Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

NORMAS ISO DE SEGURIDAD DE LA INFORMACION

Abstract

Marzo 2014

SEGURIDAD DE LA INFORMACIÓN

Especialmente en los últimos años se viene dando un desarrollo sostenido de las TIC, es decir las Tecnologías de la Información referidas a los sistemas de computación y a los medios de intercambio local y remoto de la información.

Tales tecnologías se han convertido en activos estratégicos para las empresas y las propias personas, facilitando el uso de los datos de unas y otras a lo largo de todo el mundo.

Puesto que la problemática parece a primera vista estar centrada en la tecnología, se han ido formando una cantidad de especialistas en **seguridad informática**, es decir con conocimientos de las tecnologías propias de sistemas de computación, redes y comunicaciones.

Pero también pueden producirse eventos debido al uso inadecuado y descuido no sólo de los sistemas informáticos, sino también de otras fuentes de datos por parte de quienes manejan la información.

De hecho, las estadísticas muestran que tales situaciones pueden causar mayor daño que las propias de la tecnología. Y aunque se tomen medidas de seguridad ocurre que muchas de estas medidas plantean cambios de conducta que pueden entrar en conflicto con los esquemas de las personas por su resistencia natural a los cambios y los mecanismos de defensa que se disparan.

Esta mayor dependencia de la ***gente*** (1) amerita un replanteo del escenario original.

Además, los ***riesgos de seguridad de la información*** implican un panorama corporativo integral que lleva incluso a considerar cómo es una organización, las interrelaciones del organigrama y de la realidad, y la cultura corporativa, la que concibe la operatividad de una empresa como una *malla* organizativa especialmente en las nuevas estructuras matriciales.

De esta manera se puede concluir que para una gestión confiable y segura que permita concretar las metas y objetivos de una organización, además de los recursos técnicos habrá que considerar la gente, los procesos y funciones de negocio.

Precisamente en parte por las circunstancias señaladas, últimamente se viene dando el cambio de denominación de ***seguridad informática*** a ***seguridad de la información*** (2), con una visión más amplia de un marco de riesgos de negocios respecto de la perspectiva tradicional de seguridad técnica o de IT.

En la práctica, lo anterior muestra al menos lo limitado del paradigma tan difundido que la seguridad es una cuestión técnica (Figura 1).

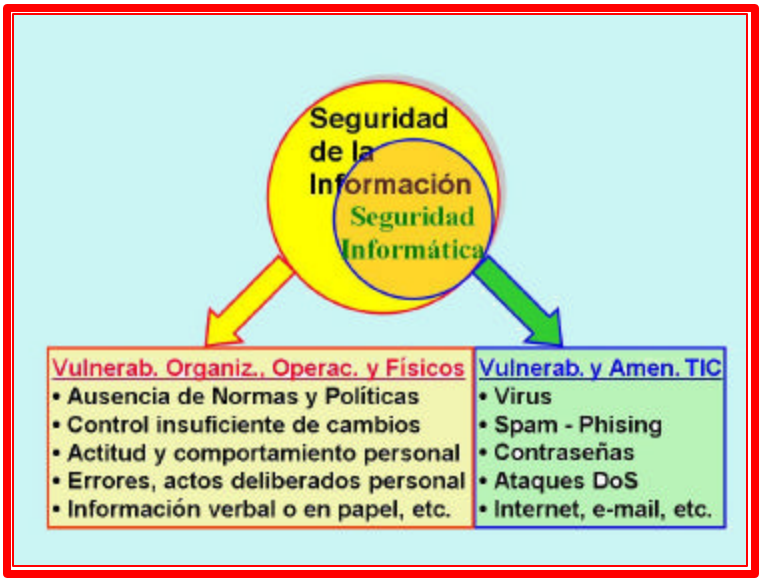

Figura 1

SEGURIDAD DE LA INFORMACIÓN Y GOBIERNO CORPORATIVO

Las conclusiones anteriores no responden solamente a lo comentado al principio, sino que tienen fuerte fundamento incluso desde hace más de diez años.

El nuevo enfoque comentado responde también a los conceptos del **Gobierno Corporativo** o **Corporate Governance**, es decir, cómo dirigir, administrar o controlar adecuadamente una empresa.

Los antecedentes en tal sentido se encuentran en la **OECD** (Organización para la Cooperación y Desarrollo Económico, **OCDE** en español) que estableció las ***responsabilidades del Directorio*** de una empresa como uno de los seis **Principios de un Gobierno Corporativo**.

Ya en el encabezamiento de dicho Principio se dice que el marco de trabajo del Gobierno Corporativo debiera asegurar el *monitoreo* de las funciones de la gerencia..

La mención del monitoreo por parte del directorio indica una separación entre ***gobierno y gestión***, donde el **gobierno** de un organización es función del ***directorio*** y la **gestión**, de la ***gerencia ejecutiva***.

Por su parte, el concepto de seguridad de la información ha venido evolucionando con el tiempo. Así fue como la Seguridad de la Información fue pasando de lo ***técnico*** a la ***gestión*** y de aquí a la ***institucionalización*** bajo normas universales, para actualmente fortalecer la toma de conciencia que ***la seguridad es parte de los negocios***, puesto que la información es un activo corporativo crítico para mantener sustentables las operaciones, entroncándose así en el paradigma del **Corporate Governance**,

De esta manera, el aseguramiento de la información debe responder también a un esquema de gobierno, **Gobierno de la Seguridad de la Información**, tema sobre el que volveremos más adelante.

