ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"MIGRACIÓN DE UN SGSI BASADO EN ISO/IEC 27001:2005 A LA VERSIÓN ISO/IEC 27001:2013"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

MARÍA JOSÉ RENDÓN FREIRE

GUAYAQUIL-ECUADOR

AÑO: 2015

AGRADECIMIENTO

A Dios por estar presente en cada momento de mi vida, iluminando y guiando mi camino.

A mis padres, hermana y enamorado por todo su apoyo durante este proceso.

Gracias a los profesores por compartir sus conocimientos y aportar en mi formación y crecimiento profesional.

.

.

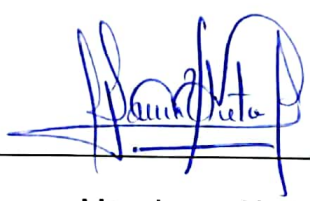
DEDICATORIA

Dedico este trabajo a mis padres, quienes me han brindado su apoyo en las diferentes etapas de mi vida, ya que gracias a sus enseñanzas y cariño he alcanzado las metas propuestas, a mi hermana por soportar mis momentos de estrés y a JuanFer por siempre tener las palabras precisas cuando las he requerido, por impulsarme a ser mejor y su amor incondicional.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

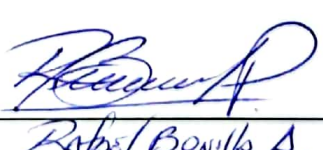
DIRECTOR MSIA



Mgs. Laura Ureta

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



Mgs. Albert Espinal

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El presente proyecto tiene como objetivo identificar los cambios en los requisitos de la norma ISO/IEC 27001:2013 respecto a la versión 2005, para lograr la actualización de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2005 acorde a lo establecido en el nuevo estándar.

En el capítulo 1 se realizará la descripción del problema, el cual hace referencia al cambio de versión de la norma ISO/IEC 27001:2005 por la versión 2013 afectando a los Sistemas de Gestión de Seguridad de la información ya implementados, por lo cual se propone la solución para la migración.

En el capítulo 2 se revisará la estructura de las cláusulas y controles del Anexo A de las dos versiones de la norma IOS/IEC 27001 para luego compararlas e identificar las diferencias.

En el capítulo 3 se presentará como resultado de la revisión y comparación realizada en el capítulo 2 un listado de los requisitos a implementar en el Sistema de Gestión de Seguridad de la información y los lineamientos para dar conformidad con lo establecido en la norma ISO/IEC 27001:2013.

Para culminar este trabajo se presentarán las conclusiones y recomendaciones.

ÍNDICE GENERAL

ABREVIATURAS

NC	No conformidad
PDCA	Plan, Do, Check, Act
SGSI	Sistema de Gestión de Seguridad de la Información.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las organizaciones que han implementado un Sistema de Gestión de Seguridad de la Información, conocen la importancia de mantener y mejorar el sistema ya que se está analizando constantemente los riesgos para establecer y ejecutar los planes de mitigación correspondientes con el propósito de velar por la confidencialidad, integridad y disponibilidad de la información.

Con el cambio de versión de la norma ISO 27001, es importante que las organizaciones conozcan los nuevos requisitos y mejoras del estándar para que su SGSI pase por una fase de transición de la versión 2005 a la 2013 para dar cumplimiento con el nuevo estándar y así mantener su sistema actualizado.

Este trabajo tiene como objetivo identificar los nuevos requisitos de la norma y dar los lineamientos para su implementación para que las organizaciones que cuentan con un SGSI basado en ISO27001:2005 puedan dar

conformidad con los requisitos de la versión 2013 del estándar y mantener vigente su Sistema de Gestión de Seguridad de la Información.

En este trabajo se revisará la estructura y requisitos de las dos versiones del estándar para luego compararlas y elaborar un listado de los nuevos requisitos y los lineamientos bases para su implementación, de tal manera que será de utilidad para cualquier organización que cuente con un SGSI basado en ISO27001:2005 para su fase de migración a la versión 2013.

.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

La Organización Internacional para la normalización (ISO) en Octubre del 2013 publicó ISO/IEC 27001:2013 la cual es una revisión de la norma ISO/IEC 27001:2005 cuyo objetivo fue incluir mejoras en los requisitos del sistema, además de buscar su integración con otros sistemas de gestión, como el de Continuidad de Negocio (ISO/IEC 22301:2012), ya que su estructura se basa en el Anexo SL.

Debido a esa actualización, las organizaciones que contaban con un SGSI certificado basado en ISO 27001:2005 tuvieron que realizar la migración de su sistema de gestión seguridad de la información para cumplir con los requisitos del nuevo estándar hasta Junio del 2015 de tal manera que su certificación se mantenga en vigencia

El mantener un Sistema de Gestión de Seguridad de la Información certificado dentro de una organización, es muy importante ya que con su implementación se vela por la confidencialidad, integridad y disponibilidad de la información, además de ser un factor que agrega valor a la organización ya que la certificación es otorgada por una entidad externa que valida la conformidad del sistema implementado con los requisitos de la norma vigente.

1.2 SOLUCIÓN PROPUESTA

El mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en una organización es uno de los principales objetivos ya que se está en constante evaluación del Sistema para verificar su eficacia e identificar oportunidades de mejora.

Con la publicación del standard ISO/IEC 27001:2013, el SGSI implementado en las organizaciones basado en ISO/IEC 27001:2005 debe ser revisado y comparado con los requisitos de la nueva versión del estándar para identificar los nuevos requerimientos para su posterior implementación y así dar conformidad con la norma en vigencia.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 IDENTIFICAR LA ESTRUCTURA DE LA NORMA ISO 27001:2005

El estándar internacional está basado en el enfoque de procesos y utiliza el modelo PDCA (Plan, Do, Check, Act) para “establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información” [1].

Se considera un proceso a cualquier actividad que usa recursos de entrada para transformarlos y obtener salidas las cuales con frecuencia se convierten en los recursos de entrada del siguiente proceso. El enfoque de procesos es la aplicación de un sistema de procesos dentro de una organización junto con la identificación, interacción y gestión de los mismos [1].

Como se observa en la figura 2.1, el modelo PDCA utiliza como entrada los requerimientos y expectativas relacionadas a la seguridad de la información de las partes interesadas para así establecer el SGSI, implementar, monitorear y mejorar el sistema con el propósito de satisfacer los requerimientos y expectativas iniciales, demostrando la gestión respecto a la seguridad de la información.

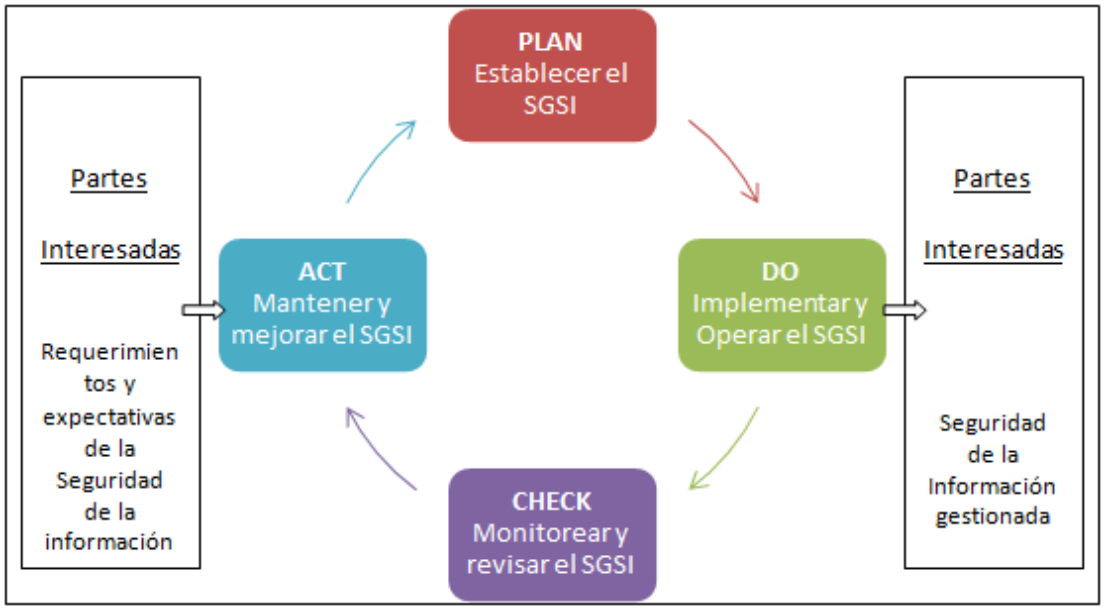


Figura 2.1 Modelo PDCA aplicado al SGSI

El estándar ISO/IEC 27001:2005 “Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la seguridad de la información – Requerimientos”, cuenta con 8 cláusulas y 3 anexos de los cuales el anexo A es normativo y presenta los objetivos de control y controles, mientras que el B y el C son informativos, donde B indica principios mientras que el C la relación con otros estándares. Se muestra la estructura en la Figura 2.2.

