GUIA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN INTEGRADO ISO 9001:2015 E ISO/IEC 27001:2013

JHON FREDY PINEDA

FUNDACION UNIVERSIDAD DE AMÉRICA
FACULTAD DE EDUCACIÓN PERMANENTE Y AVANZADA
ESPECIALIZACIÓN EN GERENCIA DE LA CALIDAD
BOGOTÁ D.C.
2017

GUIA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN INTEGRADO ISO 9001:2015, ISO/IEC 27001:2013

JHON FREDY PINEDA

Monografía para optar el título de Especialista en
Gerencia de la Calidad

Orientador:

Angélica María Álzate Ibáñez
Magíster, Ingeniera Química

FUNDACION UNIVERSIDAD DE AMÉRICA
FACULTAD DE EDUCACIÓN PERMANENTE Y AVANZADA
ESPECIALIZACIÓN EN GERENCIA DE LA CALIDAD
BOGOTÁ D.C
2017

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Firma del Director de la Especialización

_____
Firma del calificador

Bogotá, 29 de marzo de 2017

DIRECTIVAS DE LA UNIVERSIDAD

Presidente de la Universidad y Rector del claustro

Dr. Jaime Posada Díaz

Vicerrectora Académica y de Postgrados

Dra. Ana Josefa Herrera Vargas

Vicerrector de Desarrollo y Recursos Humanos

Dr. Luis Jaime Posada García Peña

Secretario General

Dr. Juan Carlos Posada García Peña

Decano de facultad de Educación Permanente y Avanzada

Dr. Luis Fernando Romero Suarez

Director Especialización en Gerencia de la Calidad

Dr. Emerson Mahecha Roa

Las directivas de la Universidad de América, los jurados calificadores y el cuerpo docente no son responsables por los criterios e ideas expuestas en el presente documento. Estos corresponden únicamente a los autores.

DEDICATORIA

Deseo expresar mi agradecimiento a todas las personas, que directamente tuvieron que ver con este nuevo reto en mi vida, especialmente a mi madre Beatriz Pineda Santos, por su constante estimulo, a todos los profesores que aportaron con su valioso conocimiento para poder concluir de forma satisfactoria la Especialización en Gerencia de la Calidad.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ACCIONES CORRECTIVAS: permite registrar y realizar el tratamiento, seguimiento y cierre de las acciones correctivas.

ACCIONES PREVENTIVAS: permite registrar y realizar el tratamiento, seguimiento y cierre de las acciones preventivas.

ALTA DIRECCION: persona o grupo de personas que dirige y controla una organización al más alto nivel.

ASEGURAMIENTO DE LA CALIDAD: parte de la gestión de la calidad orientada a proporcionar confianza de que se cumplan los requisitos de la calidad. Definición tomada de la Norma Técnica.

ANÁLISIS DEL RIESGO: uso sistemático de la información para identificar las fuentes y estimar el riesgo

CALIDAD: grado en el que un conjunto de características inherentes cumple con los requisitos. Definición tomada de la Norma Técnica Colombiana NTC-ISO9000:2000, Instituto Colombiano de Normas Técnicas y certificación (ICONTEC).

CLIENTE: persona u organización que podría recibir o que recibe un producto o un servicio destinado a esa persona u organización o requerido por ella.

COMPROMISO: participación activa en, y contribución a, las actividades para lograr objetivos compartidos

COMPETITIVIDAD: es la capacidad de una organización para obtener rentabilidad en el mercado en relación a sus competidores.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados

CONTROL: medio para gestionar un riesgo, asegurando que se alcance un objetivo de negocio o que se siga un proceso.

CONTROL DE LA CALIDAD: parte de la gestión de la calidad orientada al cumplimiento de los requisitos de la calidad

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada

EFICACIA: grado en el que se realiza las actividades planificadas y se logran los resultados planificados.

EFICIENCIA: relación entre el resultado alcanzado y los recursos utilizados.

GESTIÓN: actividades coordinadas para dirigir y controlar una organización.

MEJORA: actividad para mejorar el desempeño.

NO CONFORMIDADES: permite registrar y realizar el tratamiento, seguimiento y cierre de las no conformidades

ORGANIZACIÓN: persona o grupo de personas que tienen sus funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

PARTICIPACION ACTIVA: tomar parte en una actividad, evento o situación.

PROCESO: conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado.

PROCEDIMIENTO: forma especificada de llevar a cabo una actividad o un proceso.

REQUISITO: necesidad o expectativa establecida, generalmente implícita u obligatoria.

REQUISITO DE CALIDAD: requisito relativo a la calidad.

RIESGO: posibilidad de que una amenaza se materialice.

SERVICIO AL CLIENTE: interacción de la organización con el cliente a lo largo del ciclo de vida de un producto o un servicio.

SISTEMA: conjunto de elementos interrelacionados o que interactúan.

SISTEMA DE GESTIÓN: conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para logar los objetivos.

SISTEMA DE GESTIÓN DE LA CALIDAD: parte de un sistema de gestión relacionada con la calidad.

GESTION DEL RIESGO: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad

RESUMEN

En este trabajo se presenta una guía para la implementación de un sistema integrado de gestión basado en los requisitos de las normas ISO 9001:2015 y la ISO/IEC 27001:2013. La guía está dirigida a cualquier tipo de organización sin importar su tamaño o actividad económica o alguna persona que la tome como guía de implementación, como sabemos estas normas hoy en día son una necesidad para que las empresas puedan sobre salir en el mercado actual, como estas normas tienen grandes similitudes y para implementar las dos normas, muchas veces se repite mucha información y el esfuerzo es mucho mayor, por tal razón lo mejor es hacer un sistema integrado de gestión, ya que minimiza el esfuerzo y esto permite el crecimiento de la organización hacia el éxito, ya que cuenta con estándares de calidad.

Por tal razón primero se describe las generalidades de cada una de las normas incluyendo aspectos tales como la historia y su estructura, con el fin de tener claro sus similitudes y diferencias. A partir de estas generalidades se podrá entender que estas normas la ISO 9001:2015 y la ISO/IEC 27001:2013 tienen una misma filosofía, la ISO 9001 se ha desarrollado por la competitividad y la necesidad de permanecer en el espacio empresarial, mientras que la norma ISO/IEC 27001 ha sido promovida por el rápido crecimiento de las tecnologías de la información.

El sistema integrado de la calidad y de la seguridad de la información, es una decisión estratégica que involucra a toda la organización y para poder llegar a tener éxito debe ser apoyada por la alta gerencia; se proyecta que al implementar el sistema integrado de gestión a la organización mejorara su desempeño y productividad.

Palabras Claves: Integración de sistemas de gestión, ISO 9001:2015, ISO/IEC27001:2013, calidad.

INTRODUCCIÓN

En la actualidad, gran cantidad de organizaciones, dentro de las cuales se encuentran las empresas del sector TI, están en el proceso de implementación de un sistema de gestión con la cual buscan la fiabilidad de cada uno de sus procesos. La necesidad de tener una enfoque general de los sistemas de gestión para que sean compatibles entre si, para de esta forma tener los objetivos alineados y tomar de una manera más clara las decisiones.

Inicialmente los modelos de calidad se centraban en operar en la inspección y planeación a corto plazo, su apoyo principal radica en las ganancias y no en el cliente, trabajaban de una forma rígida y vertical y no innovaban en sus procesos. El ingreso de nuevos mercados los cuales traen nuevas metodologías, a largo plazo con una mejora continua a cada uno de sus productos y procesos ha causado la necesidad de cambiar la forma de hacer negocios. Las empresas van definiendo e implementando sistemas de gestión certificables lo cual hace cada vez más evidente la necesidad de unir esfuerzos, recursos y costos destinados a los mismos cuando estas normas comparten requisitos y metodologías de gestión similares.

De acuerdo con Cortés y Ardila[1], para asegurar la competitividad y ser líder en el mercado, una organización debe mostrar que cada uno de sus servicios son gestionados de una manera eficiente, segura y eficaz; una manera efectiva de lograr las nuevas metas es la implementación de sistemas de calidad documentados según los requisitos establecidos en la norma ISO9001:2015, ISO/IEC27001:2013

Las normas ISO9001:2015 y la ISO/IEC27001:2013 son una necesidad para que las empresas puedan sobre salir en el mercado actual, ambas normas tienen grandes similitudes y muchas veces cuando se implementa las dos normas ISO 9001:2015 y ISO/IEC 27001, las organizaciones repiten mucha documentación por el afán de cumplir con los requisitos que son exigidos, para mejorar esto se tiene UN SISTEMA DE GESTION INTEGRADO, donde se realizara el análisis de las normas, en donde obtendremos las diferencias y concordancias, para de esta manera ayudar a las empresas que realicen una implementación más efectiva de estas normas.

Inicialmente se identifica algunas actividades involucradas en las normas ISO9001:2015 y la ISO/IEC27001:2013, las organizaciones son sistemas complejos e integrales, las cuales están conformadas por recursos físicos como humanos, las empresas han tomado la iniciativa de adecuar sus procesos a lo que está

[1] CORTÉS R., Diana Marcela y ARDILA, Alix Victoria. Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001 [en línea]. Trabajo de grado Especialista en Gerencia de Procesos y Calidad. Bogotá: Universidad EAN, 2012 [consulta: 10 de diciembre de 2016]. Disponible en internet: <http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2>.

establecido por las normas vigentes y para ello es necesario una revisión y adecuación de los sistemas de gestión, los cuales deben estar delineados de forma que se pueda dar un mejor manejo a los recursos. “Para tener éxito en la implementación del sistema de gestión debe ser una decisión que involucra a toda la organización”[2]

El objetivo es ofrecer un guía de implementación, para la implementación del Sistema Integrado de Gestión, depende del tamaño, y en qué estado se encuentra el sistema de gestión de la organización, a la cual se le implementará el sistema, para el desarrollo de este sistema de gestión integrado es necesario basarnos en los requisitos que exigen las normas ISO9001:2015 y ISO/IEC27001:2013, la metodología es descriptiva ya que por este medio se podrá definir, clasificar, y categorizar

La norma ISO/IEC27001:2013 es una norma que nos permite salvaguardar la información de las partes interesadas, es adecuada para proteger la integridad y disponibilidad de la información; Los clientes cuando tienen el conocimiento de que cuentan con una empresa certificada, profesan confianza y respaldo en que los productos y servicios que se están ofreciendo, cuentan con unos controles basados en estándares, que permiten disminuir los riesgos y a través de esto llegar al éxito organizacional.