Por otra parte, el mismo Principio mencionado establece que el Directorio tiene que cumplir con ciertas **funciones claves**, entre ellas la de revisar y conducir la "***política de riesgos***", y determinar los "***tipos y nivel de riesgos***" que una empresa está dispuesta a aceptar en el cumplimiento de sus objetivos.

El tema de la política de riesgos corporativos se puede ampliar aplicando cierta forma de clasificación o taxonomía, como indican las **Guías de Seguridad** también de la **OECD**.

Estas Guías también establecen sus propios **Principios**, dos de los cuales importan especialmente.

Uno se refiere a la ***Concientización*** donde aparecen las personas como individuos y como grupos, es decir la *gente* como ya mencionáramos antes.

El otro Principio considera la ***Valuación de riesgos***, en base a *amenazas* y *vulnerabilidades*, y establece que los factores que determinan los riesgos pueden ser de carácter ***tecnológico, físico y humano***.

Todo este conjunto señala en la práctica cuatro tipos de riesgos, los tradicionales ***riesgos técnicos*** *de sistemas IT, los* ***riesgos organizacionales****, los* ***riesgos operacionales*** *y los* ***riesgos de carácter físico****,* como producto de las correspondientes *vulnerabilidades.*

Y, por cierto, a diferencia de las vulnerabilidades técnicas propias de las TIC que más bien responden a un esquema blanco-negro o a lo sumo de tres niveles, las vulnerabilidades organizacionales y operacionales se extienden en una amplia gama de grises, muy relacionada con el comportamiento humano y las opiniones subjetivas de las personas, la cultura empresarial, la forma de comunicación, la resistencia al cambio, etc.

NORMAS BASICAS DE SEGURIDAD DE LA INFORMACIÓN

En la década pasada se han venido desarrollando varias normas relacionadas con la seguridad de la información siguiendo diferentes enfoques que hacen al conjunto, y ya en los últimos años la visión para el usuario puede verse como mucho más integral

De todas las normas publicadas de seguridad de la información dos de ellas constituyen las bases de todo el conjunto.

Son la **ISO 27002** (anteriormente ISO 17799 y ésta a su vez derivada de la BS 7799-1) y la **ISO 27001** (que evolucionó a partir de la BS 7799-2).

Las versiones 2005 de ambas normas fueron actualizadas a fines de 2013.

En forma similar a otras normas (como la de Calidad, Ambiental, etc.), se puede certificar el correspondiente **Sistema de Gestión de Seguridad de la Información, SGSI**.

Otras dos normas que expresan ***recomendacione**s* pueden usarse en el proceso de implementación de medidas de seguridad de la información como complemento de las dos normas anteriores. Se trata de las **ISO 27005** de Riesgos y la **ISO 27004** de Métricas.

A continuación se comentan las principales características de las cuatro normas citadas (Ver Nota al final).

NORMA ISO 27002:2013

La ISO 27002 es una guía de ***recomendaciones*** de buenas prácticas para la gestión de seguridad de la información.

Cubre no sólo la problemática IT sino que hace una aproximación holística a la seguridad corporativa de la información, extendiéndose a todas las funcionalidades de una organización en cuanto a que puedan afectar la seguridad de la información.

Para ello la norma, en la última versión publicada en octubre de 2013 define para su selección un total de 114 controles generales de seguridad a partir de 35 objetivos de control estructurados en 14 áreas, 4 de ellas técnicas, 9 de gestión y 1 de seguridad física.

La ISO 27002 está redactada bajo la forma verbal "should", un término presente en otras normas **ISO** y también del **IETF** y el **IEEE** que, por convención, expresa una forma condicional que no implica imposiciones.

Es así como la norma, como ya se dijo, hace precisamente ***recomendaciones*** y por lo tanto no establece requisitos cuyo cumplimiento pudieren certificarse, sino simplemente una serie de controles que pudieren ser necesarios implementar.

En la Tabla 1 se pueden ver las Cláusulas/Capítulos y la Numeración correspondiente, así como los Objetivos de Control de cada cláusula de la ISO 27002:2013.

Tabla 1

#	Cláusulas	Objetivos de Control
0	**Introducción**	
1	**Alcance**	
2	**Referencias normativas**	
3	**Términos y definiciones**	
4	**Estructura de esta norma**	
5	**Políticas de Seguridad de la Información**	5.1 Dirección de la gestión de la seguridad de la información.
6	**Organización de la seguridad de la información**	6.1 Organización interna 6.2 Dispositivos móviles y teletrabajo
7	**Seguridad de los recursos humanos**	7.1 Previo a la contratación 7.2 Durante el empleo