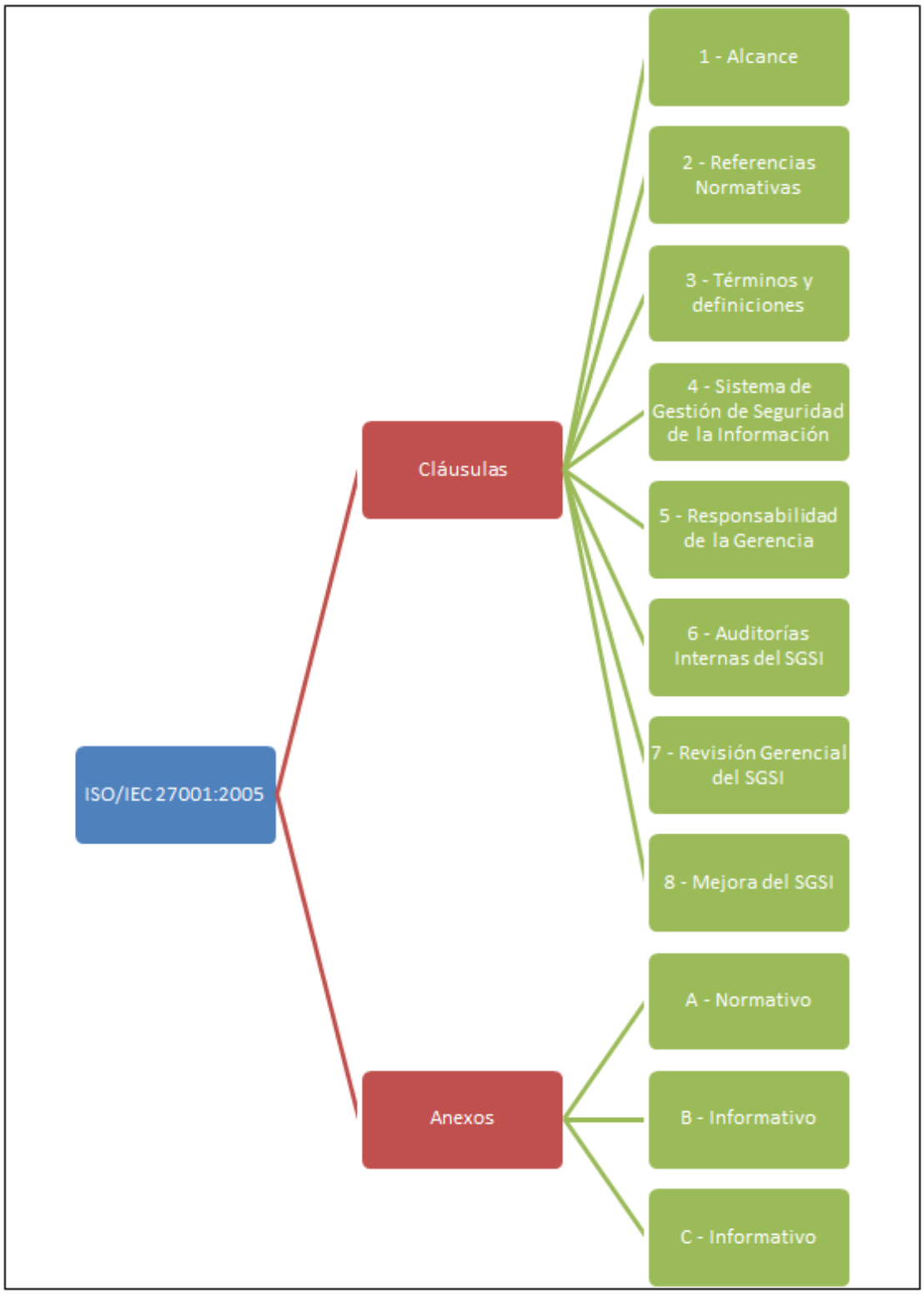


Figura 2. 2 Estructura de la norma ISO/IEC 27001:2005

Para que una organización certifique su SGSI basado en ISO/IEC 27001:2005 era mandatorio cumplir con todos los requisitos de las cláusulas 4, 5, 6, 7 y 8, además de los controles del Anexo A sin embargo para este último si se permitían exclusiones con su respectiva justificación.

Cláusula 1 – Alcance

En esta sección se menciona que los requisitos del estándar son aplicables a cualquier organización, sin importar su tipo, tamaño o naturaleza con el propósito de proteger los activos de información y brindar confianza a las partes interesadas.

Cláusula 2 – Referencias Normativas

Indica los documentos a los cuales hace referencia dentro del estándar y los lineamientos respecto a la versión de los mismos en base a su fecha, es decir en caso de no especificar fecha se tomará en cuenta el documento vigente (última actualización), en caso de mencionar la fecha se utilizará ese documento sin importar si existe una nueva versión.

Cláusula 3 – Definiciones

El estándar utiliza cierta terminología las cuales en esta sección se muestra con su respectiva definición.

Cláusula 4 – Sistema de Gestión de Seguridad de la información

Con esta cláusula la organización establece, implementa, opera, monitorea, mantiene y mejora su SGSI el cual debe estar documentado y alineado con las actividades comerciales de la organización y los riesgos a los que se enfrentan, los procesos utilizados se basan en el modelo PDCA Figura 2.1.

Como se puede observar en la figura 2.3, la cláusula consta de tres partes:

- 4.1 Requerimientos Generales.
- 4.2 Establecer y mantener el SGSI.
- 4.3 Requerimientos de Documentación.

La primera parte “4.1 Requerimientos Generales” es una introducción en la cual se indica que el SGSI de una organización debe estar documentado, alineado a sus requisitos comerciales y a los riesgos que debe enfrentar siguiendo el modelo PDCA en busca de la mejora continua.

En la segunda parte del estándar “4.2 Establecer y mantener el SGSI” se dan las pautas de lo que requiere el sistema para su establecimiento, implementación, operación mantenimiento y mejora, esta parte cuenta con cuatro secciones:

- 4.2.1 Establecer el SGSI. (Plan)
- 4.2.2 Implementar y Operar el SGSI. (Do)
- 4.2.3 Monitorear y revisar el SGSI. (Check)

- 4.2.4 Mantener y mejorar el SGSI. (Act)

En la Tabla 1 se muestra un resumen de las actividades que debe ejecutar la organización en cada una de las cuatro secciones de tal manera que se cumpla con los requisitos definidos en el estándar [2].

Tabla 1 Actividades para establecer el SGSI

Cláusulas	Actividades Organizacionales
Establecer el SGSI (4.2.1)	a) Definir el alcance del SGSI b) Definir un enfoque sistemático para la evaluación del Riesgo c) Identificar el riesgo d) Analizar y evaluar el riesgo e) Definir política del SGSI f) Identificar y evaluar opciones para el tratamiento del riesgo g) Seleccionar objetivos de control y controles del Anexo A h) Preparar un enunciado de aplicabilidad i) Obtener aprobación de la gerencia
Implementar y operar el SGSI (4.2.2)	a) Formular un plan para tratamiento del riesgo. b) Implementar el plan de tratamiento del riesgo. c) Implementar todos los objetivos de control y controles seleccionados. d) Definir como ser medirá la efectividad de los controles e) Implementar programa de entrenamiento y toma de conciencia. f) Gestionar operaciones. g) Gestionar recursos.
Monitorear y revisar el SGSI (4.2.3)	a) Ejecutar procedimientos de monitoreo b) Efectuar revisiones regulares de la eficacia del SGSI. c) Revisar el nivel de riesgo residual y del riesgo aceptable. d) Conducir auditorías internas del SGSI. e) Registrar todos los eventos que tienen un efecto en el desempeño del SGSI.
Mantener y Mejorar el SGSI (4.2.4)	a) Implementar las mejoras identificadas. b) Tomar apropiadas acciones correctivas y preventivas. c) Comunicar los resultados a todas las partes interesadas. d) Asegurar que las mejoras alcancen los objetivos deseados.

La última parte de la cláusula 4 es la sección “4.3 Requerimientos de Documentación” donde se indica la documentación que es indispensable en un SGSI de cualquier organización para que sea conforme con los requisitos del estándar ISO/IEC 27001:2005. Esta parte cuenta con 3 secciones:

- 4.3.1 General
- 4.3.2 Control de documentos
- 4.3.3 Control de registros.

En la sección “4.3.1 General” se recalca la importancia de los documentos para demostrar la relación con los controles seleccionados producto de la evaluación del riesgo, su plan de tratamiento, objetivos planteados y política del sistema, en las secciones “4.3.2 y 4.3.3” se especifican los puntos relevantes para el control de documentos y registros, a continuación se presenta una lista de documentos mandatorios:

- Política y objetivos del SGSI.
- Alcance del SGSI.
- Metodología de evaluación del riesgo
- Resultados de la evaluación del riesgo.
- Plan del tratamiento de los riesgos.
- Enunciado de aplicabilidad.
- Procedimientos documentados para asegurar la gestión de seguridad de la información.
- Procedimiento de control de documentos y de registros.