[2] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

OBJETIVOS

OBJETIVO GENERAL

Realizar una guía de implementación del Sistema de Gestión Integrado basado en los requisitos de las normas ISO9001:2015 y la ISO/IEC27001:2013 en empresas del sector TI.

OBJETIVOS ESPECÍFICOS

- Realizar un análisis de la estructura y requisitos establecidos en las normas ISO9001:2015, ISO/IEC27001:2013.

- Identificar concordancias y diferencias entre los diferentes requisitos de las normas ISO9001:2015, ISO/IEC27001:2013, con el fin de realizar la Integración del Sistema de Gestión.

- Describir las etapas y actividades necesarias para realizar la Integración de los Sistemas de Gestión basados en los requisitos de las normas ISO9001:2015, ISO/IEC27001:2013 en empresas del sector TI.

- Determinar los factores claves a tener en cuenta para la implementación de estas normas, de manera que si son exitosas aseguren el funcionamiento competitivo de las organizaciones.

1. METODOLOGÍA

1.1 TIPO DE INVESTIGACIÓN

La investigación a realizar es de tipo documental, y el alcance de esta investigación es de tipo descriptivo.

1.2 FUENTES DE INFORMACIÓN

Como fuente de información se hará uso de las bibliotecas públicas, bases de datos suscritas por la Universidad, en especial las que corresponden a la consulta de las normas ICONTEC (ISO 9001:2015, ISO/IEC 27001:2013) y las bases de datos de acceso libre

1.3 ACTIVIDADES DETALLADAS

Revisión bibliográfica: esta etapa se realiza durante todo el desarrollo del trabajo de grado y corresponde a la búsqueda y recuperación de información relacionada con el tema objeto de estudio. La información recopilada será analizada y clasificada de acuerdo a los criterios de búsqueda establecidos, esta revisión dará lugar al marco teórico de la monografía, el cual incluirá principalmente unos componentes conceptuales e históricos, aplicaciones y casos de estudio.

- Se realiza un estudio en detalle de cada uno de los requisitos de las normas con el fin de identificar los aspectos claves y diferenciadores, la coherencia entre normas, se realizara un paralelo entre las normas.

- Se definirán las etapas y actividades requeridas para realizar el proceso de implementación del sistema integrado de gestión a partir del estudio realizado a las normas, la revisión documental y el criterio del investigador basado en su experiencia, se describen las actividades que sean necesarias para la implementación de un sistema de gestión integrado teniendo en cuenta los requisitos establecidos en las normas.

- Se establecerá una guía metodológica involucrando los aspectos claves a tener en cuenta para la implementación de un sistema de gestión integrado basado en los requisitos de las normas ISO 9001:2015, ISO 27001:2013, la cual servirá de orientación a empresas del sector TI.

- Conclusiones y recomendaciones: a partir del estudio realizado se detallaran las conclusiones del estudio y se propondrán recomendaciones a las organizaciones o empresas que deseen realizar la implementación de las normas.

2. SISTEMAS DE GESTIÓN DE LA CALIDAD

2.1 EVOLUCIÓN HISTÓRICA DE LA CALIDAD.

Uno de los más antiguos referentes sobre el concepto de calidad, aparece en el código de Hammurabi (2150 a. de C.), según Laboucheix "si un albañil ha construido una casa y, no siendo ésta suficientemente sólida, se hunde y mata a sus ocupantes, el albañil deberá ser ejecutado"[3]. "ya entonces surgía la noción de calidad asociado a una responsabilidad para con otras personas..."[4], desde aquellos tiempos se busca la satisfacción de los clientes, a cambio de lo personal, concepto relacionado e implantado como norma en ISO 9001:2015

Posteriormente, desde la época de la revolución industrial (mediados del siglo XVIII), con la realización de actividades o productos por más de un trabajador, llevo a la estandarización y hacer que se tengan claras las especificaciones, aparecen con ello conceptos como las inspecciones, para que los productos coincidan con su respectiva especificación, separándose en pleno auge del Taylorismo (finales del siglo XIX) la planificación (el pensar) de la ejecución (el hacer) de los productos.

Posteriormente al Taylorismo, Henry Ford con su producción en cadena, hace que las funciones de planificación, ejecución e inspección se separen. "En dicho sistema basado en la inspección, se emplearon desarrollo de técnicas de muestreo centradas en los riesgos del comprador, del proveedor y niveles de calidad aceptables"[5].

Los principales representantes de la calidad moderna aparecen con sus ideas en el siglo XX: George Edwards, creando la noción de aseguramiento de la calidad; Walter Shewhart, quien "fue el primero en reconocer que la variabilidad (diferencias reales entre productos teóricamente idénticos) es inherente a la fabricación industrial, pero que puede ser medida y controlada mediante herramientas estadísticas. de esta forma introdujo el control estadístico aplicado a los procesos de producción industrial, con el fin de disminuir la variabilidad y mejorar la fiabilidad de los sistemas de transmisión fabricados en la compañía"[6]

---

[3] LABOUCHEIX, Vincent. Tratado de la calidad total. México: Limusa, 2001, p. 14

[4] ZUBIETA GUILLÉN, José M.a y ALFARO LARRAGUETA, Eduardo Alfaro. Soluciones en las empresas de TI mediante la aplicación de un sistema de gestión ISO 20000 parte 1 integrado a un sistema ISO 27001 e ISO 9001 [en línea]. Trabajo de grado Ingeniero Técnico Industrial Eléctrico. Pamplona (España): Universidad Pública de Navarra, 2010 [consulta: 20 de noviembre de 2016], p

[5] Ibíd., p. 6.

[6] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

Armand Feigenbaum, con un artículo publicado en 1945, desarrolla la primera aplicación de gestión de calidad, con el concepto de Calidad Total. Joseph Juran, en los años 50 plantea la gestión de la calidad con la relación de tres conceptos: plantificación, control, y mejora continua[7]; Edward Deming dio nombre a la metodología conocida como “Ciclo Deming” (PDCA), aunque Walter Shewhart fue quien lo desarrollo.

En la tabla 1, se describe una cronología, referente a todos aquellos eventos relacionados con la calidad desde el año 1939 hasta el año 1989.

Tabla 1. Cronologías de eventos relacionados con la calidad

AÑO	EVENTO
1939	Shewhart publica " Método desde el puntos de vista del control de calidad" en septiembre estalla la segunda guerra mundial.
1945	Finaliza la guerra
1947	Se crea el organismo normalizador internacional ISO
1949	Se funda la JUSE (unión de científicos e ingenieros japoneses
1950	Deming imparte su primer seminario de gestión de calidad en Japón
1952	Japón entra hacer parte de la organización ISO
1954	Juran es invitado a dictar varios seminarios relativos a la gestión de calidad a los empresarios japoneses
1959	el departamento de defensa de EEUU publica las normas NMIL-Q-9858
1979	British Standard, publica la norma BS 5750
1989	ISO publica la primera norma ISO 9001:1987

Fuente: LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación Confemetal, 2016. ISBN 978-84-16671-00-7.

En el año de 1946, en Londres, representantes de 25 países se reúnen con el objetivo de fundar una nueva organización internacional de estandarización. Para el año siguiente, inicia actividades la ISO.

[7] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

2.2 EL ESTANDAR ISO 9001.

La norma ISO9001 nació como una norma orientada a la gestión de una organización para la producción a través de la satisfacción de los requisitos del cliente. La norma ISO9001 se elabora por el comité técnico ISO /TC176 de ISO Organización Internacional para la Estandarización. Con título "Sistemas de Gestión de la Calidad" es por esta razón que la norma ISO9001 constituye el tronco central de gran parte de los Sistemas Integrados.

La norma ISO9001 nace como BS 5750 la cual fue publicada por British Standards Institution (BSI) en el año de 1979. Inicialmente la norma ISO9001 presento las versiones de los años 1987 y 1994 que contemplaban: ISO 9001 (para organizaciones con diseño de producto), ISO 9002 (para organizaciones sin diseño de producto pero con producción/fabricación), ISO 9003 (para organizaciones sin diseño de producto ni producción/fabricación –comerciales–) Excluyéndose así los requisitos que no le aplicaba, tras lo cual apareció en el 2000 la nueva ISO 9001 donde se incluían las tres normas y donde ya se permitía hacer exclusiones.[8]

Después de 25 años y con una serie de versiones, ISO 9001 es la norma más certificada en todo el mundo, con más de un 1 millón de certificaciones, luego del proceso de revisión de la ISO 9001:2008 y la publicación de la ISO 9001:2015, avalan que la ISO 9001 es la norma de referencia para las organizaciones que desean implementar un Sistema de Gestión de calidad.

2.2.1 Quién puede implementar la norma ISO 9001:2015. La norma ISO 9001:2105, es una norma genérica que es aplicable a cualquier organización sin tener en cuenta su tamaño o tipo, sector al que hace parte o la actividad que lleva a cabo.

Desde su publicación en 1987, la norma ha ido evolucionando según las necesidades cambiantes de las organizaciones y por supuesto de los mercados globales.

La generación ISO 9001:2015 se ha conseguido gracias a los cinco elementos claves presentados por la ISO en la revisión del año 2000 y que se mantienen actualmente.

- Requisitos generales y de la documentación.
- Requisitos para la dirección de la organización.
- Gestión de los recursos.

[8] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

- Gestión de la producción y apoyada en la gestión por procesos.
- El análisis, medican y la mejora del sistema de gestión.

Puede ser aplicada a empresas de servicios, producción y sirve como herramienta para la mejora a la empresa privada y pública.

2.2.2 ISO en el mundo. Anualmente ISO, hace un seguimiento de las certificaciones en el mundo y publica el informe ISO Survey, este informe permite seguir la respectiva evolución de la norma 9001 entre otras, en todo el mundo.

En la tabla 2, se detalla la evolución de la ISO: 9001 en todo el mundo, desde el año 2012 al 2015, donde por año se puede ver el número de certificados y se aprecia que al pasar los años fue disminuyendo la cantidad de certificados

Tabla 2. Evolución número de certificados ISO 9001

Norma	No	Número de certificados (año)				Evolución 2014-2015 (%)
		2012	2013	2014	2015	
ISO 9001	Certificados	1096987	1022877	1036321	1033936	-0,23%
	Países	184	187	188	201	6,91%

Fuente: ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: http://www.iso.org/

El crecimiento de la norma ISO 9001, es moderado a comparación con años pasados, su mayor auge tuvo lugar hace dos décadas, la norma insignia de la ISO es la 9001, ya que es la más certificada en el mundo.