		7.3 Terminación y cambio de empleo
8	**Gestión de activos**	8.1 Responsabilidad por los activos. 8.2 Clasificación de la información. 8.3 Manejos de los medios de almacenamiento
9	**Control de acceso**	9.1 Requerimientos de negocios del control de accesos. 9.2 Gestión de acceso de los usuarios. 9.3 Responsabilidades de los usuarios. 9.4 Control de acceso de sistemas y aplicaciones.
10	**Criptografía**	10.1 Controles criptográficos
11	**Seguridad física y ambiental**	11.1 Áreas seguras 11.2 Seguridad del equipamiento.
12	**Seguridad de las operaciones**	12.1 Procedimientos y responsabilidades operacionales. 12.2 Protección contra el malware. 12.3 Respaldo. 12.4 Registro y monitoreo 12.5 Control del software operativo. 12.6 Gestión de las vulnerabilidades técnicas. 12.7 Consideraciones de la auditoría de sistemas de información.
13	**Seguridad de las comunicaciones**	13.1 Gestión de la seguridad de redes. 13.2 Transferencia de información.
14	**Adquisición, desarrollo y mantenimiento de sistemas**	14.1 Requerimientos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.3 Pruebas de datos.
15	**Relaciones con proveedores**	15.1 Seguridad de la información en las relaciones con proveedores. 15.2 Gestión de entrega de servicios de proveedores.
16	**Gestión de incidentes de seguridad de la información**	16.1 Gestión de incidentes y mejoras de la seguridad de la información.
17	**Aspectos de seguridad de la información en la Gestión de Continuidad de Negocios**	17.1 Continuidad de la seguridad de la información. 17.2 Redundancias.
18	**Cumplimiento**	18.1 Compromiso con los requerimientos legales y contractuales. 18.2 Revisiones de la seguridad de la información.

NORMA ISO 27001:2013

En contraposición con la ISO 27002, la ISO 27001 usa la expresión "shall", otro término convencional, en este caso para expresar mandato u obligación.

De esta manera la ISO 27001 especifica los ***requisitos*** para establecer un plan de seguridad constituido por un **Sistema de Gestión de Seguridad de la Información, SGSI** (o **ISMS**, por su nombre en inglés) dentro del contexto de los riesgos totales de negocios de una empresa.

En definitiva, las especificaciones y las implementaciones correspondientes hacen que tanto la auditoría como la certificación se hagan con referencia a la ISO 27001.

Así las cosas, para fines de Febrero de 2014 se habían emitido más de 20.000 certificaciones correspondientes a organizaciones de 100 países diferentes.

Claro que prácticamente todas estas certificaciones lo fueron con la versión 2005, por lo que en un lapso de dos años tendrán que ser actualizadas con la última versión que estamos comentando.

En esta nueva versión de 2013, el cambio más evidente está en la estructura de la norma, ya que se adaptó a la estructura definida en el **Apéndice 2** del **Anexo SL** del **Suplemento Consolidado de Procedimientos específicos para ISO** de la **Parte 1 de las Directivas ISO/IEC**.

Con ajuste al **Anexo SL** (anteriormente **ISO Guide 83**) todas las normas de ***sistemas de gestión*** tienen o tendrán una estructura común, con idéntico texto principal, salvo en el Apartado **Operación** referido en gran parte a las cuestiones específicas de cada norma, y que luego comentaremos más en detalle

De esta manera se facilita trabajar con más de un **Sistema de Gestión**, lo que permite una ***integración*** más simple con otras normas similares de Sistemas de Gestión tales como la ISO 9001, la ISO 20000-1 y la ISO 14001.

Por otra parte, la norma hace hincapié en que el SGSI debe proteger la **Confidencialidad, Integridad y Disponibilidad (CIA)** de la información, aplicando un proceso de gestión de riesgos de forma tal que proporcione a las *partes interesadas* confianza en que los riesgos están gestionados adecuadamente.

Un nuevo concepto que se incorpora es el de las ***partes interesadas***, que incluye no sólo a los accionistas o los propietarios de una empresa sino a todas las personas interesadas directa o indirectamente en la organización (shareholders), así como las propias autoridades legales o regulatorias.

Los nuevos Capítulos/Cláusulas, su numeración y apartados se visualizan en la Tabla 2:

Tabla 2

#	Cláusulas	Apartados
0	**Introducción**	
1	**Alcance**	
2	**Referencias normativas**	
3	**Términos y definiciones**	
4	**Contexto de la organización**	4.1 Comprensión de la organización y su contexto. 4.2 Comprensión de las necesidades y expectativas de las partes interesadas. 4.3 Determinación del alcance del sistema de gestión de continuidad de negocios 4.4 Sistema de Gestión de Continuidad de Negocios
5	**Liderazgo**	5.1 Liderazgo y compromiso. 5.2 Compromiso gerencial. 5.3 Política. 5.4 Roles, responsabilidades y autoridades de la organización.
6	**Planificación**	6.1 Acciones para atender los riesgos y las oportunidades. 6.2 Objetivos de continuidad de negocios y planes para lograrlos.
7	**Soporte**	7.1 Recursos 7.2 Competencia 7.3 Concientización 7.4 Comunicación 7.5 Información a documentar
8	**Operación**	8.1 Planificación y control operacional. 8.2 Análisis de impactos en los negocios y valuación de riesgos. 8.3 Estrategia de continuidad de negocios. 8.4 Establecimiento e implementación de los procedimientos

		de continuidad de negocios. 8.5 Ejercicios y pruebas
9	**Evaluación del desempeño**	9.1 Monitoreo, medición, análisis y evaluación 9.2 Auditoría interna. 9.3 Revisión gerencial.
10	**Mejoramiento**	10.1 No conformidades y acciones correctivas. 10.2 Mejoramiento continuo.