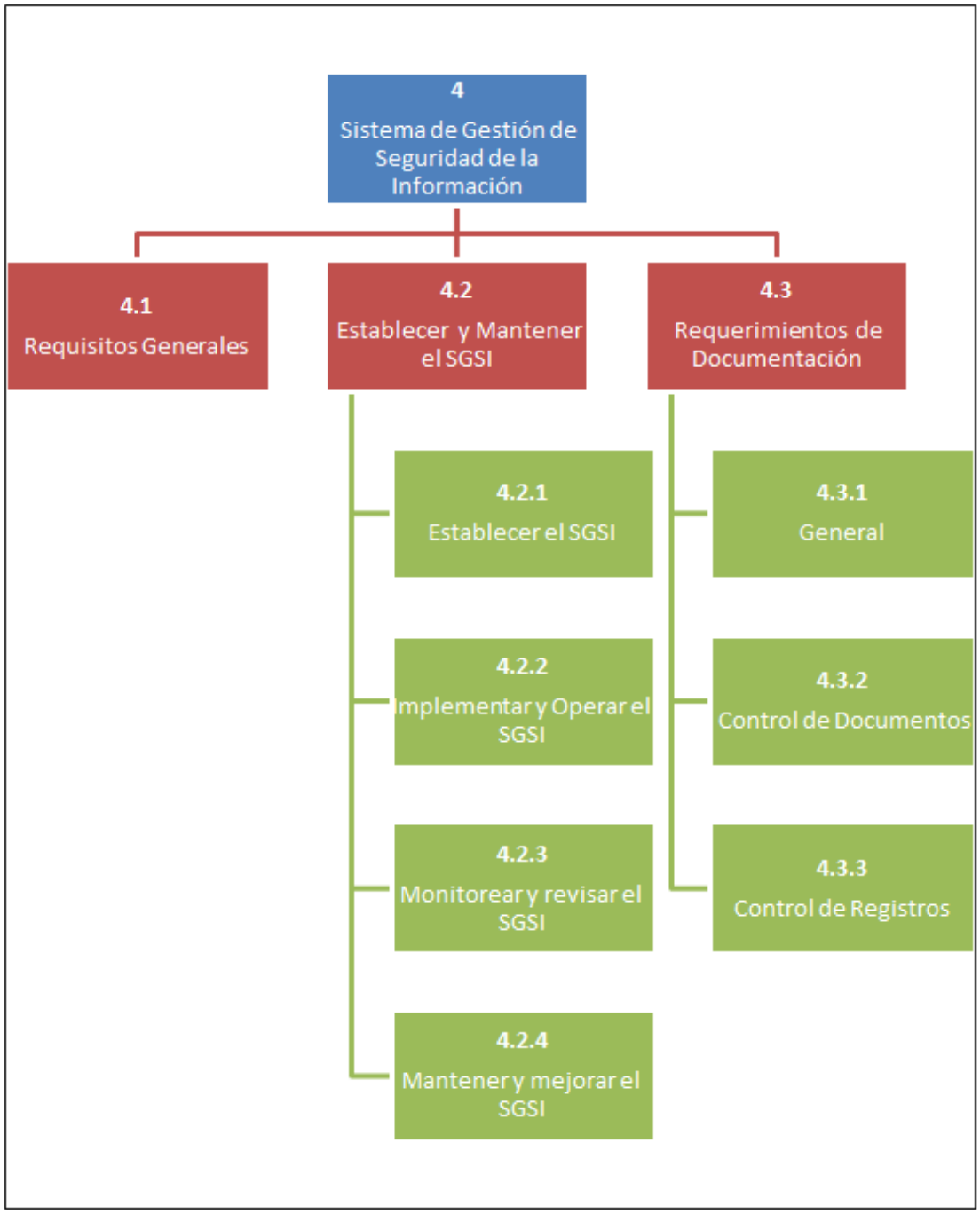


Figura 2. 3 Estructura de la cláusula 4 – ISO/IEC 27001:2005

Cláusula 5 – Responsabilidades de la Gerencia

Esta sección del estándar se enfoca en que la Gerencia de la organización debe contar con evidencia de su compromiso con el SGSI en todas sus fases desde el establecimiento, operación, revisión, mantenimiento y mejoramiento, además de la asignación de recursos y capacitación. En la figura 2.4 se presenta la estructura de la cláusula 5.

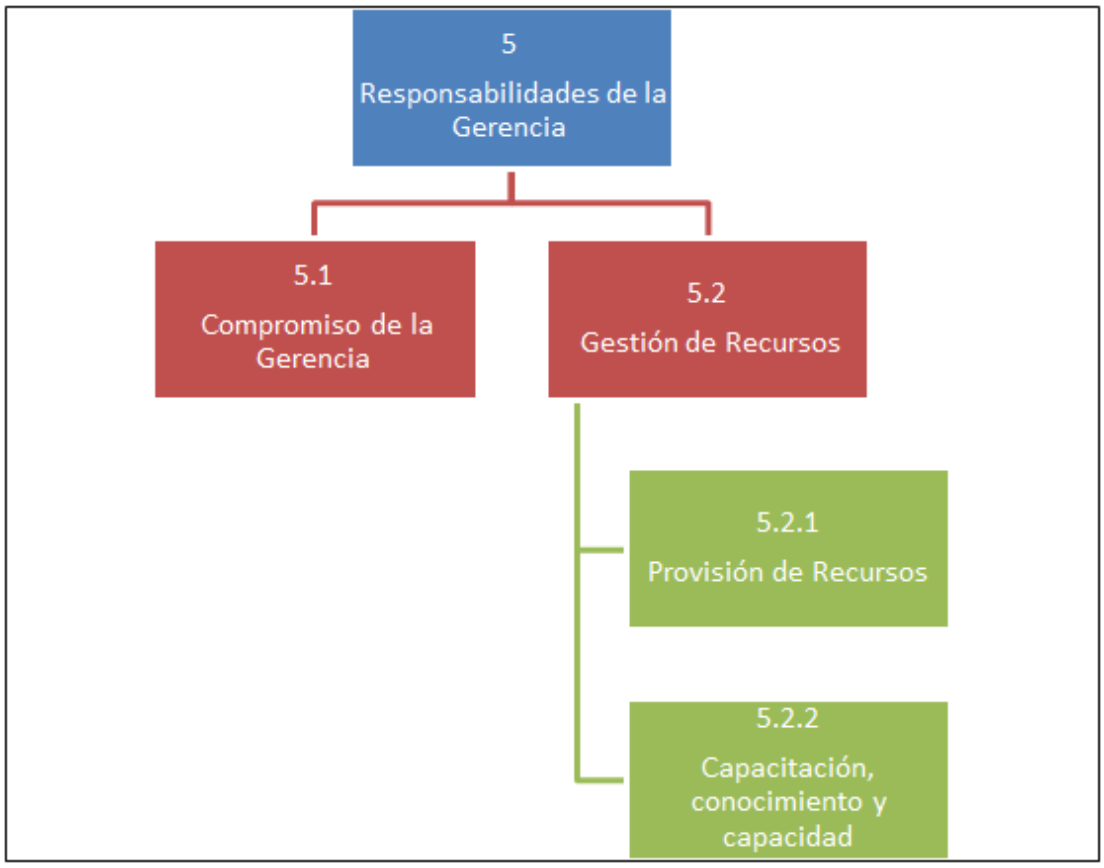


Figura 2. 4 Estructura de la cláusula 5 – ISO/IEC 27001:2005

A continuación se van a listar las actividades que debe realizar la gerencia para evidenciar su compromiso (Cláusula 5.1) con el SGSI de la organización:

- Establecer la política del SGSI
- Asegurar el establecimiento de objetivos y planes del SGSI
- Establecer roles y responsabilidades asociadas a la seguridad de la información.
- Comunicar la importancia de alcanzar los objetivos y el cumplimiento de la política del SGSI, las responsabilidades de cada rol dentro del sistema y la necesidad de mejorar continuamente.
- Proporcionar los recursos para todas las fases del SGSI.
- Decidir los criterios de aceptación del riesgo y los niveles de riesgo que son aceptables.
- Asegurar que se ejecuten las auditorías internas del SGSI.
- Realizar revisiones gerenciales del sistema.

Respecto a la cláusula 5.2 Gestión de recursos es relevante destacar que las actividades y/o procedimientos de seguridad de la información deben apoyar a los requerimientos comerciales además de cumplir con las regulaciones del país donde se encuentra la organización que ha implementado su SGSI. Dado que el SGSI busca la mejora continua es necesario que se realicen revisiones periódicas y tomar acciones frente a los resultados obtenidos en caso de requerirlo.

Se debe asegurar que el personal que tiene asignadas responsabilidades de la seguridad de la información cuente con el conocimiento y capacidades para el buen desempeño de su rol dentro del SGSI. Se debe contar con los registros asociados a la educación del personal, capacitaciones y experiencia.

Es importante que el personal de la organización esté consciente de su aporte respecto a la seguridad de la información para el logro de los objetivos planteados para el SGSI.

Cláusula 6 – Auditorías Internas del SGSI

Las auditorías internas al SGSI son un mecanismo mediante el cual la organización evalúa el cumplimiento de los objetivos de control, controles, procesos y procedimientos establecidos para el sistema de gestión de seguridad de la información respecto a los requisitos del estándar ISO/IEC 27001:2005 y las regulaciones del país donde se encuentra la organización.

Las auditorías internas deben ejecutarse a intervalos planificados, la frecuencia de ejecución de las auditorías es decisión de la organización ya que el estándar no especifica un valor. Se debe documentar un procedimiento de auditorías internas donde se definan:

- Responsabilidades.
- Requerimientos de planificación y ejecución.
- Reporte de Resultados.

Cláusula 7 – Revisión Gerencial del SGSI

Es responsabilidad de la gerencia revisar al menos una vez al año su Sistema de Gestión de Seguridad de la información con el propósito de validar su efectividad e identificar oportunidades de mejora o cambios en el SGSI asociados a su política y objetivos de seguridad de la información. Se debe mantener registros de los resultados de las revisiones. En la Figura 2.5 se muestra la estructura de la cláusula, la cual consta de tres partes:

- 7.1 General.
- 7.2 Insumo de la revisión.
- 7.3 Resultado de la revisión.

