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

LAS NUEVAS VERSIONES DE LAS NORMAS ISO 27001 e ISO 27002

NORMA ISO 27002:2013

Esta nueva versión mantiene las cláusulas 0, 1, 2 y 3 de la versión 2005 aunque intercala otra referida a **Referencias Normativas** donde menciona la **ISO 27000** que contiene los términos con sus definiciones para todas las normas de la serie 27K.

Por otra parte, y esto es muy importante de destacar, la cláusula 4 de **Valuación y Tratamiento de los riesgos** se ha eliminado en la versión 2013 de la ISO 27002, aunque en realidad se puede decir que ha pasado a la cláusula de **Planificación** de la ISO 27001, como se verá más adelante.

En cuanto a las cláusulas que definen Objetivos de control y Controles, la nueva versión tiene 14 ***capítulos*** (del 5 al 18) correspondientes a 14 **cláusulas** de seguridad, en lugar de las 11 de la versión 2005. De estas 14 cláusulas, 4 son de carácter *técnico*, 1 *físico* y las 9 restantes son de *gestión*, cuando en la versión 2005 teníamos 11 cláusulas con 3, 1 y 7 cláusulas respectivamente.

En lo referente a la diferencia en el número de cláusulas, surge por un lado que **Criptografía** ahora constituye una cláusula aparte, lo mismo que **Relaciones con Proveedores**. A su vez, la cláusula **Gestión de Comunicaciones y Operaciones** de la versión 2005 ahora aparece dividida en las dos partes, **Comunicaciones** y **Operaciones** por separado.

Yendo a los **objetivos de control** se observa que ahora sólo son **35**, frente a los **39** de la versión 2005.

También se ha reducido en la versión 2013 la cantidad de **controles** a **114**, contra los **133** de la versión 2005. De los respectivos listados de controles se deduce que de los 133 controles de la versión 2005:
a) 27 controles se han eliminado
b) 8 controles de los restantes se han consolidado en sólo 4 controles en la versión 2013
c) 1 control de la versión 2005 se divide en 2 controles en la versión 2013
d) 11 controles nuevos se han agregado.

También se observa que algunos de los controles eliminados en realidad han pasado como ***requisitos*** a la norma ISO 27001, mientras que otros se han considerado en parte redundantes de otros que han quedado.

Respecto de los controles que no han cambiado, salvo su numeración, igualmente corresponde hacer notar que en parte de ellos se han modificado los *Lineamientos de Implementación* correspondientes

Otra observación importante es que ahora en lo referente a la **Continuidad de Negocios** se habla en realidad de **Continuidad de la Seguridad de la Información** embebida en el **Sistema de Gestión de Continuidad de los Negocios (SGCN)**.

De esta manera ahora sólo hay tres controles referidos a la planificación, implementación, y verificación, revisión y evaluación de la *continuidad de la seguridad de la información*.

Para las referencias a las distintas partes tanto de la ISO 27001 como de la ISO 27002 hemos elegido las siguientes denominaciones:
a) Cláusulas para los Capítulos.
b) Apartados para las partes de cada Cláusula
c) Secciones para las partes de cada Apartado

La única excepción ocurre justamente en la ISO 27002 donde los Apartados resultan ser los Objetivos de Control, y las Secciones los Controles correspondientes.

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

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

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**	17.1 Continuidad de la seguridad de la información. 17.2 Redundancias.

	Gestión de Continuidad de Negocios	
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 esta nueva versión 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.

Un dato interesante es que en el mencionado Apéndice del Anexo SL se establecen 45 ***"shall"*** que determinan 84 **requisitos** de cumplimiento efectivo obviamente. como elementos básicos de cualquier norma de **sistema de gestión**.

Con los agregados específicos, la ISO 27001 como norma de **Sistema de Gestión de Seguridad de la Información (SGSI)**, establece en total 50 ***"shall"*** que determinan 130 **requisitos** frente a los 102 requisitos de la versión 2005.

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.

El concepto de ***partes interesadas*** 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.

Antes de entrar en los principales detalles de la nueva versión, vamos a puntualizar las relaciones por cláusulas/capítulos a partir de la versión 2005 y su traslado/mapeado a la nueva versión.

Los cuatro primeros Capítulos (del 0 al 3) de la versión 2005 se mantienen con algunas modificaciones.