Quizás el detalle más significativo en esta nueva versión es que no hay mención específica del modelo **PDCA**, aunque hay todo un Capítulo (el 10) dedicado al ***Mejoramiento*** del proceso.

De cualquier manera, esto no significa que ya no deba usarse el PDCA, sino simplemente que se hace lugar también a otros modelos de **mejoramiento continuo**.

Una opción podría ser el **Six Sigma** que trabaja con el ciclo **DMAIC** (*definir* las oportunidades, *medir* el rendimiento, *analizar* las oportunidades, y *mejorar* y *controlar* el rendimiento).

También podría llegarse a aplicar el **TQM**, es decir la ***Gestión de Calidad Total***.

Además, en la nueva versión se ha ampliado el tema del ***tratamiento de riesgos*** alineándolo con la **ISO 31000** referida a la ***Gestión de Riesgos*** de distinta índole (no sólo de seguridad de la información) que pueden afectar una organización.

Por lo demás, obviamente el Anexo A refleja los controles correspondientes a la nueva versión de la ISO 27002, listando los objetivos de control y controles que detalla dicha norma.

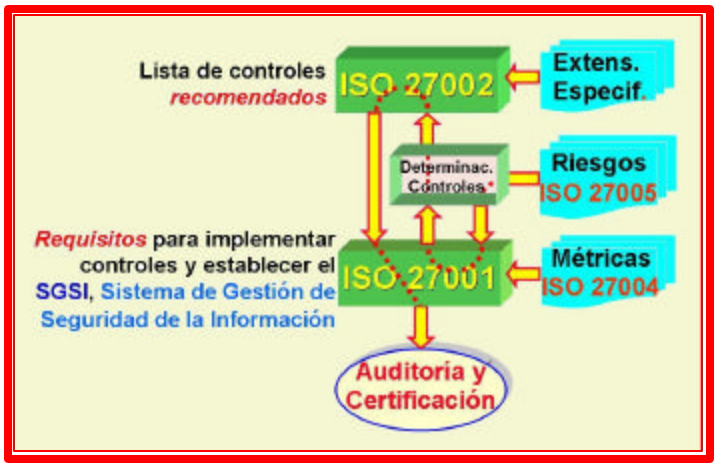

Figura 2

Implementación

El proceso de implementación bajo la ISO 27001 comienza con la determinación del **Alcance** del proyecto, que puede extenderse a todas las actividades de una empresa, o bien a un servicio o área determinados.

A continuación se debe redactar una **Política General**, un documento corto pero con el detalle concreto del Alcance y demás consideraciones pertinentes, y que debe ser refrendado por las autoridades máximas de la empresa para poder luego establecer las responsabilidades correspondientes.

La selección de controles responde a los resultados de una adecuada **valuación de los riesgos** a que están sujetos los activos a proteger.

En este punto, la ISO 27001 no impone una forma determinada de realizar dicha valuación, pudiéndose recurrir a alguno de los diferentes métodos tanto de libre uso como de herramientas comerciales, aunque es recomendable el marco de trabajo dado por la norma ISO 27005 que se

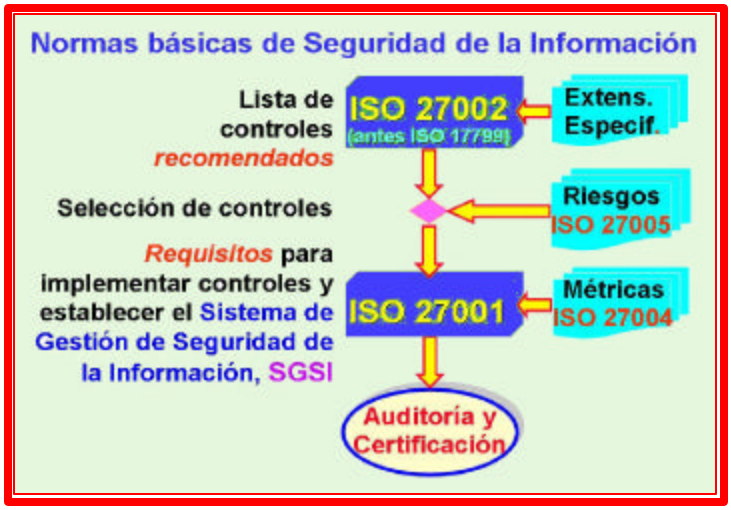

Figura 3

comenta más adelante.

Los resultados de la valuación de riesgos se contrastan con la situación de seguridad existente en un proceso de pre-auditoría que generalmente se realiza por medio de un *análisis gap*.

De esta manera, ahora los riesgos encontrados deben dar lugar directamente a la determinación de los controles correspondientes, controles que recién ***después*** se compararán con los del Anexo A de la ISO 27001 (Figura 2).