En la tabla 3 se describen los países con el mayor número de empresas certificadas en la norma ISO 9001, China es el país con más certificaciones seguida de Italia

Tabla 3. Los 10 mejores países para los certificados ISO 9001, año 2015

Posición	País	Número de certificaciones
1	China	292.559
2	Italia	132.870
3	Alemania	52.995
4	Japón	47.101
5	Reino Unido	40.161
6	India	36.305
7	Estados Unidos	33.103
8	España	32.730
9	Francia	27.844
10	Rumania	20.524

Fuente: AENOR. ISO Survey 2015. España, en el top ten en las principales certificaciones [en línea]. [Consulta: 10 de diciembre de 2016]. Disponible en internet: <http://www.aenor.es/revista/pdf/nov16/28nov16.pdf>

En la tabla 4, se muestra el crecimiento anual de la norma ISO 9001 en todo el mundo, tomando como inicio el año 2007 hasta el 2015.

Tabla 4. Crecimiento anual de la norma ISO 9001 en el mundo

Año	2007	2008	2009	2010	2011	2012	2013	2014	2015
TOTAL	6,0%	3,0%	9,0%	1,0%	-6,0%	1,0%	1,0%	1,0%	-0,2%
África	0,0%	15,0%	-1,0%	-9,1%	6,5%	18,5%	1,5%	3,3%	19,8%
Central / Sur América	34,0%	-5,0%	-5,0%	38,6%	4,9%	-0,4%	2,0%	-4,4%	-1,8%
Norte América	23,0%	1,0%	12,0%	12,7%	-2,5%	2,8%	25,9%	-14,7%	13,2%
Europa	4,0%	6,0%	10,0%	5,9%	-13,3%	2,3%	-2,3%	-1,1%	-3,1%
Asia Oriental y Pacífico	11,0%	4,0%	11,0%	-2,9%	-1,5%	-1,5%	-2,2%	7,0%	1,9%
Central y Sur de Asia	12,0%	12,0%	1,0%	-15,4%	-10,7%	-3,6%	38,5%	-0,1%	-8,9%
Medio oriente	10,0%	-3,0%	20,0%	23,4%	-9,4%	11,6%	9,2%	2,5%	6,7%

Fuente: ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: <http://www.iso.org/>.

De la tabla 4, se resalta que en los últimos 3 años, Norte América presento el mayor crecimiento de la norma ISO9001, a comparación con el resto del mundo

A continuación se muestra en la tabla 5, los principales sectores de la industria, que adquirieron certificaciones de la ISO 9001 en el año 2015.

Tabla 5. Principales sectores Industriales certificados con la norma ISO 9001

Sector	2015
Metales básicos y productos metálicos	104.652
Equipamiento electrónico y óptico	75.260
Construcción	67.354
Reparación de vehículos de motor, motocicletas, artículos personales y de uso doméstico	66.975
Maquinaria y equipo	56.413

Fuente: ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en Internet: <http://www.iso.org/>.

En la tabla 5, se observa que en año 2015, el sector industrial que presento el mayor número de certificados con la ISO 9001, es metales básicos y productos metálicos, con una amplia ventaja.

2.2.3 ISO en Colombia. Para Colombia es significativo que las organizaciones generen la política de aplicar las normas de calidad en cada uno de sus procesos, ya que a partir de esto, se generara confianza a los clientes y permitirá la evolución de la organización.

A pesar de tener una participación baja a nivel mundial, Colombia está muy bien ubicada en países con más certificaciones. Según información de ISO, para el año 2008, Colombia ocupaba el puesto 13 de entre 195 países en certificaciones (12.324 de 1'029.746 certificaciones mundiales), muy cerca de Australia, Brasil y Rumania. Colombia ocupó para el 2008 el puesto 10 (con 22.156 de 754.234), solo después de Italia, China, Japón, España, Francia, Reino Unido, Estados Unidos, India y Alemania, y muy cerca pero por encima de Australia, Canadá y Brasil.

Para nuestro país se tiene la siguiente información sobre el número de certificados

En nuestro país, tenemos algunos sectores de la industria que cuentan con la certificación de la norma ISO 9001.

Tabla 6. Colombia. Principales sectores Industriales certificados con la norma ISO 9001

Sector	No de certificaciones
Construcción	1490
Otros servicios	1233
Transporte, almacenamiento y comunicaciones	1107
Reparación de vehículos de motor, motocicletas y artículos personales y de uso doméstico	729
Servicios de Ingeniería	531
Intermediación financiera, bienes raíces, alquiler	462
Administración pública	416
Productos químicos	335
Productos farmacéuticos	305
Productos alimenticios, bebidas y tabaco	302
Tecnologías de la información	292
Productos de caucho y plásticos	285
Hoteles y restaurantes	142
Suministro de electricidad	137
Minas y canteras	129

Tabla 6. (continuación)

Empresas de impresión	
Tejidos y productos textiles	98
Otro equipo de transporte	96
El suministro de agua	82
En el sector de la agricultura y pesca	72
Suministro de gas	67
Pulpa de madera, papel y productos de papel	57
Industria de la madera	42
Coquerías y refino de petróleo	42
Empresas editoriales	31
Cuero y del calzado	23
Reciclaje	21
Construcción naval	10
Aeroespacial	9

Fuente: ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en Internet: <http://www.iso.org/>.

En la tabla 6, se muestra como un dato estadístico, que para Colombia el sector que más cuenta con certificados con la norma ISO9001 es la industria de la construcción.

2.3 REVISIONES EXISTENTES DE LA ISO 9001.

Todas las normas ISO son revisadas por su comité técnico cada cinco años, con el fin de verificar si es necesario alguna modificación o actualización con el objetivo de mantener su vigencia y relevancia, en el caso de la norma ISO 9001, se trata del comité técnico 176, que cuenta con la opinión de todas las partes involucradas en el proceso; en la figura 1, se muestra gráficamente las revisiones de la ISO9001[9]

[9] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

El proceso de revisión está dividido en seis etapas:

- **Etapa 1. Propuesta de nuevos temas de trabajo (NWIP).**Se lleva a cabo la evaluación de la norma para así determinar si es necesario un cambio o modificación.
- **Etapa 2. Borrador de trabajo (WD).**Ya con unas propuestas de revisión aceptadas, se inicia con el borrador de trabajo

- **Etapa 3. Borrador del comité (CD)**.Los miembros del comité, realizan comentarios, en este momento el documento todavía es interno

- **Etapa 4. Proyecto de norma internacional (DIS).**el documento final de la etapa anterior, es sometido a votación, para así poder ser registrado como proyecto de norma internacional.

- **Etapa 5. Proyecto final de norma internacional (FDIS).**el nuevo borrador de la norma es distribuido a los miembros de la ISO para revisar y hacer su respectiva votación.

- **Etapa 6. Norma internacional**.es aprobado y su contenido ya no puede ser, modificado, y es publicado como norma internacional[10].

Figura 1. Revisiones de la norma ISO 9001

Fuente: Elaboración propia, basado en BURCKHARDT, Leiva, SOLER, Víctor Gisbert y PÉREZ MOLINA, Ana Isabel. Estrategia y desarrollo de una guía de implementación de la norma ISO 9001:2015. Aplicación pymes de la Comunidad Valenciana

[10] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

2.3.1 Generalidades ISO 9001:2015 última versión[11]. La adopción de un sistema de gestión de la calidad es una decisión estratégica para la organización que le puede ayudar a mejorar su desempeño, esta norma está basada en los principios de la gestión de la calidad que están descritos en la norma ISO 9000.

2.3.2 Enfoque al Cliente. Las organizaciones dependen de sus clientes, por lo cual deberían entender las necesidades actuales y futuras de sus clientes.

2.3.3 Liderazgo. Los líderes en todos los niveles, establecen un propósito y la dirección, y crean las condiciones a las que las personas se implican en el logro de los objetivos de calidad de la organización.

2.3.4 Compromiso De Las Personas. El personal de todo nivel, es la esencia de una organización, ya que ellos son los que nos permite aumentar la capacidad de la organización para generar valor[12].

2.3.5 Enfoque A Procesos. Permite alcanzar resultados coherentes y previsibles de manera más eficaz[13].

2.3.6 Toma de Decisiones Basada En La Evidencia. Las decisiones basadas en el análisis y la evaluación de datos, tienen mayor posibilidad de producir resultados deseados.

2.3.7 Gestión De Las Relaciones. Para poder tener éxito sostenido, las organizaciones gestionan sus relaciones con las partes interesadas pertinentes.

2.4 ESTRUCTURA DE ISO 9001:2015

La nueva estructura de alto nivel de la norma ISO9001:2015, con respecto a la versión anterior muchos de sus requisitos son similares, pero la ubicación de muchos de ellos han cambiado, la unificación de la estructura facilita la lectura y la compresión de la misma.

El propósito de la estructura de alto nivel es poder adquirir un alineamiento de los estándares de sistemas de gestión.