La mayor parte de los tres Apartados del Capítulo 4 sobre el SGSI se abren en partes que se cruzan con aporte compartido en seis Capítulos de la nueva versión, desde el 4 hasta el 9. Sin embargo, pese a este cambio estructural se podría decir que el contenido se mantiene en más del 70%.

El Capítulo 5 (Responsabilidad Gerencial) de la versión 2005 con aporte del Apartado 4.3 (Requerimientos de Documentación) forma el nuevo Capítulo 7 (Soporte) de la versión 2013.

Los Capítulos 6 y 7 (Auditoría Interna y Revisión Gerencial) confluyen conjuntamente en el nuevo Capítulo 9 (Evaluación del Desempeño) que por cierto también recibe contribución del Apartado 4.2 (Establecimiento y Gestión del SGSI) de la versión 2005.

Finalmente el Capítulo 8 de la versión 2005 (Mejoras del SGSI) se mapea al nuevo Capítulo 10 (Mejoramiento), salvo las ***acciones preventivas*** que desaparecen con ese nombre, aunque se puede decir que pasan a las Secciones de Valuación y Tratamiento de la Cláusula de Planificación.

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*** en forma genérica, es decir a los riesgos de todo tipo (no sólo de seguridad de la información) que pueden afectar una organización.

La **ISO 31000**, que se revisa más adelante, reconoce su origen en la norma australiana neozelandesa **AS/NZS 4360**.

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*.

Por lo demás, obviamente el Anexo A refleja los controles correspondientes a la nueva versión de la ISO 27002.

Veamos ahora una descripción algo más detallada de cada una de las cláusulas de la versión 2013.

4 - Contexto de la organización

En este capítulo, además del **Alcance** del SGSI, se introducen tres nuevos Apartados.

Un Apartado se refiere a *conocer y entender la organización y su contexto*, y un segundo Apartado a *reconocer y comprender las necesidades y expectativas de todas las partes interesadas* (concepto ya definido antes) en el ámbito de la seguridad de la información.

El tercer Apartado, por su parte, establece las condiciones de un **Sistema de Gestión de Continuidad de Negocios (SGCN)** especialmente en lo referido a la Seguridad de la Información.

5 - Liderazgo

En este tema se destacan dos puntos.

Uno es la referencia a la ***alta gerencia*** (*top management*) en lugar del usual ***gerencia*** (*management*) a secas. De esta manera se enfatiza que las cuestiones de seguridad de la información deben ser incumbencia de los altos directivos de una organización y no solamente de los gerentes de área y gerencia media.

Todo lo anterior se explicita en los Apartados de “Compromiso Gerencial” y el de “Roles, responsabilidades y autoridades de la organización”

El otro punto se refiere a que ya no se habla de *Política del SGSI* en forma diferenciada de la *Política de Seguridad de la Información.* Ahora sólo queda la **Política de Seguridad de la Información**, de manera que en todo caso la primera termina embebida en esta última.

6 - Planificación

Este capítulo trata en general diferentes temas en la **gestión de riesgos**.

Lo primero es comenzar con un claro entendimiento de las estrategias corporativas, enlazando la seguridad de la información con los objetivos propios de la organización.

Ya en el tema central de la gestión de riesgos, comentaremos cinco de esos temas: PDCA, Oportunidades, Valuación de Riegos, Tratamiento de Riesgos, y Continuidad de Negocios.

PDCA

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***.

Oportunidades
Otro punto referido a la Planificación es la incorporación del concepto de **Oportunidades** junto con el de **Riesgos**.

Aquí el concepto de *oportunidades* responde a la adhesión de la norma ISO 27001 a la norma ISO 31000 que, para el caso, define el *riesgo* como el "efecto de la incertidumbre en los objetivos".

A partir de esto se puede decir que una ***oportunidad*** es simplemente la incertidumbre respecto de un efecto *positivo* en un objetivo.

Este escenario se puede considerar mediante el análisis **FODA** (ver recuadro aparte).

ANALISIS FODA

Las Oportunidades es un concepto presente en el análisis **FODA (Fortalezas, Oportunidades, Debilidades, Amenazas)**.

FODA es una herramienta de planificación estratégica para comprender un proyecto, negocio y organizaciones y tomar las decisiones adecuadas para el propósito buscado.