La primera parte del párrafo anterior puede resultar complicada salvo para especialistas con mucha experiencia. Sin embargo, la Nota del inciso b) del punto 6.1.3 de la ISO 27001:2013 acepta que los controles a determinar pueden ser de “cualquier origen”.

En la práctica, la Nota mencionada facilita mantener el tan conocido proceso anterior de trabajo, que consiste en comparar primero los riesgos encontrados con los controles de la ISO 27002, y los controles así seleccionados son los que luego se implementan conforme la ISO 27001 (Figura 3).

De una u otra forma, el resultado de esta parte del proceso debe producir la **Declaración de Aplicabilidad (SoA)** que, por cierto, debe incluir todos los controles implementados o no con los correspondientes motivos.

También, el **SGSI** resultante puede someterse a auditoría y el proceso de certificación.

Análisis y Tratamiento de los Riesgos

En la práctica, el análisis de riesgo puede realizarse a partir de dos enfoques diferentes, considerando las variables con que ocurren los incidentes, o bien estimando la protección que requieren los recursos con sus debilidades y los factores que pueden afectarlos, según se puede observar en la Tabla 3.

Tabla 3

Método	Descripción	Componentes	Descripción
Leading	Por los factores o **Entidades** involucradas en el análisis del aseguramiento corporativo	***Activos* o recursos**	Valor que representan para los procesos de negocio de la empresa.
		Vulnerabilidades	Que tengan esos Activos.
		Amenazas	Que puedan explotar dichas vulnerabilidades
Lagging	Por las **Pérdidas** que ocasiona un *incidente* de seguridad conforme datos históricos propios o de terceros.	***Frecuencia de ocurrencia***	De cada incidente
		Impacto	Monetario que causa el incidente al producirse.

En este análisis hay que tener en cuenta que los diferentes tipos de vulnerabilidades y los riesgos correspondientes ya comentados antes.

Y específicamente, en el caso de las vulnerabilidades organizacionales y operacionales, es recomendable para su determinación trabajar con algún método de investigación prospectiva como Delphi, por medio de una encuesta con una serie de preguntas ajustadas al objetivo, complementada en este caso por entrevistas personales para establecer el valor de las opiniones vertidas en las respuestas a dicha encuesta.

El objetivo de los controles determinados obviamente responde a reducir algunos de los riesgos a valores residuales aceptables. Para esto se usan salvaguardas o contramedidas adecuadas cuya efectividad puede medirse bajo el marco de trabajo de la norma **ISO 27004** que también se comenta más adelante.

Una de las formas básicas de mitigar riesgos es por medio de normas de uso, controles de seguridad y procedimientos. Adicionalmente, muchas de las salvaguardas para los riesgos técnicos se basan en software/productos de seguridad adecuados.

En cambio, con otros tipos de riesgos especialmente los operacionales, la mitigación de los mismos se puede lograr a partir de planes de concientización y capacitación, controlados por medio de métricas.

Se puede medir el resultado de un programa de concientización o capacitación encuestando a los que asistieran al programa conforme la metodología Delphi ya menconada.

Para el caso se pueden aplicar técnicas de **Psicología Social** por medio de cuestionarios sobre los temas tratados conforme tres criterios que conforman lo que denominamos el **Factor Gente** (1): **Conocimiento, Actitud y Comportamiento**.

Así puede medirse la adhesión o aceptación no sólo del ***conocimiento*** transferido, sino también de la ***actitud*** que toman los usuarios respecto de dicho conocimiento y del ***comportamiento*** que asumen cuando tienen que aplicar dicho conocimiento.

NORMA ISO 27005

Esta norma se refiere a la valuación y gestión de riesgos y la última versión es de 2011. En gran parte se basa en la **ISO 13335**. Igualmente ha tomado varios temas relacionados con el ciclo de vida de la gestión de riesgos conforme la norma británica **BS 7799-3**, que si bien también trata de los riesgos tiene un enfoque especial en los negocios.

Estrictamente la **ISO 27005** hace ***recomendaciones*** respecto de un marco de referencia para el análisis y gestión de riesgos, permitiendo el uso de alguno de los muchos productos comerciales y gratuitos al efecto.

Por otra parte, esta norma reconoce el formato y diagrama de flujo de la **ISO 31000** ya mencionada.

De cualquier manera, el alineamiento con la ISO 31000 no significa que la **ISO 27005** de Riesgos de Seguridad de la Información pierda relevancia, ya que su uso se puede justificar puesto que esta norma trata especialmente los ***riesgos técnicos o de IT***, mientras que la ISO 31000 provee un marco de trabajo más adecuado para los ***riesgos de negocios***.

Si bien la ISO 27005 promueve el cálculo de riesgos por el método de las frecuencias de ocurrencia e impactos, igualmente habla de activos, amenazas y vulnerabilidades, incluyendo incluso tres de sus Anexos con listados y tablas al efecto.

También introduce el concepto de ***activos dependientes***, lo que implica que el valor de un activo pueda influir en el valor de otro activo, aumentándolo cuando el valor del activo dependiente sea mayor que el valor del activo del cual depende.

Adicionalmente, en uno de los Anexos de la norma se establece que, además de los tres parámetros básicos de seguridad **(CIA)** que establece la ISO 27002, se debieran considerar también la ***Responsabilidad*** (en cuanto a rendir cuentas de las acciones), la ***Confiabilidad***, la ***Autenticación*** y su complemento del ***No-Repudio***.