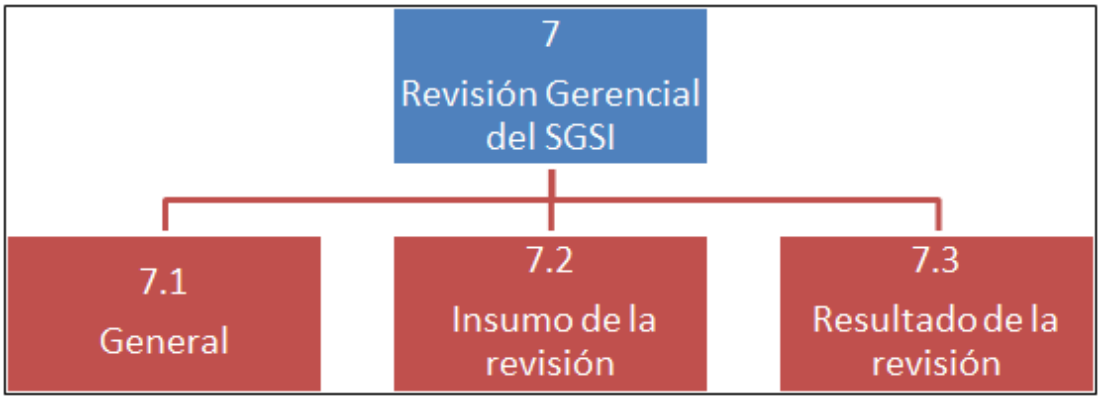


Figura 2. 5 Estructura de la cláusula 7 – ISO/IEC 27001:2005

La revisión por parte de la gerencia de la organización debe incluir los siguientes datos de entrada:

- Resultados de auditorías y revisiones del SGSI.
- Retroalimentación de partes interesadas.

- Estado de las acciones preventivas y correctivas.
- Vulnerabilidades o amenazas no tratadas de forma adecuada en la evaluación del riesgo previa.
- Resultados de la medición de la efectividad del sistema.
- Acciones de seguimiento de revisiones gerenciales previas.
- Cambios que pueden afectar el SGSI.
- Recomendaciones para la mejora del sistema.

Luego de la revisión, los resultados deben quedar registrados los cuales incluirán las decisiones y acciones relacionadas con:

- Mejora de la efectividad del SGSI.
- Mejora en la medición de efectividad de controles
- Actualización de la evaluación y plan del tratamiento del riesgo.
- Necesidades de recursos.
- Cambios en procedimientos y controles que afecten la seguridad de la información asociados a modificación de requerimientos comerciales, de seguridad, leyes, niveles de riesgo o criterios de aceptación.

Cláusula 8 – Mejora del SGSI

La mejora del Sistema de Gestión de Seguridad de la información está formada por tres partes, tal como se muestra en la figura 2.6:

- Mejora continua.
- Acción correctiva.
- Acción preventiva.

Figura 2. 6 Estructura de la cláusula 8 – ISO/IEC 27001:2005

La organización debe mejorar de manera continua la efectividad de su Sistema de Gestión de Seguridad de la Información mediante el uso de lo que se lista en Tabla 2.

Tabla 2 Documentación relevante para la mejora del SGSI

Información importante para mejorar la efectividad del SGSI
Política de Seguridad de la Información
Objetivos de seguridad de la Información
Resultados de auditoría
Análisis de eventos monitoreados
Acciones correctivas y preventivas
Revisiones Gerenciales

Las acciones correctivas en el SGSI tienen como objetivo eliminar la causa de las no conformidades asociadas a los requerimientos del sistema para evitar su recurrencia, mientras que las acciones preventivas buscan eliminar las causas de las no conformidades potenciales. Cada una de estas acciones debe contar con un procedimiento documentado.

Anexo A – Objetivos de control y controles.

La norma cuenta con el Anexo el A donde se definen objetivos de control y controles para que la organización los seleccione luego de la evaluación y análisis de riesgos para su posterior implementación con el fin de mantener un sistema de gestión de seguridad de la información que vela por la confidencialidad, integridad y disponibilidad de sus activos. En el enunciado de aplicabilidad se listan todos los controles y se justifica el motivo de su selección o exclusión. El anexo tiene un total de 133 controles y 11 dominios los cuales se muestran en la Tabla 3.

Tabla 3 Dominios de Seguridad - Anexo A - ISO/IEC 27001:2005

Dominios de Seguridad
A.5 Política de Seguridad
A.6 Organización de la seguridad de la información
A.7 Gestión de los activos
A.8 Seguridad de los recursos humanos
A.9 Seguridad física y ambiental
A.10 Gestión de las comunicaciones y operaciones
A.11 Control de acceso
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información
A.13 Gestión de incidentes de seguridad de la información
A.14 Gestión de la continuidad comercial
A.15 Cumplimiento

2.2 IDENTIFICAR LA ESTRUCTURA DE LA NORMA ISO 27001:2013

El estándar internacional ISO/IEC 27001:2013 proporciona los requisitos que debe cumplir una organización para establecer, implementar, mantener y mejorar de manera continua su Sistema de Gestión de Seguridad de la Información. El establecimiento e implementación del SGSI depende de los siguientes factores:

- Necesidades y objetivos de la Organización.
- Requisitos de Seguridad.
- Procesos Organizacionales.
- Tamaño y Estructura de la Organización.

El propósito del SGSI es conservar la confidencialidad, integridad y disponibilidad de la información utilizando un proceso para la gestión de riesgos que permita garantizar a las partes interesadas que estos son atendidos de manera adecuada.

Este estándar tiene una estructura de alto nivel, donde los títulos de subcapítulos, textos, términos y definiciones básicas se basan en lo establecido en el Anexo SL del ISO/IEC Directivas, Parte1, por lo que se mantiene compatibilidad con otras normas del sistema de gestión que utilizan la estructura del Anexo SL [3]. En la figura 2.7 se muestra la estructura.

El mantener un enfoque común en estructura, basado en el Anexo SL permite a las organizaciones que operen con un solo Sistema de Gestión que cumpla con los requisitos de varias normas.

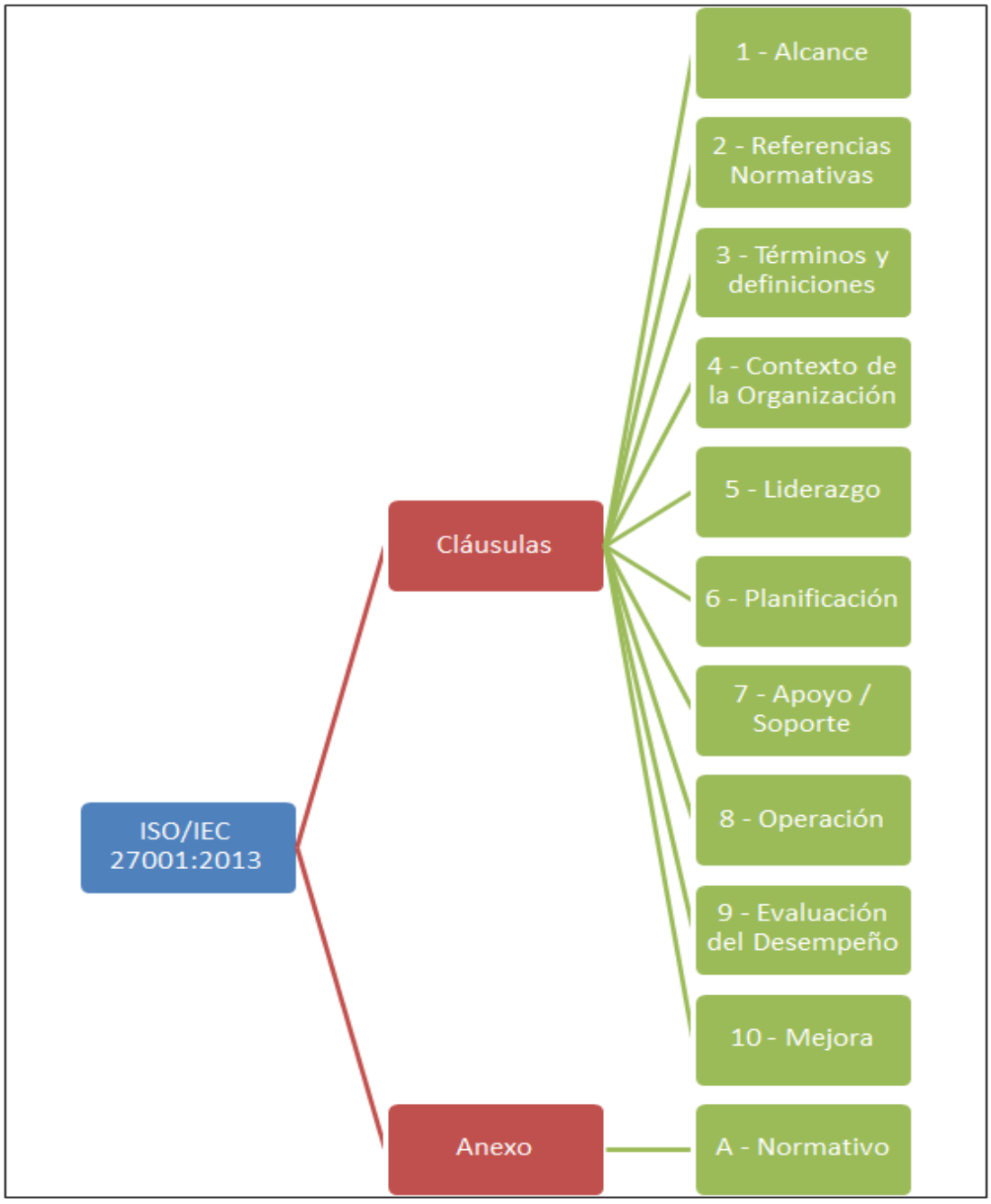


Figura 2. 7 Estructura de la norma ISO/IEC 27001:2013

Cláusula 1 – Alcance

En esta sección del estándar se recalca que los requisitos definidos son genéricos y pueden ser aplicados a cualquier organización que requiera establecer, implementar, mantener y mejorar un SGSI alineados a su contexto. Vale la pena destacar que si la organización quiere certificar su sistema basado en ISO/IEC 27001:2013 no se acepta la exclusión de requisitos especificados en las cláusulas del 4 al 10.