---

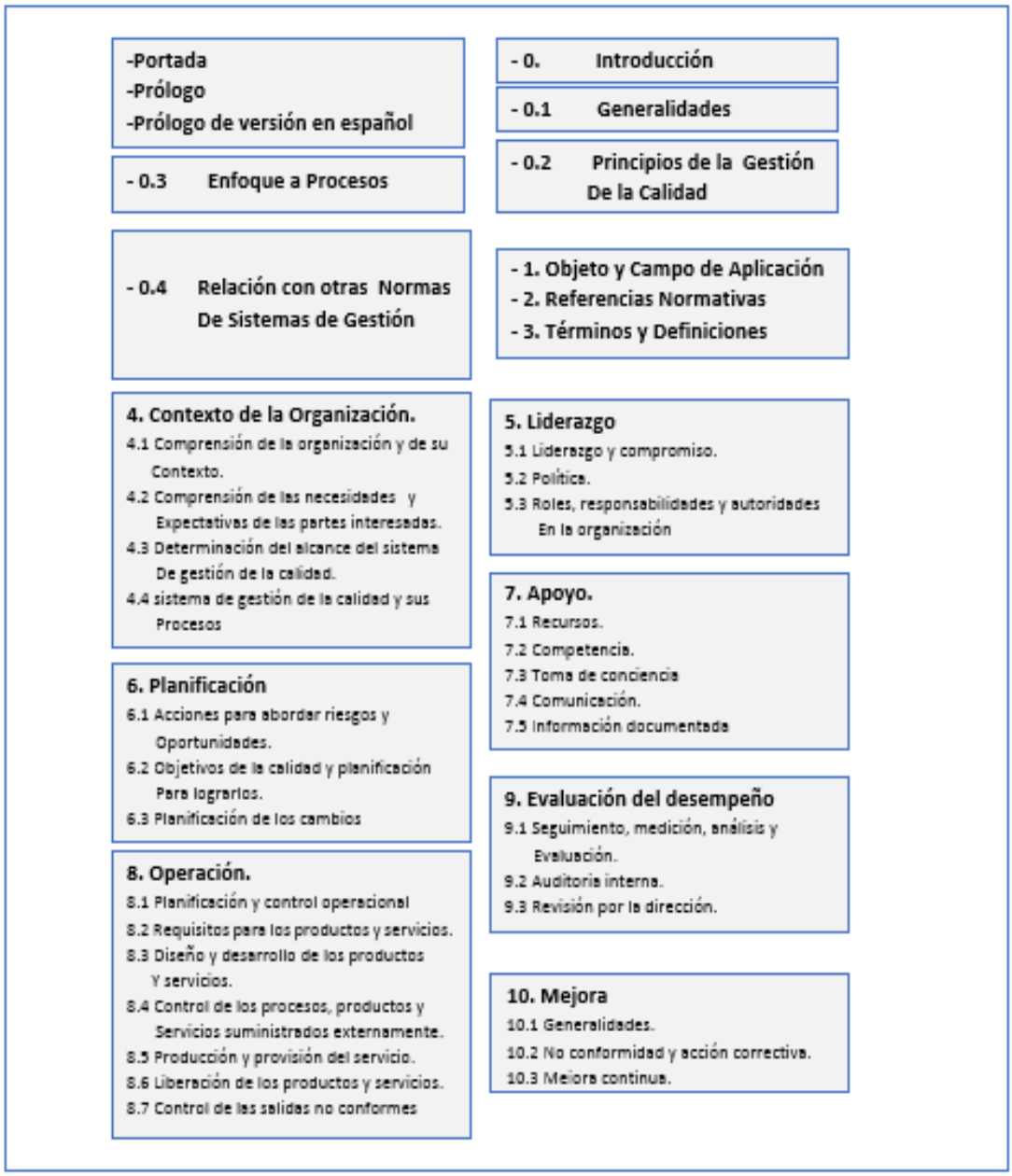
[11] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN [ICONTEC]. NTC-ISO 9001, Sistemas de gestión de la calidad. Requisitos, 4.a actualización. Bogotá: El Instituto, 2015. 33 p.

[12] YAÑEZ, Carlos 5 diciembre 2008, Articulo, Área de Gestión, sistemas de gestión de la calidad (ISO 9001) 2 p

[13] YAÑEZ, Carlos 5 diciembre 2008, Articulo, Área de Gestión, sistemas de gestión de la calidad (ISO 9001) 2 p

En la figura 2, se describe la estructura y cada uno de los requisitos de la norma ISO 9001:21015, ya que es importante para poderla interpretar

Figura 2. Estructura completa norma ISO 9001:2015



Fuente: INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION [ICONTEC]. NTC-ISO 9001, Sistemas de gestión de la calidad. Requisitos, 4.actualización Bogotá: El Instituto, 2015. 33 p.

De la figura 2, es importante tener presente toda la estructura y requisitos de la norma ISO9001, ya que nos permite promover la compatibilidad entre las diferentes normas.

3. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1 GENERALIDADES DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

"La información es uno de los activos más importantes de cualquier organización y siempre ha estado amenazada, la seguridad de la información debe formar parte de todos los procesos del negocio, ya sean los procesos manuales o automáticos, para proteger de una forma adecuada la información se debe dar respuesta a las preguntas: QUE, DÓNDE, CÓMO, Y CUÁNDO"[14].

- **QUE:** se debe poder garantizar de una u otra forma y sin ningún tipo de duda el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de la información de la organización.

  La seguridad de la información consta de unas dimensiones de la seguridad: Confidencialidad, Integridad, Disponibilidad, Autenticidad, trazabilidad.

- **DÓNDE**: la información es almacenada, procesada y transmitida por los sistemas de información y comunicaciones, por lo tanto es preciso garantizar la seguridad de los sistemas de información de una forma total, se debe proteger todos y cada uno de los elementos que forman parte del sistema de información y comunicaciones frente a las posibles amenazas a las que están expuestas.

- **CÓMO:** todas las amenazas a las que está expuesta la información de la organización, deben ser contrarrestadas por medio de controles.

- **CUÁNDO:** la información debe ser protegida durante todo el ciclo de vida de la misma, desde el momento que ingresa hasta el momento que deja de ser útil para la organización.

Es la capacidad que tiene la norma de poder llegar a cualquier tipo de organización, sin importar su tamaño, o razón de ser, esta norma nos brinda los pasos para poder hacer seguimiento, mantener y mejorar el SGSI, como lo dice la norma específica los requisitos para así poder satisfacer las necesidades organizacionales con respecto a la seguridad de la información[15].

---

[14] BADA MERINO, Cristina y CAÑIZARES SALES, Ricardo. Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001. Madrid: Fundación Confemetal. ISB13:978-84-92735-87-7

[15] BADA MERINO, Cristina y CAÑIZARES SALES, Ricardo. Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001. Madrid: Fundación Confemetal. ISB13:978-84-92735-87-7

La organización que adopte un modelo de gestión adecuado, generara confianza en cada uno de sus procesos, por tal confianza a la organización y será capaz de alcanzar sus objetivos.

3.2 EL ESTANDAR ISO 27001 Y SU ESTRUCTURA

El estándar ISO 27001, es un estándar internacional publicado en el mes de octubre de 2005, dedicado a la organización de la información; es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI)[16].

Esta norma ayuda a proteger los activos de información y otorga seguridad en las partes interesadas, adopta un enfoque por procesos para implantar, supervisar, operar, mantener y mejorar Sistema de Gestión de Seguridad de la Información, la norma es especialmente interesante si la protección de nuestra información es crítica, como por ejemplo en tecnologías de la información.

La más reciente versión de esta norma es la ISO /IEC 27001: 2013, en la tabla 7 se describe el número de certificados de la norma y como está su evolución a nivel mundial comparando entre el año 2014 y 2015.

Tabla 7. Evolución número de certificados norma ISO/IEC27001

NORMA	NUMERO DE CERTIFICADOS EN 2014	NUMERO DE CERTIFICADOS EN 2015	EVOLUCION EN %
ISO / IEC 27001	23.005	27.536	20%

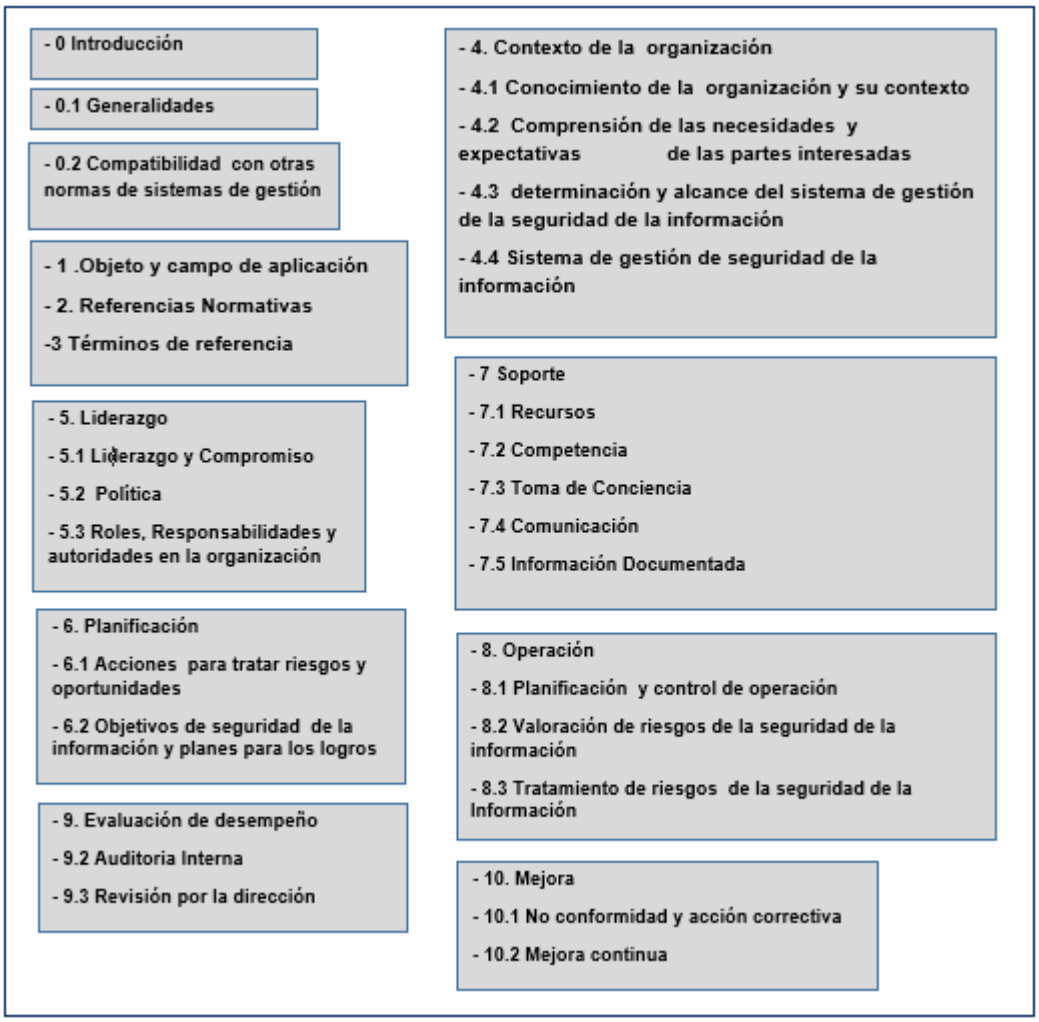
Fuente: ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: <http://www.iso.org/>.