NORMA ISO 27004

Esta norma es una guía que especifica las mediciones y su uso, como base de información del SGSI para la toma de decisiones al respecto.

Para ello estipula un modelo de ***atributos de objetos de seguridad*** y formas de su cuantificación y medición correspondientes a la efectividad del SGSI y de los controles implementados.

El proceso parte de ***mediciones*** básicas, de las que se derivan ***métricas*** las que, a su vez, combinadas o incluso con otras mediciones constituyen ***indicadores*** que con criterios asociados de decisión permiten la toma de decisiones en cuando a la efectividad deseada.

Métricas

Si bien esta norma no ofrece detalles de las métricas a usar, se pueden mapear los controles ISO 27002 a controles NIST en forma inversa a lo presentado por el estándar **NIST 800-53**, y luego optar por las métricas que se encuentran en **NIST 800-55** (3).

El **GQM *(Métricas de Metas por Cuestionarios)*** es otra herramienta que permite definir métricas a partir de un modelo de tres niveles dados primero por el establecimiento de metas, luego preguntas específicas respecto de los motivos, atributos, contexto y punto de vista sobre el proceso que se mide, y finalmente la obtención de las respuestas correspondientes que son las métricas deseadas.

Adicionalmente hay que mencionar un importante mecanismo adecuado para el control y medio de gestión de dichas medidas de seguridad, y que facilita la toma de decisiones para las mejoras correspondientes.

Se trata del **Balanced Scorecard (BSC)** (4) que, además de su funcionalidad estratégica, genera ***valor*** para el desarrollo de los procesos corporativos actuando de puente entre las áreas de seguridad de la información y la de negocios.

LA SERIE DE NORMAS ISO 27K

Las normas ISO 27002 e ISO 27001 constituyen el núcleo de toda una serie, conocida como **27K**, de más de treinta normas ISO 27000, de las cuales ya se han publicado 22 (tres de ellas en forma parcial), ofreciendo el conjunto una estructura auto-consistente e integral.

Algunas de dichas normas (Figura 4) son extensiones a la ISO 27002 para la seguridad en áreas específicas. Otras detallan indicaciones y especificaciones bajo la órbita de la ISO 27001. Finalmente un par de ellas se refieren a la auditoría y certificación.

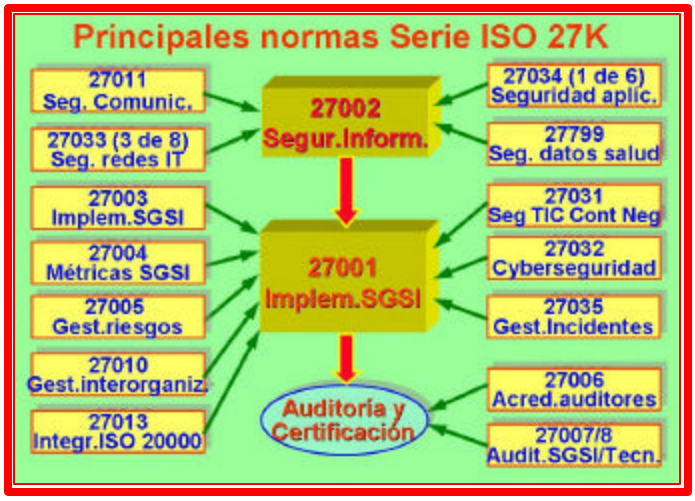

Figura 4

Sigue un listado de las normas *publicadas* para febrero de 2014.

- **ISO 27000**: Define el vocabulario técnico específico. Publicada en Enero de 2014.
- **ISO 27001**: Nueva versión publicada en 2013.
- **ISO 27002**: Nueva versión publicada en 2013.
- **ISO 27003**: Guía general de implementación de la serie. Publicada en Febrero de 2010.
- **ISO 27004**: Métricas, ya comentada, fue publicada en 2009.
- **ISO 27005**: Gestión de riesgos, ya comentada; la última versión fue publicada en 2011..
- **ISO 27006**: Requerimientos para la acreditación de entidades de auditoría y certificación de SGSI. Publicada en 2007.
- **ISO 27007**: Auditoría del SGSI, derivada de ISO 19011. Publicada en 2011.

- **ISO 27008**. Auditoría de la Gestión de la Seguridad de la Información (no del *Sistema* propiamente dicho de Gestión de Seguridad de la Información, que es tema de la ISO 27007) en cuanto a los controles implementados.

- **ISO 27010**: Comunicaciones intersectoriales y entre organizaciones. Publicada en 2012.

- **ISO 27011**: Extensión de la ISO 27002 en cuanto a la gestión de seguridad en telecomunicaciones. Publicada en 2008.

- **ISO 27013:** Guía para la implementación sucesiva o combinada de la ISO 27001 con la ISO 20000 (ITIL). Pensada para manejar los puntos de solapamiento en cuanto a seguridad TIC del ITIL con la ISO 27001. Publicada en 2012.

- **ISO 27014** Gobierno de Seguridad de la Información. Se comenta por separado más adelante.