Cláusula 2 – Referencias normativas.

Esta norma en ciertos puntos hace referencia a otros estándares, por tal motivo en esta sección se indican los lineamientos para el adecuado uso de la documentación que menciona, en caso de no contar con fecha aplica la última versión vigente mientras que si es explicita la versión entonces ese es el documento que aplica.

Cláusula 3 – Términos y definiciones

Esta sección hace referencia a los términos y definiciones que se encuentran en ISO/IEC 27000 en su última versión los cuales se aplican en este estándar.

Cláusula 4 – Contexto de la Organización.

Es importante conocer que la organización identifique los asuntos internos y externos que puedan influir en el los resultados esperados de su sistema de gestión, además las partes interesadas y sus requisitos relacionados a seguridad de la información.

Esta cláusula está formada por cuatro partes tal como se puede observar en la figura 2.8.

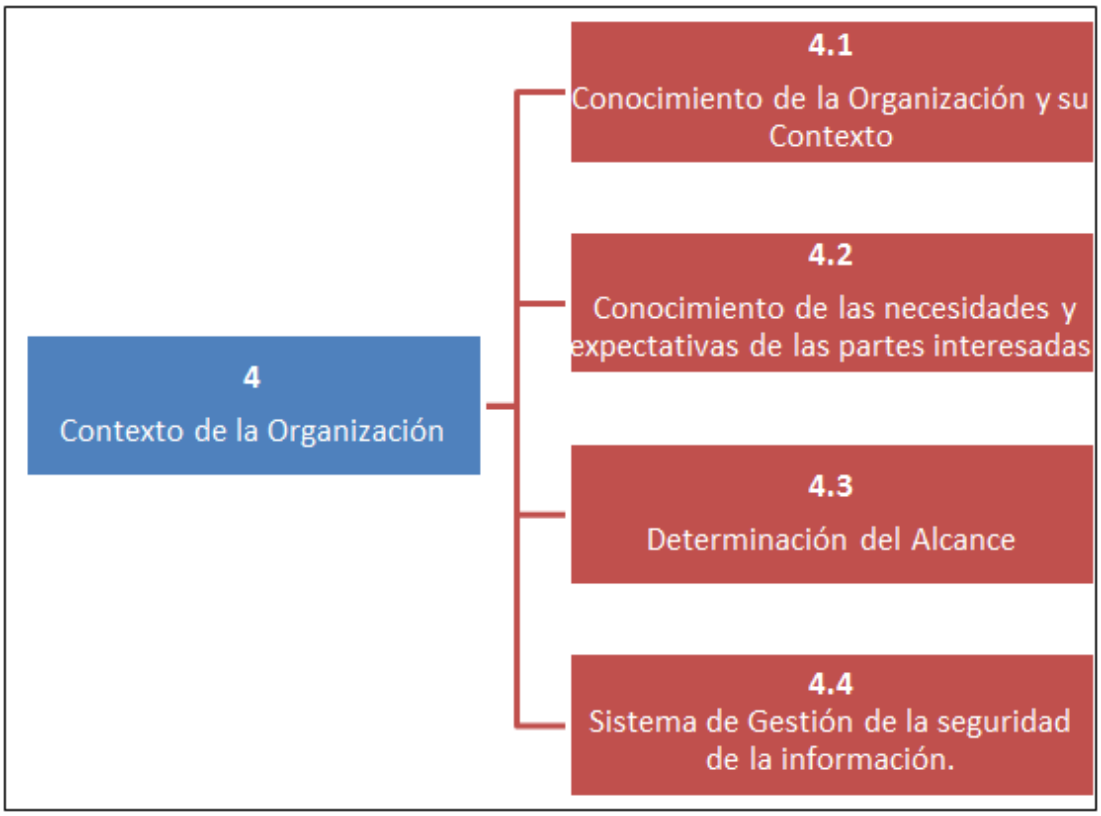


Figura 2. 8 Estructura de la cláusula 4 – ISO/IEC 27001:2013

El alcance del Sistema de Gestión de Seguridad de la Información debe quedar documentado, para determinar el mismo es necesario considerar:

- Asuntos internos y externos.
- Requisitos de las partes interesadas respecto a la seguridad de la información.
- Interfaces y dependencias entre las actividades de la organización con otras instituciones.

Cláusula 5 – Liderazgo.

El liderazgo y compromiso de la dirección con respecto al SGSI es un pilar fundamental para que el sistema se integre a los procesos y esté alineada con los objetivos estratégicos de la organización. Esta cláusula consta de tres partes las cuales se muestran en la figura 2.9.

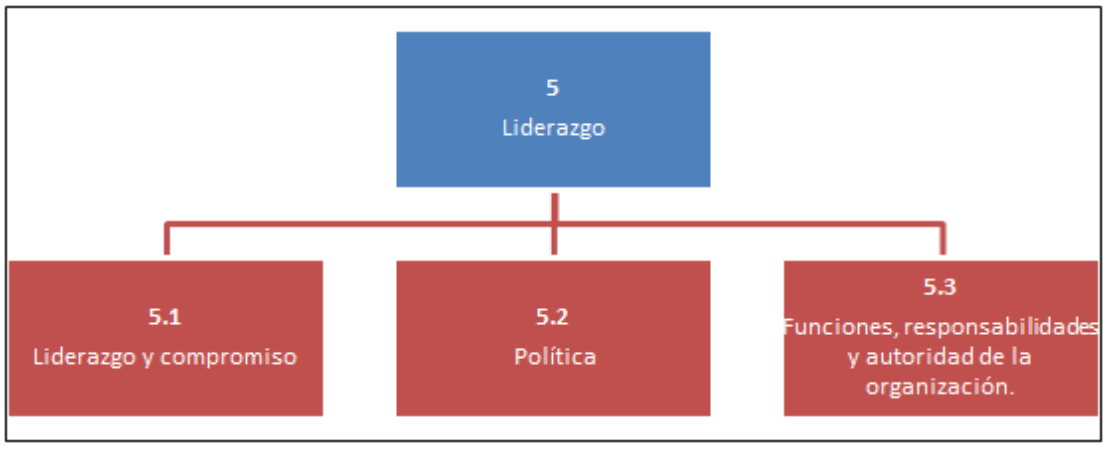


Figura 2. 9 Estructura de la cláusula 5 – ISO/IEC 27001:2013

El establecimiento de la política de seguridad de la información es responsabilidad de la Alta Dirección de la organización y debe incluir los objetivos de seguridad de la información y el compromiso de la mejora continua. La política es información documentada del SGSI y debe estar disponible para las partes interesadas y ser comunicada internamente.

La Alta Gerencia debe velar que las responsabilidades y autoridad para los roles en la seguridad de la información sean asignados y comunicados, dentro de las responsabilidades se encuentra:

- Garantizar que el SGSI se adapta a los requisitos de ISO 27001:2013.
- Informar el desempeño del SGSI.

Cláusula 6 – Planificación.

La planificación del Sistema de Gestión de Seguridad de la información consta de dos partes, tal como se muestra en la Figura 2.10.

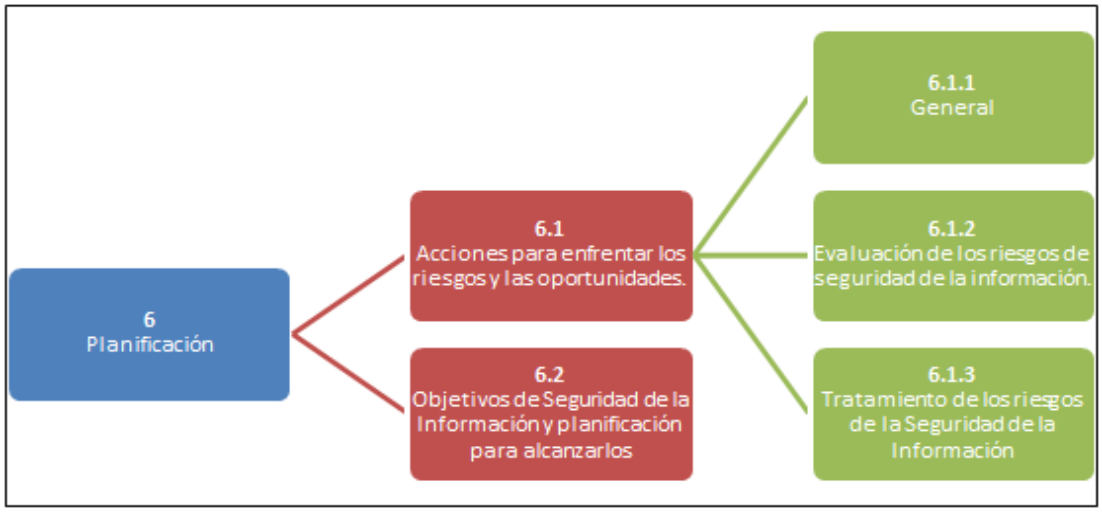


Figura 2. 10 Estructura de la cláusula 6 – ISO/IEC 27001:2013

En la primera parte de la planificación del SGSI se toman en cuentan los asuntos internos y externos, los requisitos de las partes interesadas para identificar los riesgos y oportunidades con el propósito de que el SGSI logre los resultados, mejore continuamente o evite efectos no deseados. Se deben planificar las acciones para atender los riesgos y oportunidades.