De la tabla 7, es significativo conocer la evolución del número certificados de la norma ISO/IEC27001, en el año 2015, con una evolución en porcentajes de 20% en comparación del año 2014

En la figura 3, se muestra gráficamente la estructura y los requisitos de la norma ISO/IEC 27001:2013

[16] BADA MERINO, Cristina y CAÑIZARES SALES, Ricardo. Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001. Madrid: Fundación Confemetal. ISB13:978-84-92735-87-7

Figura 3. Estructura completa norma ISO/IEC 27001:2013



Fuente: Basado en INSTITUTO COLOMBIANO DE NORMASTÉCNICAS Y CERTIFICACIÓN [ICONTEC]. NTC-ISO/IEC 27001, Sistemas de gestión de la Seguridad de la información.

3.2.1 El Estándar ISO 27001 en el mundo.

Dada la evolución de las tecnologías de la información a nivel mundial, a este mismo ritmo crece la cantidad de amenazas y riesgos, lo que hace que todas las organizaciones busquen la forma más apropiada de proteger su valor más importante, que es la información y la manera más eficiente es gestionar los riesgos, de esta forma se puede identificar los elementos que se encuentra más venerables, esto ha hecho que la norma ISO/IEC 27001 se convierta en la más importante en el tema de seguridad de la información a nivel mundial

A continuación se muestra en la tabla 8, el crecimiento anual de la norma ISO 27001 a nivel mundial.

Tabla 8. Crecimiento anual de la norma ISO/IEC 27001

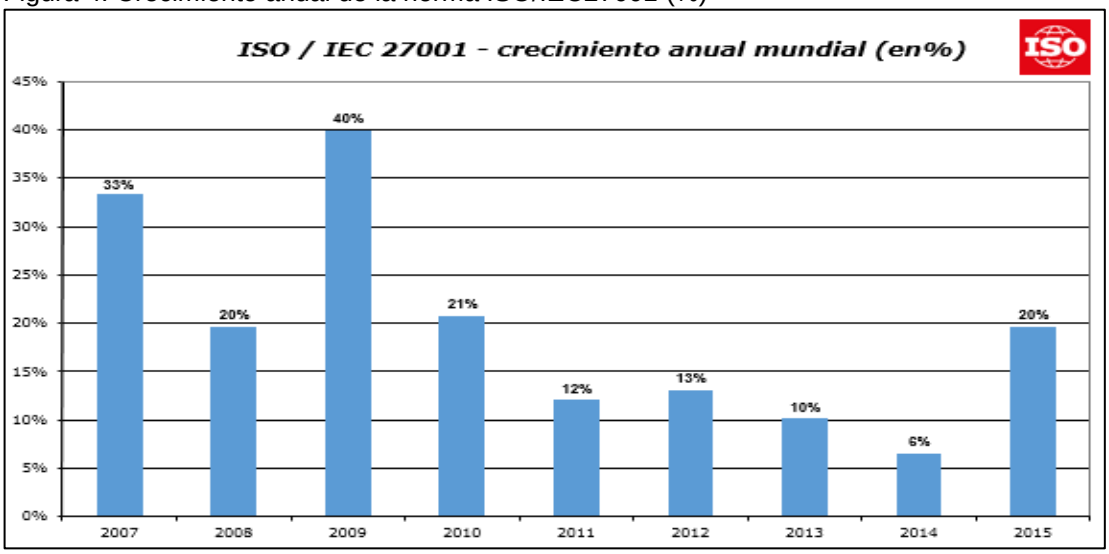
CRECIMIENTO ANUAL DE LA NORMA EN %									
AÑO	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
TOTAL	**33%**	**20%**	**40%**	**21%**	**12%**	**13%**	**10%**	**6%**	**20%**
África	67%	60%	194%	-2%	-13%	60%	55%	-20%	63%
Central / Sur América	111%	89%	39%	17%	28%	35%	34%	0%	27%
Norte América	42%	89%	52%	2%	32%	27%	29%	14%	78%
Europa	35%	52%	64%	35%	13%	21%	25%	9%	21%
Asia oriental y Pacifico	32%	5%	27%	19%	10%	8%	-3%	3%	15%
Central y Sur de Asia	36%	62%	55%	2%	13%	11%	20%	12%	14%
Medio Oriente	92%	80%	61%	6%	28%	19%	36%	13%	19%

ISO.ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: <http://www.iso.org/>.

De la tabla 8, es importante mencionar que para el año 2015, el continente Africano es uno de los que presentó un aumento certificados del 63%

En la figura 3, se describe el crecimiento que ha tenido la norma en todo el mundo, desde el 2007

Figura 4. Crecimiento anual de la norma ISO/IEC27001 (%)



ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: <http://www.iso.org/>.

A continuación en la tabla 9, se describe el top 10 de los países más certificados con esta norma, es importante conocer que países, tienen ventaja en la implementación de esta norma de seguridad.

Tabla 9. Certificados por país norma ISO/IEC27001

Top 10 de los Países de la Norma ISO/IEC27001 - 2015 Certificados		
1	Japón	8.240
2	Reino Unido	2.790
3	India	2.490
4	China	2.469
5	Estados Unidos	1.247
6	Rumania	1.078
7	Italia	1.013
8	Alemania	994
9	Taipei,China	939
10	España	676

ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: <http://www.iso.org/>.

El país que cuenta con más certificados en la norma ISO/IEC27001 en el mundo es Japón, con un total de 8.240 certificados

En la tabla 10, se presenta los sectores industriales a nivel mundial, que están optando por la certificación de seguridad de la información.

Tabla 10. Cinco principales sectores Industriales certificados con la norma ISO/ IEC 27001

Los Cinco Principales Sectores Industriales para la Norma ISO/IEC 27001 en el Año 2015		
1	Tecnologías de la Información	5.573
2	Otros Servicios	959
3	Transporte, Almacenamiento, y Comunicaciones	301
4	Equipamiento Electrónica y Óptico	296
5	Salud y Trabajo Social	231

ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: <http://www.iso.org/>.

Como la norma ISO/IEC 27001:2013, es una norma de seguridad de la información, el sector que cuenta con más certificados es el de las tecnologías de la información con un número de 5.573

3.2.2 Claves para tener éxito con la norma ISO 27001:2013.como dice Calder[17] Primero tener claro que se va a tener éxito, y para esto tener claro lo siguiente:

- Conocer y ser capaz de comunicar con claridad, porque la seguridad de la información es importante para cualquier organización.
- Saber que la norma ISO 27001 muestra lo que es el camino correcto para proporcionar seguridad de la información, lo cual con lleva a contar con un conocimiento de fondo de la norma.
- Tener claro cómo se va a estructurar el proyecto, elementos claves y ver la mejor manera de emprenderlo.
- Ventajas y desaciertos al contrata consultores o si nosotros mismos lo realizaremos.

Como dice Calder[18], la seguridad de la información es un asunto empresarial no tecnológico, se relaciona con el aseguramiento de la disponibilidad, confidencialidad, e integridad de la información de nuestra organización.

La seguridad de la información según la norma 17799:2005 es “la protección de la información contra una gran variedad de amenazas, con el fin de asegurar la continuidad de la empresa, minimizar el riesgo para la misma, y maximizar el retorno de la inversión y oportunidades de negocio”. “El propósito de un sistema de gestión de seguridad de la información, es reducir y controlar los riesgos para la seguridad de la información. por consiguiente la organización debe comprender que los riesgos existen en relación con sus propias operaciones”[19].

Debe agrupar los problemas de seguridad de la información, que vive en su propia organización, o tener unas proyecciones de las consecuencias que podrían tener las vulnerabilidades individuales de seguridad en su organización, serian como una “lista de amenazas” su objetivo es poder generar una preocupación en las personas para que atiendan la necesidad de una acción de carácter importante[20].

La seguridad de la información es un asunto de dirección y gobierno, para tener un SGSI eficaz, depende por completo del apoyo efectivo de la alta dirección de la organización, sin este respaldo no existe la mínima posibilidad de lograr el éxito, ya que se trata de un proyecto a nivel de la organización no de un proyecto de TI por

[17] CALDER,Alan.Nueve claves para el éxito una Visión general de la implementación de la norma NTC-ISO /IEC27001

[18] Ibíd., p. 34.

[19] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

[20] Ibíd., p. 37.

lo cual debe estar alineado completamente con el modelo, las metas y las estrategia de la empresa entendiendo las prioridades de la misma.

3.2.3 ISO 27001 – ISO 17799. La norma de seguridad de la información, es una norma que se compone de partes, que en estos años ha sufrido sus diferentes perfeccionamientos. La primera, es la norma ISO27001:2005 también es conocida como la norma BS7799-2:2005, la cual ofrece una especificación para SGSI, en la cual se tiene el término "debe", la segunda parte la ISO 17799:20025 también conocida como BS7799-1:2005, tiene el estatus de un código de mejor práctica.

Como dice Calder[21] La diferencia entre una especificación y un código de práctica, en el tema de las normas de sistemas de gestión, es que una especificación contiene el término "debe" con lo cual dicta aspectos obligatorios de un sistema que busque cumplir la norma, mientras que el código de partica ofrece orientación y tiene la palabra "debería" la cual indica que la conformidad no es obligatoria. La certificación acreditada se otorga contra una especificación de requisitos no contra un código de práctica, la norma ISO27001 depende de la norma ISO17799, y exige que los miembros de la organización busquen allí orientación sobre los controles, Debe medirse la Conformidad contra estas dos normas, por lo tanto su contenido exacto predomina sobre cualquier otro comentario u orientación.

3.2.4 Evolución Norma ISO 27001. "La norma tiene su origen británico, ya en el año 2005, la organización Internacional para la Normalización (ISO) la oficializó como una norma, la norma ISO27001:2005, según la investigación de Aníbal Mantilla es el único estándar certificable que es aceptado internacionalmente de manera mundial para la gestión de seguridad de la información"[22]

El estándar ISO/IEC 27001, es el nuevo estándar oficial, el nombre completo que tiene esta norma es BS 77992-:2005 (ISO/IEC 27001).

Son 1870 organizaciones en 57 países que han reconocido la importancia y los beneficios de esta norma[23], el conjunto de estándares que aportan información a la familia de las ISO27001, que se deben tener en cuenta son los que se indican en la Tabla 11.

