2008 – Sistemas de gestión de la calidad - Requisitos

[34] de la Villa, Manuel; Ruiz, Mercedes; Ramos, Isabel, Modelos de Evaluación y Mejora de Procesos: Análisis Comparativo, http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-120/paper4.pdf, (consultado el 26/11/2010) - Ruiz, Delmi M. X., Normas ISO 9000 vs. CMMI-SW como estándar de calidad en el desarrollo del software y proceso de obtención de la certificación en cada estándar,

Universidad de San Carlos de Guatemala, 2007, http://biblioteca.usac.edu.gt/tesis/08/08_7983.pdf, (consultado el 26/11/2010)

[35] Scholtz, Tom, Security Program Maturity Timeline Update, Gartner Research, Connecticut, 2009

[36] Chapin, David A. y Akridge, Steven, ¿Cómo Puede Medirse la Seguridad?, ISACA, Illinois, 2005, http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf, (consultado el 24/09/2012)

[37] ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements. Actualizada en 2013

[38] ISO/IEC 27005:2008 - Information technology - Security techniques - Information security risk management. Actualizada en 2011

[39] ISO 31000:2009 - Risk mangement - Principles and guidelines

[40] Software Engineering Institute (SEI), CMMI - Capability Maturity Model Integration

[41] ISO/IEC 27002:2008 - Information technology — Security techniques — Code of practice for information security controls. Actualizada en 2013

[42] ISO/IEC 15504 - Information Technology - Process assessment -- Part 2: Performing an assessment

[43] Scholtz, Tom, Security Program Maturity Timeline Update, Gartner Research, Connecticut, 2009

[44] IT Governance Institute (ITGI), http://www.itgi.org/template_ITGI923a.html?Section=About_ITGI&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=57434, (consultado el 04/05/12)

[45] IT Governance Institute (ITGI), Information Security Governance - Guidance for Boards of Directors and Executive Management, 2nd. Edition, Illinois, 2006, págs. 11 y 12

[46] IT Governance Institute (ITGI), Information Security Governance - Guidance for Boards of Directors and Executive Management, 2nd. Edition, Illinois, 2006, pág. 14, 2006

[47] ITGI, Information Security Governance: Guidance for Information Security Managers, 2nd Edition, Illinois, 2008, pág. 25

[48] Corporate Governance Task Force Report - Information Security Governance – A call to action, www.cyberpartnership.org/InfoSecGov4_04.pdf, 2004, (consultado el 05/05/12)

[49] John P. Hopkinson, THE RELATIONSHIP BETWEEN THE SSE-CMM AND IT SECURITY GUIDANCE DOCUMENTATION, http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CEUQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.198.2131%26rep%3Drep1%26type%3Dpdf&ei=uXkpULDxF6Xr0gHKvoDICw&usg=AFQjCNHWgtffPU7

5kX2-8N1A08FFKfKP6A&sig2=l9ApooZ_rOxZxNkhFERffQ, (consultado el 13/08/12)

[50] Geoffrey Karokola, Stewart Kowalski and Louise Yngström, Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View, Department of Computer and Systems Sciences Stockholm University/Royal Institute of Technology Forum 100, SE-164 40 Kista, Stockholm, Sweden, 2011, su.diva-portal.org/smash/get/diva2:469623/FULLTEXT01, (consultado el 24-09-2012)

[51] Steve Wexler, Raising The Bar: Security Comes of Age With O-ISM3, Network Computing, EEUU, 2011, http://www.networkcomputing.com/wan-security/raising-the-bar-security-comes-of-age-wi/229500460, (consultado el 24-09-2012)

[52] Software Engineering Institute (SEI), CMMI for Services, Versión 1.3, 2010, pág. 9

[53] Software Engineering Institute (SEI), CMMI for Services, Versión 1.3, 2010, pág. 7

[54] Software Engineering Institute (SEI), CMMI for Services, Versión 1.3, 2010, pág. 11

[55] Software Engineering Institute (SEI), CMMI for Services, Versión 1.3, Pittsburgh, 2010, págs. 21-22

[56] Software Engineering Institute (SEI), CMMI for Services, Versión 1.3, Pittsburgh, 2010, págs. 26-27

[57]iProfesional.com, Selección de personal: qué "antecedentes" ponen bajo la lupa empresas y consultoras, Fecha de emisión: 07/05/2010, http://management.iprofesional.com/notas/98173-Seleccion-de-personal-que-antecedentes-ponen-bajo-la-lupa-empresas-y-consultoras.html, Fecha de consulta: 15/10/2012