Es de vital importancia que la organización evalúe los riesgos de seguridad de la información siguiendo un proceso o metodología que permita:

- Establecer criterios de aceptación del riesgo.
- Definir criterios para el desempeño de las evaluaciones de los riesgos.
- Identificar riesgos de seguridad de la información
- Identificar a los originadores de los riesgos.
- Analizar los riesgos evaluando sus consecuencias y sus probabilidades de ocurrencia.
- Determinar niveles de riesgo.
- Priorizar riesgos para su posterior tratamiento.

Con los resultados de la evaluación de riesgos de seguridad de la información, la organización debe seleccionar las opciones de tratamiento de los riesgos y definir tomando como referencia el Anexo A los controles que pueden implementar y que apoyan al tratamiento de los riesgos. Los poseedores de riesgos deben aprobar su plan de tratamiento de riesgos y aceptar los riesgos residuales.

Cabe recalcar que se debe conservar información documentada asociada al proceso de evaluación de riesgos de la seguridad de la información y su plan de tratamiento.

Es mandatorio elaborar una Declaración de Aplicabilidad en la cual constan todos los objetivos de control y controles del Anexo A, en este documento se debe especificar si estos fueron seleccionados o no y justificar el motivo de su inclusión o exclusión según sea el caso.

En la cláusula 6.2 se especifica que la Organización debe establecer los objetivos de seguridad de la información los cuales deben estar relacionados y ser consistentes con la política de seguridad, ser medibles en caso de que aplique y difundir o comunicarlos. Los objetivos de seguridad de la información deben quedar registrados como información documentada.

La organización debe planificar como alcanzar los objetivos planteados respecto a la seguridad de la información, para lo cual debe determinar:

- ¿Qué hacer?
- Recursos necesarios.
- ¿Quién es el responsable?
- ¿Cuándo se alcanzará el objetivo?
- ¿Cómo medir los resultados?

Cláusula 7 – Apoyo/Soporte.

Esta sección del estándar cuenta con cinco partes las cuales se muestran en la figura 2.11. Dentro de un SGSI la asignación de recursos (Cláusula 7.1) para establecer, implementar, mantener y mejorar el sistema es una acción de apoyo al sistema. Respecto a la competencia de las personas se debe garantizar que sea en base a:

- Educación
- Entrenamiento
- Experiencia

En caso de que el personal no cuente con las competencias necesarias, se deben tomar acciones que permitan adquirirlas y evaluar la efectividad de las acciones. Es importante contar con la información correspondiente la cual sirve como evidencia de la competencia del personal.

La cláusula 7.3 respecto a concientización es muy clara con la información con la cual el personal debe estar consciente dentro de la organización las cuales son:

- Política de Seguridad.
- Su contribución al SGSI.
- Consecuencias de la no conformidad con los requisitos del SGSI.

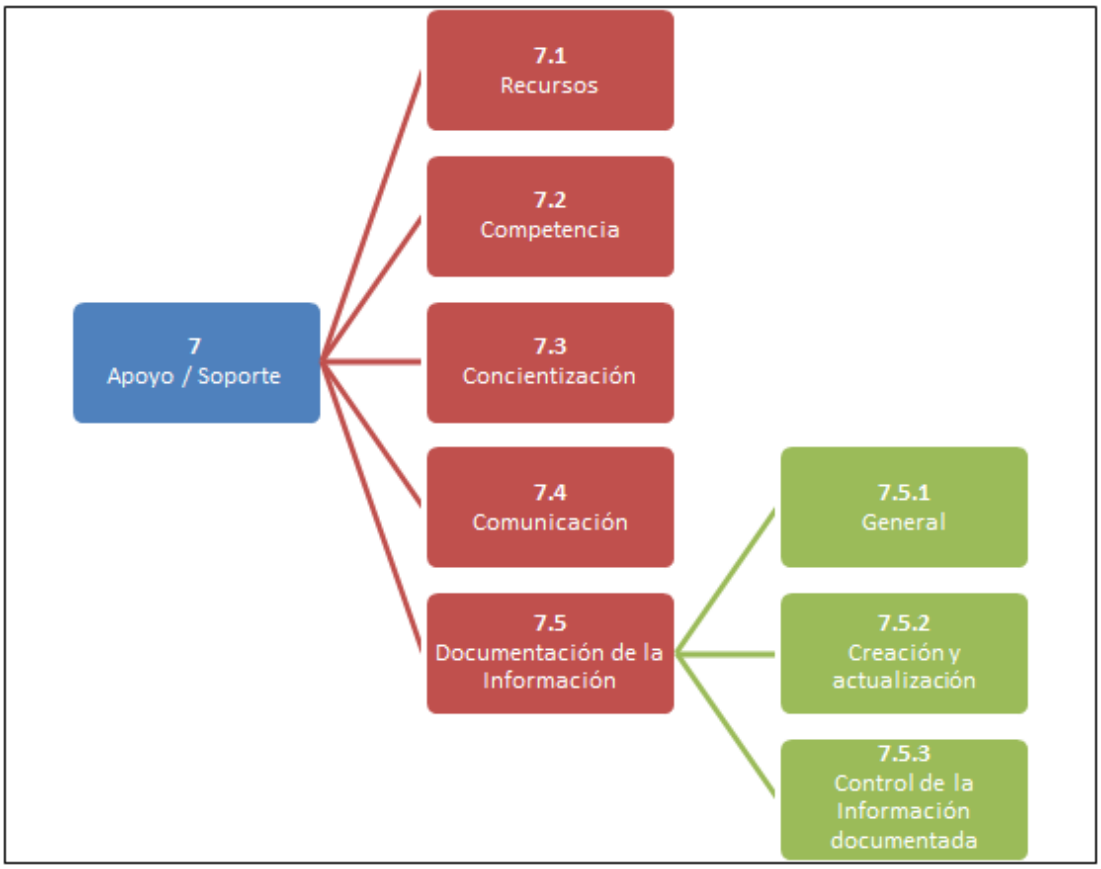


Figura 2. 11 Estructura de la cláusula 7 – ISO/IEC 27001:2013

Otro tema relevante dentro del SGSI es la comunicación interna y externa respecto al SGSI, para lo cual la organización debe definir lo siguiente:

- ¿Qué se debe comunicar?
- ¿Cuándo?
- ¿A quién?
- ¿Quién es el responsable de comunicar?
- Proceso mediante el cual se hace efectiva la comunicación.

Para demostrar conformidad con los requisitos del sistema a lo largo de esta revisión en algunos puntos se ha recalcado la importancia de mantener información documentada, para lo cual en la cláusula 7.5 se presentan los requisitos asociados a la creación, actualización y control de documentación de origen interno y externo necesaria para el SGSI.

Cláusula 8 – Operación.

En esta sección se ejecuta lo planificado en la cláusula 6, manteniendo evidencia. En la figura 2.12 se muestra la estructura.

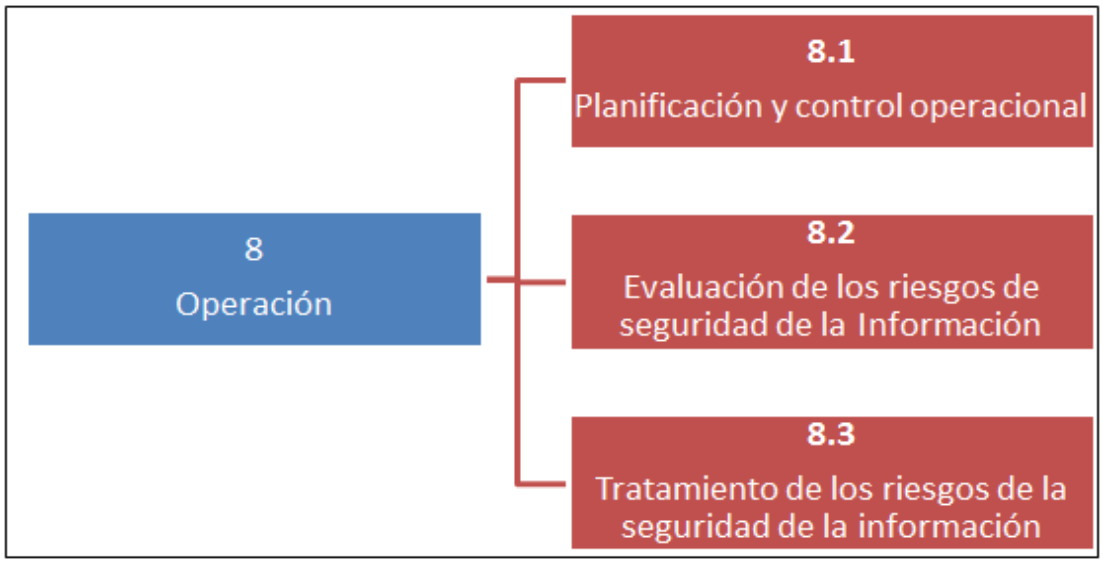


Figura 2. 12 Estructura de la cláusula 8 – ISO/IEC 27001:2013

Cláusula 9 – Evaluación del desempeño.

Mediante esta cláusula la organización puede medir y evaluar el desempeño de su SGSI, como se muestra en la figura 2.13 consta de tres partes.