---

[21] CALDER,Alan.Nueve claves para el exito.Una Visión general de la implementación de la norma NTC-ISO /IEC27001

[22] MANTILLA GUERRA, Aníbal Rubén. Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base a la norma ISO 27001. 17 [en línea]. Tesis Máster en Gestión de las Comunicaciones y Tecnologías de la Información, MSC. Quito: Escuela Politécnica Nacional, 2009 [consulta: 11 de enero de 2017], p. 7. Disponible en internet: <http://bibdigital.epn.edu.ec/retrieve/30968/CD-2254.pdf>.

[23] CORLETTI ESTRADA, Alejandro. Seguridad por niveles. Madrid: DarFE Learning Consulting, 2011

En la versión del 2013 la norma indica que el sistema de gestión de seguridad de la información está orientada a preservar la confidencialidad, integridad y disponibilidad de la información aplicando la gestión del riesgo a sus activos que da confianza a todas sus partes interesadas. Lo que se quiere decir con esto es que la reducción del riesgo implica una mejora de la seguridad de la información,
Los activos se suelen clasificar en software, aplicaciones informáticas. Hardware" equipos, dispositivos, Servicios "telefonía, servicios, personas e información"

La norma ISO / IEC 27001, fue preparada por el comité técnico conjunto con la ISO / IEC JTC 1.

Tabla11. Evolución de la norman ISO/IEC 27001

AÑO	EVENTO
1995	BS 7799-1: 1995
1999	BS 7799-2: 1999
1999	Revisión BS 7799-1: 1999
2000	ISO/IEC 17799: 2000 norma internacional código practicas
2002	Revisión BS 7799-2: 2002
2004	UNE 71502. norma española
2005	Revisión ISO/IEC 17799: 2005
2005	Revisión BS 7799: 2005
2005	ISO/IEC 27001: 2005 Norma Internacional Certificable
2013	ISO/IEC 27001: 2013 Norma Internacional Certificable

Fuente: ZUCCARDI, Giovanni y GUTIÉRREZ, Juan David. ISO-27001:2005 [en línea].[Consulta:2 de octubre de 2016]. Disponible en internet <http://pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001v0.1.pdf>.

En la tabla 11, se puede observar como en los eventos de los años 2005 y 2013, es una norma ya certificable, dato de mucha importancia y relevancia para tener presente.

3.3 ISO EN COLOMBIA

En Colombia por medio del artículo 78, de la constitución política reitera que "la ley regulara el control de la calidad de bienes y servicios, la calidad es prioridad para las empresas colombianas, la calidad en nuestro país inicia con la creación del ICONTEC "

A nivel Colombia, se tiene un número de certificados para la norma ISO/IEC 27001:2005 de 103, mientras que para la ISO 9001 son 184

En nuestro país, tenemos algunos sectores de la industria que cuentan con la certificación de la norma ISO / IEC 27001.

Tabla 12. Colombia. Principales sectores Industriales certificados con la norma ISO / IEC 27001

Sector	No de certificaciones
Tecnologías de la información	48
Otros servicios	16
Área financiera, bienes raíces, alquiler	12
Administración pública	7
Equipamiento electrónico y óptico	3
Transporte almacenamiento y comunicaciones	3
Servicios de ingeniería	3
Otros servicios sociales	3
En el sector de la agricultura y pesca	1
En el sector Maquinaria y equipo	1
Otro equipo de transporte	1
Hoteles y restaurantes	1
Educación	1

Fuente: ISO. ISO Survey 2015 [en línea]. [Consulta: 15 de noviembre de 2016]. Disponible en internet: <http://www.iso.org/>.

Para Colombia los tres sectores que cuentan con el mayor número de certificados con la norma ISO/IEC 27001 son tecnologías de la Información, otros servicios y área financiera y bienes raíces, el resto de los sectores tienen un número muy bajo.

3.4 SIMILITUD ENTRE LAS DOS NORMAS

Las normas ISO 9001:2015 y la ISO/IEC 27001:2013, tienen una estructura de alto nivel, lo cual permite su relación y comprensión más fácil, las dos normas mencionadas ISO9001:2015 y ISO/IEC 27001: 2013, como por ejemplo en el numeral 4.1 “compresión de la organización y de su contexto” hablan del mismo concepto

Las normas ISO9001:2015, ISO/IEC 27001:2013, contienen muchos aspectos con similitudes, lo que permite hacer una integración mucho más fácil.

Tabla 13. Descriptores en común de las normas ISO 9001:2015 e ISO / IEC 27001:2013

DESCRIPCIÓN	ISO9001	ISO27001
Enfoque basado en procesos	X	X
Modelo PHVA	X	X
Responsabilidad de la dirección	X	X
Control de Documentación	X	X
Auditorias	X	X
Competencia y formación	X	X
Seguimiento y Medición	X	X
Acciones Correctivas	X	X
Acciones preventivas	X	X
Gestión de proveedores	X	X
Gestión de Cambios		X
Gestión de Incidentes		X
Gestión de Problemas		X
Gestión del Riesgo		X

Fuente: basado en INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN [ICONTEC]

Es importante tener claro todos los elementos que tienen en común las normas ISO9001 e ISO27001, para el momento de hacer un sistema integrado entre estas dos normas.

Viendo la necesidad de muchas organizaciones de implementar sistemas de gestión integrados, y como la norma 9001 y la 27001, tienen ya una estructura de alto nivel definidas es mucho más fácil implementar este sistema integrado de gestión que ponernos a implementar las dos normas por separado nos llevaría mucho más esfuerzo de esa manera.

3.5 VENTAJAS Y BENEFICIOS DE LA IMPLEMENTACIÓN DE ISO 27001:2013, E ISO 9001:2015.

La globalización está llevando hacia la estandarización de los procesos que hacen parte de nuestra empresa lo cual hace la toma de mejores prácticas para llegar al éxito que estamos buscando.

De acuerdo con Cortés y Ardila[24], a continuación, se describen las ventajas de estas certificaciones, basados en 5 factores básicos para el éxito aplicables a cualquier tipo de organización.

3.5.1 CALIDAD A LA SEGURIDAD. Con la implementación de un verdadero sistema de gestión de seguridad de la información SGSI,la seguridad es una actividad de gestión , la cual será una actividad trascendente en la organización ya que transformaran un conjunto de actividades técnicas en un ciclo controlado y metódico protegiendo los activos más importantes de una organización que es la información.

3.5.2 REDUCCIÓN DE RIESGOS. A Con la introducción de los controles y la mejora continua que plantean estas normas se reducirá lo más posible todo riesgo por robo, error humano intencionado o no , mal uso de instalaciones y equipos a los cuales está expuesto el manejo de la información.

3.5.3 COMPETITIVIDAD. Este es el primer factor que le interesa a cualquier empresa, como se mencionó anteriormente, poco a poco los clientes, las grandes empresas y la red de partners comenzarán a exigir este tipo de certificaciones para generar relaciones comerciales y de negocios seguras

3.5.4 COMPROMISO Y CONCIENTIZACIÓN. Este tipo de estándares crea conciencia y compromiso de seguridad en todos los niveles de la organización, creando conciencia de calidad y seguridad la cual se ve reflejada en la calidad de los servicios y aquellos productos entregados al cliente

3.5.5 MEJORA CONTINUA. La implementación y puesta en marcha de un SGSI, debe incluir programas de Auditoría interna las cuales ofrecen una oportunidad de detectar debilidades del sistema y las áreas a mejorar para contribuir a la mejora continua de la empresa

[24] CORTÉS R., Diana Marcela y ARDILA, Alix Victoria. Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001 [en línea]. Trabajo de grado Especialista en Gerencia de Procesos y Calidad. Bogotá: Universidad EAN, 2012 [consulta: 10 de diciembre de 2016]. Disponible en internet: <http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2>.

4. SISTEMAS INTEGRADOS DE GESTIÓN

Un Sistema Integrado de Gestión se define como una serie de actividades que interactúan para dar dirección, articular, alinear los requisitos de los subsistemas que lo componen, el sistema de gestión integrada nos posibilita y simplifica la implementación de un solo sistema de gestión para la organización**.**
A través de los años, ISO ha ido publicando numerosas normas de sistemas de gestión, en todos los campos como seguridad, medio ambiente y muchas más.

Como dice Lopez[25], el interés de las organizaciones para adoptar normas lo cual ha llevado a la popularización de los sistemas de gestión integrados, en empresas de todo tipo y que cuentan con una larga experiencia en los sistemas integrados de gestión

La guía para la implementación de un sistema integrado de gestión integrado ISO 9001:2015 e ISO/IEC 27001:2013, adopta la estrategia de hacer un sistema de gestión integrado, que cubra todos los requisitos que son precisos para cada sistema de gestión que vamos a integrar.

Al integrar un sistema de gestión obtenemos unos beneficios como: uso eficiente de los recursos de la dirección, logro coherente y fiable de los objetivos organizacionales.

El objetivo de un Sistema de Gestión Integrado, es la obtención de todos nuestros procesos bajo un único cuerpo prismático que contempla todos los aspectos de las diferentes áreas o disciplinas de forma integrada.

“El tema es que a pesar de que muchas normas tienen muchos aspectos en común, muchas de ellas no tienen la misma estructura lo que dificulta la coexistencia del sistema de gestión, lo que lleva a muchas organizaciones que los sistemas de gestión que están implementados funcionan por separado; la estructura de las normas es importante ya que los sistemas de gestión están apoyados a estas estructuras, se debe tener claro que para integrar de una forma sencilla, y poder lograrlo se requiere que estas tengan una estructura en común”[26].

Teniendo claro los pro LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7blemas que se tenían con respecto a esto el grupo JTCG (Joint Technical Coordination Group) decidió desarrollar una estructura de un sistema de gestión genérico que pudiese ser aplicado por una organización.