- **ISO 27015**: Servicios Financieros. Publicada en 2012.

- **ISO 27019**: Sistema de Control de Procesos de las empresas de energía. Publicada en 2013.

- **ISO 27031**: Preparada para la seguridad IT en la Continuidad de Negocios. Publicada en 2011.

- **ISO 27032**: Guía de ciberseguridad. Publicada en 2012.

- **ISO 27033**: Extensión de la ISO 27002 en cuanto a Seguridad de redes IT, evolución a partir de la ISO 18028. Dividida en 7 partes, cinco de las cuales ya se han publicado.

- **ISO 27034**: Extensión de la ISO 27002 en cuanto a la seguridad en las aplicaciones. Publicada la primera parte de un total de 6.

- **ISO 27035:** Gestión de incidentes basada en la ISO 18044. Publicada en 2011.

- **ISO 27036:** Relaciones con proveedores. Cuatro partes publicada una de ellas.

- **ISO 27799**: Extensión de la ISO 27002 para cubrir los aspectos referidos a la protección de la información personal de salud. Publicada en 2008.

Tabla 4 – Otras Normas de la Serie 27K

Norma	Tema
ISO 27016	Economía de la gestión de seguridad de la información
ISO 27017	Aspectos de seguridad de la información en la computación en la nube
ISO 27018	Aspectos de privacidad en la computación en la nube
ISO 27037	Guía para evidencia digital.
ISO 27038	Especificaciones para redacción digital
ISO 27039	Sistemas de detección y prevención de intrusiones
ISO 27040	Guía sobre seguridad del almacenamiento
ISO 27041	Guía sobre el aseguramiento para los métodos de investigación de evidencia digital
ISO 27042	Guía sobre análisis e interpretación de la evidencia digital
ISO 27043	Guía sobre los principios y procesos de investigación de la evidencia digital.

Adicionalmente a todas las normas comentadas antes, la serie 27K incluye otras diez normas previstas y/o en proceso, y que se muestran en la Tabla 4.

GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

En 2013 se liberó la nueva norma **ISO 27014** de ***Gobierno de Seguridad de la Información***.

Esta norma completa la idea original de las normas **ISO** de **Seguridad de la Información** en cuanto a su entroncamiento en el concepto del **Gobierno Corporativo** comentado antes.

El concepto básico parte de que el aseguramiento de la información debe responder a un esquema de **gobierno**, teniendo en cuenta que no es lo mismo **gobierno** que **gestión**.

Ya comentamos que en una organización típica el **directorio** establece el **gobierno** de la misma y las directivas de gestión, monitoreando dicha **gestión**, a cargo del personal de la **gestión ejecutiva**.

Efectivamente, en el ámbito de la seguridad de la información se puede decir en primer lugar que el área de cobertura del concepto **gobierno** es el del **directorio**, ***governing body*** y en algunos casos de la **alta gerencia, *top management***, términos ambos definidos en la reciente **ISO 27000:2014**.

Y, complementariamente, se tiene que el área de cobertura del concepto **gestión** es el de la **gerencia ejecutiva, *executive management***, de nuevo según la **ISO 27000:2014.**

A partir de este paradigma, la **ISO 27014** define el escenario bosquejado estableciendo el ***marco de trabajo*** del gobierno de Seguridad de información para todas las normas de la serie 27k.

Además, la norma habla en forma taxativa del **Information Security Governance** integrado al **Corporate Governance**.

Por otra parte, el **Gobierno de la Seguridad de la Información** está separado del **Gobierno IT**; sólo hay interacción a nivel de la **seguridad IT** (Figura 5).

Esta situación es coherente con la diferencia ya comentada entre **Seguridad de la Información** y **Seguridad Informática**.

Además, en el **Gobierno de la Seguridad de la Información** están marcadamente diferenciados los conceptos de **gobierno,** a cargo del directorio, y la **gestión**, que realiza el personal gerencial.

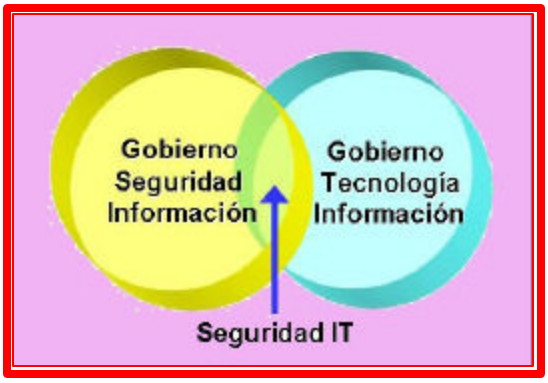

Figura 5

OTRAS NORMAS Y ESTÁNDARES

Algunas normas que no son específicamente de seguridad de la información pueden aportar complementos de importancia en una implementación.

ISO 31000

Seguramente la más transcendente es la **ISO 31000** para la **Gestión de Riesgos**. Esta norma establece Principios y ofrece guías para ayudar a gestionar cualquier tipo de riesgo corporativo con efectividad y se basa en la norma **AS/NZS 4360** de 2004.

En nuestro caso particular, la última versión de la **ISO 27005**, como ya se dijo, está adaptada a la ISO 31000, por lo que es importante considerar sus principales características.