De esta manera FODA permite identificar y evaluar precisamente los factores *favorables* (Fortalezas y Oportunidades) y *desfavorables* (Debilidades y Amenazas) para el logro de las estrategias y objetivos.

Fortalezas: son las capacidades, habilidades y recursos especiales con que cuenta la empresa, y que le permite tener una posición privilegiada frente a la competencia.

Oportunidades: son aquellos factores que resultan positivos, favorables, aprovechables, que hay que ubicar en el entorno en el que actúa una empresa, y que le permiten obtener ventajas competitivas.

Debilidades: son aquellos factores que provocan una posición desfavorable frente a la competencia y/o carencia de algunos recursos.

Amenazas: son aquellas situaciones que provienen del entorno y que pueden llegar a afectar incluso la supervivencia de la organización.

Se puede entender mejor el concepto de Oportunidades considerando que representa un aspecto de una suerte de **riesgo positivo** o **upside risk**, a diferencia del riesgo convencional que, por sus efectos, puede considerarse como un **riesgo negativo** o **downside risk**.

Estas diferencias han venido estado presentes en ambientes de Finanzas y más recientemente en el **ERM (Gestión de Riesgos Empresariales)**.

De cualquier manera, el concepto de *riesgos positivos* puede parecer un poco extraño para otros escenarios como el de seguridad de la información, puesto que en general se piensa en el riesgo como una ***consecuencia*** antes que una ***oportunidad para mejorar***.

Acá nos referimos a las ***oportunidades de negocio***, que pueden crear valor y lograr objetivos de la organización, permitiendo incluso obtener ventajas competitivas al realizar cosas que antes no se hacían, o bien proporcionar nuevas o mejores soluciones.

Uno podría ser el caso que la organización contara con un plan permanente o semipermanente de concientización que tocara algunos aspectos de seguridad. Un caso especial pueden ser las sesiones de Kaizen que en general ayudan a mejorar las operaciones.

Otro ejemplo podría ser el caso de una organización con ciertas reglas de seguridad en los accesos, lo cual así como ordena de alguna manera el comportamiento general del personal, de alguna manera también facilita el cumplimiento de las normas de seguridad.

Y para finalizar con el tema de las oportunidades corresponde mencionar que también hay que identificar los riesgos asociados con la ***pérdida de una oportunidad***, lo cual en la **teoría de las decisiones** se conoce como ***arrepentimiento*** (regret), como resultado de no haber tomado la mejor opción.

Valuación de riesgos
Siguiendo con el apartado de Planificación, también hay que mencionar la **Valuación de los Riesgos** que es considerada ahora en forma más genérica acorde con la norma **ISO 31000** ya mencionada.

Adicionalmente en la Identificación de los Riesgos aparece el nuevo concepto de "propietario del riesgo" a diferencia del "propietario de un activo" de la versión 2005.

Aquí conviene destacar que el cambio de *activos* a *riesgos* se alinea mejor a procesos como los de **ERM** ya mencionado, que no se enfocan en activos específicos sino más bien a los procesos o escenarios para valuación de riesgos.

De cualquier manera, como antes, el concepto de propietario no es el de tener derechos de propiedad, sino que el propietario antes tenía que rendir cuenta de *sus activos*, mientras que ahora debe hacerlo con todo lo relacionado con *los riesgos* que le competen.

Un punto importante en cuanto a la Valuación de Riesgos es que ahora ya no es necesario determinar riesgos a partir de los **activos, vulnerabilidades y amenazas**, aunque seguramente esta metodología perdurará por mucho tiempo.

En cambio, se mantiene el esquema más conocido de calcular *riesgos por las pérdidas*, es decir por los **impactos** que causa un incidente y las **probabilidades** de ocurrencia del mismo.

Tratamiento de riesgos
En este tema corresponde destacar muy especialmente que el **Tratamiento de los riesgos** también se adapta a la **ISO 31000** ya mencionada.

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 que, como antes, lista los objetivos de control y controles que detalla la ISO 27002.

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". O sea, en la práctica, ¿de quién sino de la ISO 27002, como era antes tal como se visualiza en la Figura 2?.

De una u otra forma, el resultado de esta parte del proceso debe producir la **Declaración de Aplicabilidad (SoA)**.