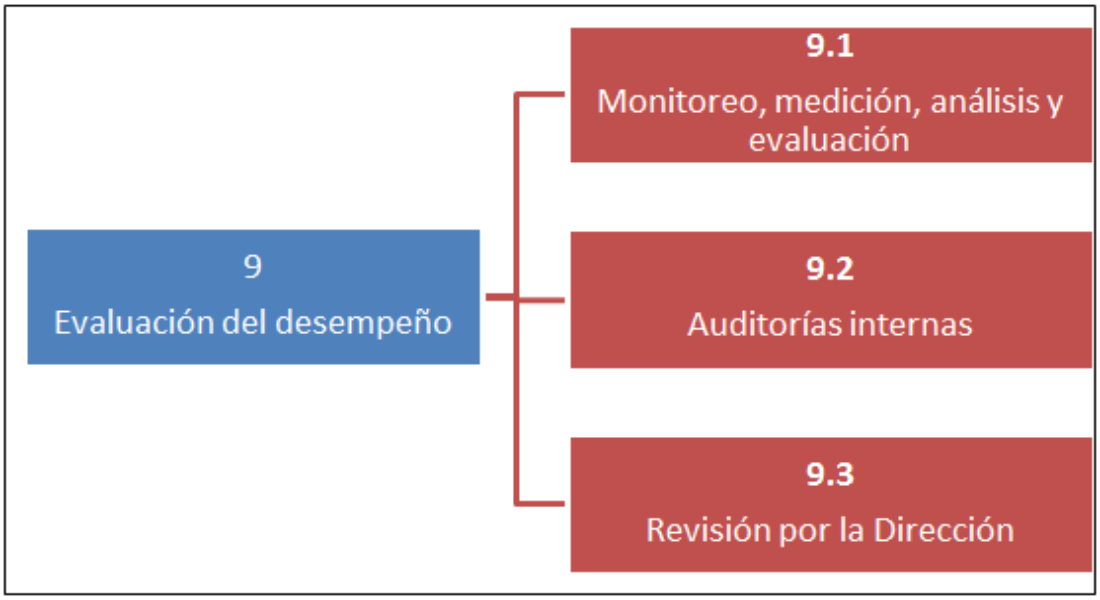


Figura 2. 13 Estructura de la cláusula 9 – ISO/IEC 27001:2013

La cláusula 9.1 tiene como objetivo evaluar el desempeño y efectividad del SGSI de la organización para lo cual se debe determinar:

- ¿Qué se debe monitorear?
- Métodos de monitoreo y medición.
- Frecuencia de ejecución.
- ¿Quién realiza monitoreo y medición?
- ¿Cuándo se evalúa y analiza los resultados?

Se debe mantener la información documentada de los resultados del monitoreo y medición ya que sirven como evidencia del SGSI.

Las auditorías internas son un mecanismo mediante el cual se puede evaluar si el SGSI se ha implementado y se mantiene de manera efectiva. Es

importante conservar información de los programas y resultados de auditoría como evidencia.

Debido al compromiso y liderazgo que tiene la Alta Dirección con el SGSI, es importante que realice la revisión del SGSI, para ejecutar esa tarea la revisión debe incluir lo siguiente:

- Estado de acciones de revisiones previas por parte de la Dirección.
- Cambios en asuntos internos y externos que afecten al SGSI.
- Retroalimentación del desempeño basado en:
    - No conformidades y acciones correctivas.
    - Resultados de Monitoreo y medición.
    - Resultados de auditoría.
- Cumplimiento de objetivos de seguridad de la información
- Resultados de evaluación de riesgos.
- Estado del Plan de tratamiento de los riesgos.
- Oportunidades de mejora.

Los resultados de la revisión por parte de la Alta dirección deben incluir las decisiones relacionadas con las oportunidades de mejora y cambios en el SGSI. Se debe conservar evidencia de los resultados de la revisión.

Cláusula 10 – Mejora.

La cláusula, tal como se muestra en la figura 2.14 cuenta con dos partes, la primera asociada a las no conformidades y acciones correctivas y la última respecto a la mejora continua.

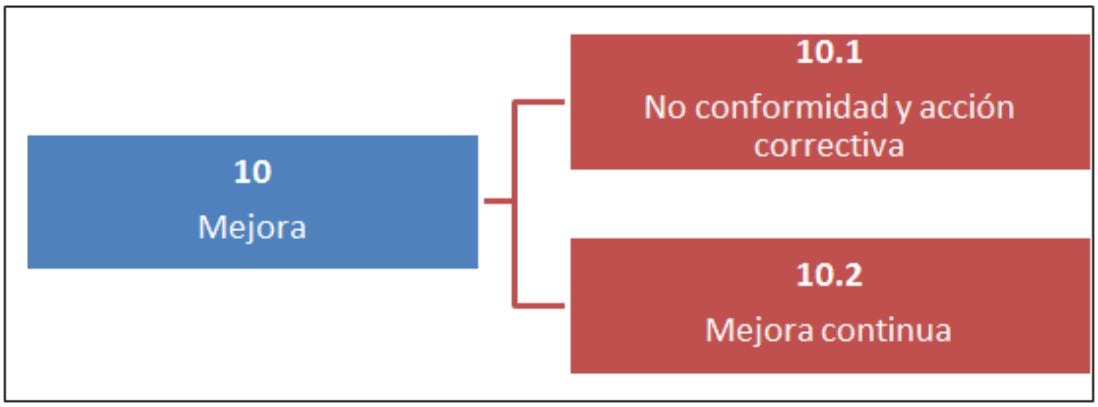


Figura 2. 14 Estructura de la cláusula 10 – ISO/IEC 27001:2013

Al identificar no conformidades en el SGSI de la organización se debe:

- Tomar acciones para controlar y corregir.
- Lidiar con las consecuencias.
- Evaluar las acciones para eliminar las causas de la NC, con el propósito de evitar la recurrencia.

Las acciones correctivas deben ser coherentes a los efectos de las NC identificadas en el SGSI. Es importante mantener registro de:

- Naturaleza de las NC y cualquier acción tomada.
- Resultados de las acciones correctivas.

Anexo A – Objetivos de control y controles de referencia.

La norma cuenta con el Anexo el A cuya introducción es simplificada y establece que los objetivos de control y controles se derivan de ISO/IEC 27002:2013 y que se utiliza en el contexto de la cláusula 6.1.3 Tratamiento de los riesgos de seguridad de la información. El anexo tiene un total de 114 controles y 14 dominios los cuales se muestran en la Tabla 4.

Tabla 4 Dominios de Seguridad - Anexo A - ISO/IEC 27001:2013

Dominios de Seguridad
A.5 Políticas de seguridad de la información
A.6 Organización de la seguridad de la información
A.7 Seguridad de los recursos humanos
A.8 Gestión de los activos
A.9 Control de acceso
A.10 Criptografía
A.11 Seguridad física y medioambiental
A.12 Seguridad de las operaciones
A.13 Seguridad de las comunicaciones
A.14 Adquisición, desarrollo y mantenimiento del sistema
A.15 Relación con proveedores
A.16 Gestión de los incidentes de seguridad de la información
A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio
A.18 Cumplimiento

2.3 COMPARAR LAS VERSIONES 2005 Y 2013 DEL ESTÁNDAR ISO 27001.

Luego de revisar la estructura de las dos versiones del estándar ISO/IEC 27001, es relevante destacar que en la versión 2013 ya no se incluye el enfoque de procesos mediante el modelo PDCA como se define en la versión 2005 [4]. La estructura del estándar vigente (2013) es de alto nivel basado en el Anexo SL, el cual tiene como propósito estandarizar terminología y los requisitos fundamentales de los sistemas de gestión para sean compatibles los sistemas de gestión basados en diferentes normas.

Se considera que el modelo PDCA está embebido en la nueva versión del estándar tal como se muestra en la figura 2.15.

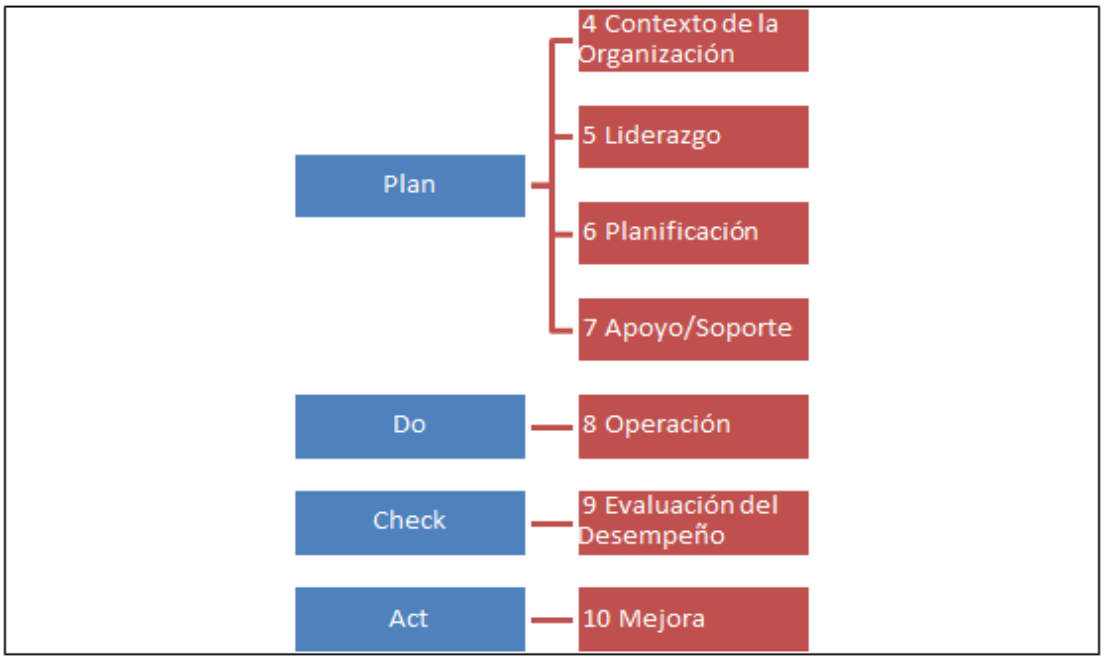


Figura 2. 15 Relación de cláusulas de ISO/IEC 27001 con modelo PDCA

Los términos y definiciones fueron removidos de la versión 2013, sin embargo en esta cláusula se hace referencia al documento ISO/IEC 27000 que es el que contiene las definiciones asociadas el SGSI.