En primer lugar, la ISO 31000 establece un marco de trabajo o estructura de soporte (framework) cuyo objetivo es integrar el proceso de gestión de riesgos con el gobierno corporativo.

Por cierto esta relación con el Corporate Governance, visto al principio, refuerza la importancia de las decisiones estratégicas de alto nivel con referencia a la seguridad de la información.

Por otra parte, el riesgo se ha venido tratando hasta ahora como la posibilidad que algo ocurra que tenga un impacto en los objetivos. A partir de la ISO 31000 el riesgo se define en términos del efecto de la incertidumbre de los objetivos.

Concretamente, la norma provee los **Principios**, el **Marco de Trabajo** (*framework*) y un **Proceso de Gestión de Riesgos** para gestionar cualquier tipo de riesgo en forma transparente, sistemática y creíble.

ISO 22301

Otra norma importante es la **ISO 22301** que sigue prácticamente el lineamiento y enfoque de la **BS 25999** para la ***Gestión de Continuidad de Negocios***, **BCM**.

Esta norma es más amplia y completa respecto de la **ISO 27031** que sólo atiende el escenario **TIC** en cuanto a la seguridad en la Continuidad de Negocios.

En este rubro también se dispone de la **ISO 24762** referida específicamente a la *Recuperación de Desastres* aunque, de nuevo, para el ambiente **TIC** como parte de la Gestión de Continuidad de Negocios.

PAS 99

En otro aspecto se distingue el **PAS 99** que es una recomendación (es decir no es una norma) que constituye una herramienta de gran utilidad especificando los requisitos de un ***sistema de gestión común***.

Con **PAS 99** se pueden integrar las normas correspondientes a los Sistemas de Gestión como la ISO 27001 y las mencionadas antes, **ISO 9001, ISO 14001 y OHSAS 18001**, e incluso la **ISO 20000** (ITIL), aunque esta última con ajuste a la **ISO 27013**.

Gracias a la integración de diferentes normas se pueden hacer auditorias y certificaciones conjuntas con reducción de costos y esfuerzos.

En la versión 2012, **PAS 99** se adaptó también al ya mencionado **Anexo SL** que, como dijimos, cubre todas las normas de **sistemas de gestión**.

ISO 15408

Adicionalmente se puede mencionar a la **ISO 15408** o de ***Criterios Comunes*** **(CC)**, que facilita evaluar y seleccionar una gama de productos **IT** a modo de salvaguardas con certificación de los niveles de aseguramiento que proporcionan.

ALGUNAS APLICACIONES

El conjunto de características mencionadas convierten a la ISO 27001 en una importante ayuda para que una empresa pueda mejorar su actual nivel de seguridad y mitigar los riesgos significativos correspondientes que pudieren afectar sus negocios.

Una aplicación muy actual en este sentido responde a los desafíos que enfrenta una estrategia de seguridad para e-business y las múltiples cuestiones que pueden limitar el conocido escenario extranet de comunicaciones B2B entre empresas.

Efectivamente, en este caso a través de Internet se interconectan redes de diferentes empresas (proveedores, clientes, socios), muchas veces con niveles de seguridad desconocidos.

La certificación con la ISO 27001 de las diferentes organizaciones interconectadas les da homogeneidad en este punto, otorgando una garantía de aseguramiento entre ellas, sin importar el tipo de dispositivos, mecanismos, productos o marcas así como los procedimientos con que se hayan implementado los controles y contramedidas de seguridad del SGSI.

Otra aplicación es el mapeado de los requisitos de reglamentaciones y directivas sobre protección de datos personales, como las de la **DNPDP** (Dirección Nacional de Protección de Datos Personales) de Argentina bajo la ley de Habeas Data**,** y la **LOPD** (Ley Orgánica de Protección de Datos) de España.

El resultado es una suerte de mini-proyecto de seguridad de la información, que incluye los controles de la ISO 27002 referidos a dichas reglamentaciones o directivas.

La ISO 27001 aparece también como la norma idónea para medir la porción de seguridad de la información en los ***riesgos operacionales*** que los bancos deben considerar además de los tradicionales riesgos crediticios, a la luz de los Acuerdos de Capitales Basilea II/III.

Por su parte las normas ISO 27002 e ISO 27001 encuentran su aplicación también para un **BCP** (Pan de Continuidad de Negocios) como parte de un **BCM** de la ISO 22301, así como también para medir la efectividad de las medidas para dar cumplimiento a la Sección 404 (a) de la Ley Sarbanes-Oxley,

Nota: Las principales diferencias entre las versiones 2013 y 2005 de las ISO 27001 e ISO 27002, así como mayores detalles de las nuevas versiones, se pueden consultar en
www.angelfire.com/la2/revistalanandwan/nuevas_versiones_ISO_27001_e_ISO_27002.pdf

REFERENCIAS

(1) www.criptored.upm.es/descarga/FactorGenteSeguInfo.zip
(2) www.criptored.upm.es/descarga/SeguridadInformatica_vs_SeguridadInformacion.zip
(3) www.criptored.upm.es/descarga/iso_27002_metricas_controles_x_mapeado_nist.zip
(4) www.criptored.upm.es/descarga/MetricasSeguInfoBSC.zip