Continuidad de Negocios
Y finalmente otro punto a mencionar es que ahora se habla de **Continuidad de Negocios** en cuanto a la determinación de los objetivos correspondientes y la planificación para lograr dicha continuidad.

7 - Soporte

En esta Cláusula también se pueden mencionar varias cuestiones interesantes.

En primer lugar se analizan los recursos, competencia del personal, concientización y comunicación. Respecto de la versión 2005 se destaca el tema de las *formas de comunicación*.

Por otra parte, un detalle a comentar es que en esta versión desaparece el concepto de ***registros*** (***records***) y que en todo caso se incluyen en la ***información a documentar*** (***documented información***).

La cuestión más significativa es que, a diferencia de la versión 2005 en que se establece una lista de la documentación a mantener, el Apartado 7.5 de la versión 2013 sólo dice que la información a documentar es la "requerida por la norma", así como otra información que la organización considere necesaria con referencia a la efectividad del SGSI.

Si entonces se hace una búsqueda en toda la norma de la expresión "documented information" surgirá una serie de documentos a mantener.

A veces dicha información se refiere a *procesos y acciones*, otras a los ***resultados*** (***results***) obtenidos por dichos procesos.

Entre los principales documentos podemos mencionar, entre otros: Alcance, Política de Seguridad de la Información, Valuación de Riesgos, Proceso de tratamiento de riesgos especialmente el SoA y el Plan de Tratamiento de Riesgos (RTP), Competencia del personal y acciones para lograrla, Proceso de Planificación y control, Resultados de la Valuación de riesgos, Resultados del tratamiento de riesgos, Resultados del monitoreo y mediciones, Programa de Auditoría, Resultados de Auditoría, Proceso de Revisión Gerencial y los Resultados correspondientes, Naturaleza de las No Conformidad, y Resultados de las Acciones Correctivas.

A esta lista se agregan otros documentos y resultados especialmente los relacionados con la Seguridad de la Información en la Gestión de Continuidad de Negocios (BCM).

8 - Operación

Este capítulo, además de la planificación y control de las operaciones, desarrolla el tema de la **Continuidad de Negocios** que antes sólo aparecía en la ISO 27002:2005 y que por cierto sigue presente también en la ISO 27002:2013.

Primero lo hace en cuanto al **Análisis de Impactos en los Negocios (BIA)** y la correspondiente Valuación de riesgos, seguido de la determinación de la Estrategia de la Continuidad de Negocios, el Establecimiento e implementación de los procedimientos correspondientes, así como de los Ejercicios y pruebas, todos componentes del **SGCN** ya mencionado antes.

Por cierto podemos decir que en el proceso mencionado se puede ampliar el trabajo en base a la norma **ISO 22301** precisamente de **Sistemas de Gestión de Continuidad de Negocios (SGCN).**

9 - Evaluación del rendimiento

Ya se comentó antes que esta Cláusula incluye las de Auditoría Interna y Revisión Gerencial de la versión 2005.

En la nueva versión se puede observar un refuerzo de los requisitos de vigilancia y medición de la eficiencia.

Esto implica que se hace necesario identificar, describir y poder documentar la eficiencia de los controles implementados.

Para estas funciones se puede apelar a los **Indicadores Clave de Desempeño (KPI)** o bien, en forma mucho más completa al **Balanced Scorecard (BSC)**, un tema éste ampliamente desarrollado (incluyendo

Trabajos Prácticos) en nuestros cursos de *Métricas de Seguridad de la Información*, así como en otros cursos que incluyen la sección de *Métricas*.

10 - Mejoramiento

En este capítulo, como ya se comentara antes, las ***Acciones Preventivas*** desaparecen con ese nombre aunque se puede decir que pasan a los *apartados* de **Valuación y Tratamiento de Riesgos** de la Cláusula de **Planificación**,

Por otra parte aquí se tiene que, junto con las ***Acciones Correctivas***, las diferentes referencias por separado existentes en la versión 2005 de las "***No Conformidades***" se han consolidado en una sección específica.

Recordemos que las No Conformidades pueden definirse como todo lo que se desvía del SGSI y los controles establecidos, cubriendo no sólo los incidentes y su manejo, sino también todo otro tipo de no conformidades,