[25] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

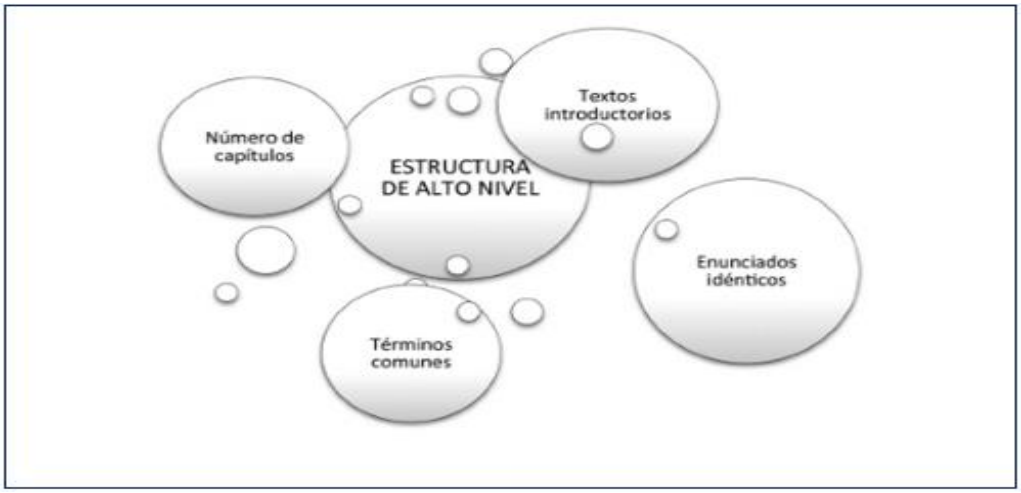
[26] Ibíd., p. 15.

Requisitos básicos de esta estructura común:

- Idéntico número de capítulos.
- Idénticos textos introductorios para los artículos
- Enunciados idénticos para requisitos idénticos
- Términos comunes

En la figura 5, se presenta los requisitos básicos de la estructura de alto nivel

Figura 5. Requisitos básicos de la estructura de alto nivel



Fuente: tomado de LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7.

Los países que más han trabajado de una u otra forma para integrar diferentes sistemas de gestión son, España, Reino Unido y la parte de Oceanía. "España publicó en el año del 2005 (AENOR) la norma **UNE 66177:2005**, es una guía para la implementación de sistemas integrados de gestión, la norma consta de 8 capítulos y 5 anexos, la cual da pauta para implementar sistemas de gestión de cualquier tipo de naturaleza, indica que es para las normas ISO 9001, ISO14001 Y OHSAS 18001, ya que estos son los sistemas de gestión más abiertos que existen"[27].

Reino Unido, la BSI (British Standards Institution), publica en 2006 la PAS 99:2006, es una especificación de requisitos comunes de los sistemas integrados de gestión y una perfil para la integración, los requisitos de esta norma está bajo o referenciado elementos comunes que están formulados en la ISO GUIDE 72:2001.En Oceanía

[27] MESQUILE C., Luis, Modelo para facilitar la interacción de estándares de gestión de TI en entornos maduros. Tesis doctoral para optar el grado en Doctor en informática. España: Universitat de les Illes Balears, 2012

se encuentra la norma AS/NZS 4581:1999, que es una guía para poder identificar los componentes más comunes en todos los sistemas de gestión.

En la tabla 14 se describe, algunas de las ventajas que se pueden obtener, al implementar un sistema integrado de gestión.

Tabla 14. Ventajas de la Implementación de un Sistema Integrado de Gestión

N°	Ventajas de la Implementación de un Sistema Integrado de gestión
1	Desarrollar servicios de TI, que esté de acuerdo con los objetivos de la organización
2	Promueve la confianza entre las partes interesadas
3	Documentación reducida debido a procedimientos comunes
4	Implantación y mantenimiento más eficaz y eficiente
5	Uso eficiente de los recursos de la dirección
6	En torno con cultura global
7	Confianza y reglas claras para las personas de la organización
8	Disminución de costos en el mantenimiento del sistema
9	Simplificación del proceso de auditoria
10	Mejora la capacidad de reacción de la organización , frente a posibles amenazas contra su sistema de información

Fuente: INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN [ICONTEC]

Es importante tener claro cada una de las ventajas que brinda la integración de un sistema de gestión, ya que por medio de estas se puede llegar a cumplir los objetivos propuestos.

4.1 NORMA UNE-66177.

Aunque esta norma, tiene por objeto proporcionar directrices para poder desarrollar implementar y evaluar el proceso de integración de los sistemas de gestión de la calidad, gestión ambiental y gestión de seguridad y salud en el trabajo, también pude ser utilizada como un marco de trabajo para poder integrar otros sistemas de gestión, basados en el modelo PDCA, como lo es el sistema de gestión de seguridad de la información[28].

[28] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

La UNE-66177 no es una norma certificable, esta fue desarrollada como ayuda a las organizaciones que quieren implementar sistemas integrados de gestión.

Esta norma UNE-66177 fija una estructura para proceso de integración

4.1.1 Desarrollo del plan de integración.

Para el desarrollo del plan de integración, se debe hacer el análisis de unos aspectos como:

- Identificación de los beneficios a conseguir
- Análisis del contexto de la organización. (madurez, limite, etc...)
- Selección del nivel de integración adecuado a las posibilidades de la organización
- Elaboración de un plan de integración
- Implicación al proyecto que estamos desarrollando a la alta dirección

4.1.2 Implantación del Plan De Integración

- Plan de integración
- Seguimiento al plan de integración

4.1.3 Revisión y Mejora. Esta es una de las partes fundamentales del proceso de integración y que constituye la evolución del resto del proceso de integración, nos permite identificar el mejor método de integración posible y los recursos necesarios para este, este contempla aspectos primordiales como:

Madurez: como lo indica el nivel de madurez, experiencia y eficacia en el uso de los sistemas de gestión, nivel de competencias de personal de la organización

Complejidad: nivel de las necesidades y expectativas de los clientes y las partes interesadas como lo son los requisitos de los clientes, de la sociedad, requisitos de los accionistas, propietarios, estrategias de la propia compañía

Alcance: es la extensión o hasta donde llega los sistemas de gestión, podemos tener como por ejemplo, inventario de los sistemas de gestión implantados, los procesos involucrados en los sistemas de gestión y su respectiva documentación.

Riesgo: nivel de riesgo debido a posibles incumplimientos legales o fallos asociados al proceso de integración, como por ejemplo, incumplimiento con los requisitos legales.

Es importante tener en cuenta que a la hora de implantar un sistema integrado de gestión en una empresa, es necesario desarrollar acciones de formación y divulgación.

4.1.4 Formación y Concienciación

La formación es fundamental a la hora de integrar sistemas de gestión, y esta se puede estructurar de la siguiente forma.

4.1.4.1 Formación previa. Busca que determinadas personas de nuestra organización conozcan de forma exhaustiva cuales son las herramientas y el tipo de gestión que se va a implementar, debe estar un referente claro de quienes son los expertos de cada área de conocimiento[29]

4.1.4.2 Formación durante el proceso de documentación. Ya cuando se ha diseñado el sistema de gestión integrado, se han reconocido cada uno de los requisitos y se ha integrado los métodos y se inicia con el proceso de elaboración de la documentación; para esto suministra formación a los equipos de trabajo dentro de las diferentes áreas de la empresa, para que las personas elaboren la documentación con criterio y método[30].

4.1.4.3 Formación durante el proceso de Implantación. Previamente a esta se debe formar a todo el personal de la organización, esta formación es sumamente importante ya que todo el personal de la empresa debe operar conforme a los procedimientos de se han elaborado[31]

4.2 DEFINICION DEL ALCANCE DEL SISTEMA INTEGRADO DE GESTIÓN

Para poder definir el alcance del sistema integrado de gestión, como dice Castillo y Martinez [32]es necesario poder garantizar una mínima información para la toma de las decisiones de una forma apropiada, esta se compone del alcance de las actividades. Productos y servicios para el cual se hace gestión.

---

[29] Guía Internacional para una mejor práctica comercial, Integración de sistemas de Gestión, Guía para las empresas, el gobierno y las organizaciones de la comunidad, Bogotá D.C. Colombia 2003 ISBN: 9383-33-5. ICONTEC

[30] Guía Internacional para una mejor práctica comercial, Integración de sistemas de Gestión, Guía para las empresas, el gobierno y las organizaciones de la comunidad, Bogotá D.C. Colombia 2003 ISBN: 9383-33-5. ICONTEC

[31] Ibíd., p. 79.

[32] CASTILLO, Diana Milena y MARTINEZ, Juan Carlos. Enfoque para Combinar e Integrar la Gestión de Sistemas.2006. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, p.175.

Los elementos básicos que se deben considerar:

- Mapa de procesos
- Mapa Físico
- Mapa de Riesgos
- Mapas de zonas de amenazas
- Estructura Jerárquica o el organigrama
- Análisis del entorno o nicho de mercado
- Listado de productos o servicios
- Listado de caracterización de clientes
- Listado de proveedores

- **Controles en el sistema integrado.** Como dice Castillo y Martinez[33] para la integración de sistemas de gestión, se trabaja sobre unos controles, que son control de tipo humano, control de documentos en lo administrativo y un control operativo y de emergencia en lo técnico.

- **Beneficios y Riesgos del Sistema Integrado de Gestión.** Al disponer de un sistema integrado de gestión, la organización dispone de varios beneficios, en términos legales, financieros, de prestación del servicio, de producción, de gestión, imagen, pero también no está sujeta a tener algunos riesgos que están unidos al estado inicial del sistema de gestión, ya que no es lo mismo integrar cuando no se cuenta con ningún modelo de gestión implementado, que cuando ya se cuenta con uno o varios ya implementados[34].

Aquellas organizaciones que desarrollan sistemas integrados de gestión, integrando los aspectos de tipo legal, se caracterizan por ser sinérgicas en las identificación, interpretación y cumplimiento de los requisitos legales. Pensar en un requisito legal de forma unificada y no por partes, nos permite tener un dominio total y monitoreo permanente sobre las acciones legales.

- **Experiencias de la implementación en Colombia.** El grupo Bavaria fue una de las primeras empresas en integrar sistemas de gestión, Bavaria en un foro del 2004 compartieron los beneficios y resultados en cuanto al desempeño, imagen, procesos y recursos[35].

- **Desempeño: l**ograron las metas del plan del negocio, incrementaron las ventas y el fortalecimiento de su proyección internacional.

---

[33] CASTILLO, Diana Milena y MARTINEZ, Juan Carlos. Enfoque para Combinar e Integrar la Gestión de Sistemas.2006. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, p.192

[34] Ibíd., p. 213

[35] Ibíd., p. 219

- **Imagen:** la mejoraron interna y externamente, ya que obtenían la credibilidad de las partes interesadas y facilidad al acceso de ayudas económicas.