En la Tabla 5 se muestra la comparación de la estructura de las dos versiones de la norma, se puede observar un incremento en cláusulas de 5 a 7 y dominios de control de 11 a 14, sin embargo la cantidad de controles disminuyó de 133 a 114.

Tabla 5 Comparación entre ISO/IEC 27001:2005 y 2013 de su estructura

ESTRUCTURA	ISO IEC/27001:2005	ISO/IEC 27001:2013
Cláusulas	5	7
Dominios de control	11	14
Controles	133	114

En la Tabla 6 se presenta la comparación de las cláusulas de ambas versiones, vale la pena recalcar que en la nueva versión los requerimientos permiten que la organización tenga más libertad para implementarlos en su SGSI.

Tabla 6 Comparación de cláusulas entre ISO/IEC 27001:2005 y 2013

ISO IEC/27001:2005	ISO/IEC 27001:2013
4 Sistema de gestión de Seguridad de la Información	4 Contexto de la organización
5 Responsabilidad de la gerencia	5 Liderazgo
6 Auditorías Internas del SGSI	6 Planificación
7 Revisión gerencial del SGSI	7 Apoyo/Soporte
8 Mejoramiento del SGSI	8 Operación
	9 Evaluación del desempeño
	10 Mejora

En la nueva versión de la norma se han actualizado o agregado ciertos conceptos, los cuales se presentan a continuación [5]:

- Contexto de la organización – Ambiente en el que opera la organización.
- Riesgos y oportunidades – Reemplaza las acciones preventivas, ya que este término se ha eliminado.
- Partes interesadas – Reemplaza al término accionistas.
- Liderazgo – Esta sección cuenta con requisitos específicos para la alta dirección.
- Comunicación – Se especifica los requerimientos para las comunicaciones internas y externas.
- Evaluación de riesgos – La identificación de activos, sus amenazas y vulnerabilidades ya no son prerrequisitos obligatorios para la evaluación del riesgo, toma como referencia ISO 31000
- Propietario del riesgo – Reemplaza al propietario de los activos.
- Información documentada – Reemplaza a control de documentos y registros.
- Evaluación del desempeño – Cubre las mediciones del SGSI y la efectividad del plan de tratamiento de riesgos.
- Mejora continua – Es factible utilizar metodologías diferentes a PDCA.

Respecto a los dominios de control del anexo A, se observa un incremento en los mismos sin embargo mantienen relación con los dominios de control de la versión 2005, tal como se muestra en la Tabla 7.

Tabla 7 Relación de dominios de control

ISO/IEC 27001:2005	ISO/IEC 27001:2013
5 Política de Seguridad	5 Política de Seguridad
6 Organización de la seguridad de la información	6 Organización de la seguridad de la información
8 Seguridad de Recursos Humanos	7 Seguridad de recursos humanos
7 Gestión de Activos	8 Gestión de activos
11 Control de Acceso	9 Control de Acceso
12 Adquisición de sistemas de información, desarrollo y mantenimiento	10 Criptografía
9 Seguridad física y ambiental	11 Seguridad física y ambiental
10 Comunicaciones y gestión de operaciones	12 Seguridad de Operaciones 13 Seguridad en las comunicaciones
12 Adquisición de sistemas de información, desarrollo y mantenimiento	14 Adquisición de sistemas, desarrollo y mantenimiento 15 Relaciones con suplidores
13 Gestión de incidentes de seguridad de la información	16 Gestión de incidentes de seguridad de la información
14 Gestión de la continuidad del negocio	17 Aspectos de seguridad de información de la gestión de continuidad del negocio.
Cumplimiento	18 Cumplimiento

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 LISTADO DE REQUISITOS A IMPLEMENTAR BASADO EN ISO/IEC 27001:2013.

El sistema de gestión de seguridad de la información de una organización para dar cumplimiento con los requisitos del estándar ISO/IEC 27001:2013 requiere tener cierta documentación y cumplir con requisitos que son muy importantes, los cuales menciono a continuación:

- Alcance del SGSI.
- Política de Seguridad de la Información
- Proceso de evaluación de riesgos de seguridad de la información
- Declaración de Aplicabilidad
- Acciones para atender riesgos y oportunidades.
- Procedimiento de control de información documentada.
- Monitoreo, medición, análisis y evaluación.

3.2 LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LOS REQUISITOS DEL LISTADO.

El listado que se menciona en la sección 3.1 en este trabajo es el más relevante para la migración del SGSI y que requiere que la organización los revise de manera detallada.

Alcance del SGSI

El alcance del SGSI se puede mantener en la organización, sin embargo dicho documento debe incluir el contexto de la organización, es decir identificar los asuntos internos y externos podrían afectar a la seguridad de la información, además de las partes interesadas con sus necesidades y expectativas.

Política de Seguridad de la Información

En la versión 2005 se la llamaba “Política de Sistema de gestión de seguridad de la información”, para la transición no se requiere cambiar el nombre a la misma.

Proceso de evaluación de riesgos de seguridad de la información

En la nueva versión de la norma la evaluación de riesgos tiene su enfoque en las consecuencias y no es mandatorio el identificar los activos sus amenazas y vulnerabilidades para este proceso.

Declaración de Aplicabilidad

Es un documento mandatorio en el SGSI, el cual debido a los cambios del estándar este se debe revisar en su totalidad de tal manera que los controles seleccionados para atender los riesgos sean los adecuados para velar por la seguridad de la información.

Acciones para atender riesgos y oportunidades.

Estas acciones reemplazan al término “acciones preventivas” de ISO/IEC 27001:2005 y se definen en base a la revisión de asuntos internos y externos que pudieran afectar al logro de objetivos del SGSI más las necesidades y expectativas de las partes interesadas.

Procedimiento de control de información documentada.

En la versión 2005 se contaba con los procedimientos de control de documentos y registros para el SGSI, sin embargo en la nueva versión esta terminología se eliminó y ahora se utiliza “información documentada” por lo tanto se debe actualizar el procedimiento para utilizar el término actual.

Monitoreo, medición, análisis y evaluación.

Esta sección hace referencia a los requisitos de la cláusula 9.1 de la versión 2013, en la cual los requisitos tienen más detalle con el propósito de medir la eficacia del SGSI, se debe contar con evidencia de los resultados obtenidos por monitoreo.

CONCLUSIONES

1. La estructura del estándar ISO/IEC 27001:2013 es más sencilla de entender y permite que las organizaciones implementen su SGSI de acuerdo sus necesidades respecto a la seguridad de la información sin dejar de lado su visión estratégica.
2. A pesar de ser sencilla la nueva estructura del estándar, su implementación puede ser compleja, por lo que se requiere que la organización gestione sus riesgos relacionados con la seguridad de la información de manera adecuada y que evalué constantemente su SGSI para validar la eficacia el mismo, buscar la mejora continua y proporcionar confianza a sus clientes.
3. La migración de un SGSI implementado en ISO/IEC 27001:2005 hacia la versión 2013 puede ser sencilla ya que las organizaciones cuentan con una base de procedimientos, políticas establecidas e implementadas de su sistema de seguridad de la información, sin

embargo esto depende del tamaño de la organización y madurez de su sistema.

4. Al migrar el Sistema de gestión de seguridad de la información para cumplir con los requisitos de ISO/IEC 27001:2013, este se podrá integrar a otros sistemas de gestión que cuenten con la estructura del Anexo SL, lo cual es ventaja ya que poco a poco otras normas utilizarán esa estructura de alto nivel.

RECOMENDACIONES

1. Para la migración del SGSI de una organización hacia la nueva versión, los responsables del sistema deben conocer y entender los requisitos del estándar, identificar los requisitos que requieren una revisión minuciosa para su implementación o actualización.

2. Para la transición del SGSI de la versión 2005 a la 2013 se recomienda mantener la metodología el análisis y evaluación de riesgos implementados, sin embargo se debe identificar al propietario del riesgo, y contar con la aprobación del riesgo residual. Los controles seleccionados para el tratamiento de los riesgos deben ser revisados a detalle y seleccionar los controles correspondientes al Anexo A.

BIBLIOGRAFÍA

[1]. ISO/IEC 27001, “Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información”, Primera Edición 2005 – 10 - 15, fecha de consulta Julio 2015

[2]. ISO27000, Implantación del ISO 27001:2005, http://www.iso27000.es/download/Implantacion_del_ISO_27001_2005.pdf, fecha de consulta Julio 2015

[3]. ISO/IEC 27001:2013, “Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos”, Segunda Edición 2013 – 10 -01, fecha de consulta Julio 2015

[4]. Eficiencia Gerencial, Nuevo estándar en Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2013, http://eficienciagerencial.com/tienda/temario/nuevo_sgsi_2013.pdf, fecha de consulta Julio 2015

[5]. BSI, Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013, http://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf, fecha de consulta Julio 2015