- **Procesos:** mayor prevención en el cumplimiento de los requisitos legales y otros.Se puede identificar aquellas actividades que no agregan valor y permitió crear otras actividades con un mayor enfoque al cliente.

- **Recursos:** presentaron mejoras en la infraestructura tecnológica, que llevo al fortalecimiento de las comunicaciones

- **Recomendaciones para Implementar el sistema integrado de gestión. "**Todas las organizaciones se hallan en un entorno cambiante, ya sea en lo tecnológico o todo lo que tenga que ver con los sistemas de gestión, esto lleva a que las organizaciones efectúen esfuerzos para que se adapten a las situaciones, ya que esta es la única forma de seguir siendo competitivas y activas en el mercado del cual hacen parte".

Como dice Castillo[36] La integración de los sistemas de gestión, debe afrontarse no por adición, manteniendo estructuras similares en paralelo, sino debe integrar realmente y unificando políticas y criterios.

Los cuatro objetivos fundamentales para la integración no solo en organizaciones de TI, sino de cualquier tipo son:

- Rentabilidad
- Prevención de Perdidas
- Aprovechamiento de las oportunidades
- Crecimiento

Recomendaciones para tener buenos resultados en la integración, y vencer aquellos paradigmas de impedimento de integrar**.**

En la tabla 15, se nombra algunas recomendaciones para tener éxito en la integración de las normas ISO 9001:2015, ISO/IEC 27001:2013, es importante tenerlas en cuenta para poder llegar a cumplir el objetivo.

[36] CASTILLO, Diana Milena y MARTINEZ, Juan Carlos. Enfoque para Combinar e Integrar la Gestión de Sistemas.2006. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, p.192

Tabla 15. Recomendaciones para tener buenos resultados en la integración, de la norma ISO 9001:2015, ISO/IEC 27001:2013

• Se debe mostrar a la alta dirección la importancia del ciclo PHVA, para la aplicación del concepto de gestión y sus respectivos beneficios, para que emprenda los proyectos de mejoramiento.
• La gestión integral se lleva a cabo mediante la utilización de una misma plataforma de gestión, el enfoque por procesos es el elemento indicado
• Realizar una revisión inicial de la organización, la cual nos debe suministrar una información básica
• Establecer cuáles son las autoridades, partes interesadas que interactúan de una forma directa o indirecta con la organización
•Tener presente que toda organización cuenta con clientes, compromisos, personal, requisitos legales, recursos que provienen del medio ambiente, bienes, esto hace que cada acción que decida iniciar la compañía considere los efectos sobre el resto de elementos
• La secuencia que debe circular la compañía que toma la decisión de integrar sus sistemas, lo primero es reducir consecuencias, por lo cual debe trabajar primero en protección y generar las garantías necesarias, luego migrar hacia la prevención, lo primero que toca trabajar es el tratamiento de los riesgos
• Para mejorar la satisfacción de todos nuestros clientes, es importante seguir soportándose en la norma ISO 9001, ya que es la herramienta apropiada como parte del sistema de gestión total
• La secuencia de utilización de las herramientas de gestión, depende de cada uno de los intereses de la compañía, es necesario tener este punto en cuenta ya que haciéndolo como otras lo desarrollaron, puede ser que no funcione, ya que cada organización es única
• Es importante sensibilizar a la alta dirección
• Antes de iniciar, adquirir la mayor información posible de la organización y del entorno de esta
• No establecer la política integral, si la alta dirección no está participando como responsable de su generación
• Las competencias desarrolladas son muy importantes para los resultados de la gestión, ya que al contar con personal sensible a los diferentes intereses de la organización, es una de las primeras fortalezas de la integración de sistemas de calidad en este caso la ISO 9001:2015 , ISO/IEC 27001:2013
• Un buen esquema de trabajo, es el definido por los objetivos, y no por el cumplimiento del horario de trabajo.
• Para definir los objetivos, se debe contar con mediciones previas que tengan que ver con la realidad de la organización

Tabla 15. (Continuación)

• El pilar más importante para la integración, es la competencia del personal que hace parte de los controles de tipo humano
• Se debe documentar lo que se está haciendo y no lo que se piensa hacer
• Las acciones correctivas y preventivas, son importantes para empezar a conocer a partir de qué punto la organización se empezó a comportar como una organización con gestión integral de carácter proactivo
• Para una integración es importante reducir el número de indicadores, es importante quedarnos con los que son de interés de la alta dirección

Fuente: CASTILLO, Diana Milena y MARTINEZ, Juan Carlos Enfoque para Combinar e Integrar la Gestión de Sistemas.2006. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC

Las recomendaciones de la tabla 15, son de gran importancia y se debe tener presente para lograr el éxito en la integración de las normas ISO9001 e ISO/IEC27001:2013.

4.3 ESTRUCTURA DE ALTO NIVEL.

La estructura de alto nivel es la base, para poder integrar los sistemas de gestión, esta estructura como dice Lopez[37] ,fue denominada " Estructura de Alto Nivel", esta estructura, se está aplicando a todas las normas nuevas de sistemas de Gestión, y a sus respectivas revisiones de normas ya existentes, como la norma ISO 9001 en su revisión del 2015

Algunos de los cambios de esta nueva estructura, están sustituir los conceptos de documentos y registros por información documentada, como la desaparición definitiva del concepto de "responsable del sistema".

En el cuadro 1 se muestra la similitud de requisitos entre las normas ISO 9001:2015 y la norma ISO/IEC 27001:2013

[37] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

Cuadro 1 Similitud de requisitos de las normas ISO9001:2015 ISO/IEC 27001:2013

SIMILITUD REQUISITOS DE LAS DOS NORMAS			
ISO 9001:2015		**ISO/IEC 27001:2013**	
0	Introducción	**0**	Introducción
0.1	Generalidades	**0.1**	Generalidades
0.2	Principios de la gestión de calidad	**N/A**	N/A
0.3	Enfoque por procesos	**N/A**	N/A
0.4	Relación con otras normas del sistema de gestión	**0.2**	Compatibilidad con otras normas de sistemas de gestión
1.	Objeto y campo de aplicación	**1.**	Objeto y campo de aplicación
2.	Referencias normativas	**2.**	Referencias normativas
3.	Términos y definiciones	**3.**	Términos y definiciones
4	Contexto de la organización	**4.**	Contexto de la organización
4.1	Compresión de la organización y de su contexto	**4.1**	Conocimiento de la organización y de su contexto
4.2	Comprender las necesidades y expectativas de las partes interesadas	**4.2**	Compresión de las necesidades y expectativas de las partes interesadas
4.3	Determinación del alcance del sistema de gestión de calidad	**4.3**	Determinación del alcance del sistema de gestión de la seguridad de la información
4.4	Sistema de gestión de la calidad y sus procesos	**4.4**	Sistema de gestión de la seguridad de la información
5.	Liderazgo	**5.**	Liderazgo
5.1	Liderazgo y compromiso	**5.1**	Liderazgo y compromiso
5.2	Política	**5.2**	Política
5.3	Roles, responsabilidades y autoridades en la organización	**5.3**	Roles, responsabilidades y autoridades en la organización

Cuadro 1 (Continuación)

6.	Planificación	**6.**	Planificación
6.1	Acciones para abordar riesgos y oportunidades	**6.1**	Acciones para tratar riesgos y oportunidades
6.2	Objetivos de la calidad y planificación para lograrlos	**6.2**	Objetivos de seguridad de la información y planes para lograrlos
6.3	Planificación de los cambios	**N/A**	N/A
7.	Apoyo	**7.**	Soporte
7.1	Recursos	**7.1**	Recursos
7.2	Competencia	**7.2**	Competencia
7.3	Toma de conciencia	**7.3**	Toma de conciencia
7.4	Comunicación	**7.4**	Comunicación
7.5	Información documentada	**7.5**	Información documentada
8.	Operación	**8.**	Operación
8.1	Planificación y control de operación	**8.1**	Planificación y control de operación
8.2	Requisitos para los productos y servicios	**8.2**	Valoración de riesgos de la seguridad de la información
8.3	Diseño y desarrollo de los productos y servicios	**8.3**	Tratamiento de riesgos de la seguridad de la información
8.4	Control de los procesos ,productos y servicio suministrados externamente	**N/A**	N/A
8.5	Producción y provisión del servicios	**N/A**	N/A
8.6	Liberación de los productos y servicios	**N/A**	N/A
8.7	Las salidas no conformes	**N/A**	N/A
9.	Evaluación del desempeño	**9.**	Evaluación del desempeño
9.1	Seguimiento, medición, análisis y evaluación	**9.1**	Seguimiento, medición, análisis y evaluación
9.2	Auditoria interna	**9.2**	Auditoria interna
9.3	Revisión por la dirección	**9.3**	Revisión por la dirección
10.	Mejora	**10.**	Mejora
10.1	Generalidades	**N/A**	N/A
10.2	No conformidad y acción correctiva	**10.2**	No conformidad y acción correctiva
10.3	Mejora Continua	**10.3**	Mejora Continua

Fuente: Elaboración propia. Basado en trabajo de grado especialización gestión integral QHSE, Diseño de un sistema integrado de gestión basado en la norma ISO9001-2015, ISO 27001:2013. Cristian Cárdenas y Dayron Higuera.

Las normas que ya han sido armonizadas con esta estructura son las indicadas en la Tabla 16: y al estar ajustadas es mucho más fácil realizar la integración

Tabla 16. Normas ya Armonizadas

NORMA	DESCRIPCIÓN
ISO 22301: 2012	Sistemas de Gestión de la Continuidad del Negocio
ISO 39001: 2012	Sistemas de Gestión de Seguridad Vial
ISO 27001: 2013	Sistemas de Gestión de la Seguridad de la Información
ISO 90011: 2015	Sistemas de Gestión de Calidad
ISO 14001 : 2015	Sistemas de Gestión del Medio Ambiente

Fuente: LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7.

Esta estructura es aplicada a las normas ISO, especificaciones de acceso público (PAS) y especificaciones técnicas (TS), esta estructura está compuesta por 10 cláusulas, las cuales de muestran en la tabla 17.

Tabla 17. Estructura Alto Nivel

NORMA	DESCRIPCIÓN
1 Cláusula	Objeto y campo de aplicación
2 Cláusula	Referencias Normativas
3 Cláusula	Término y definiciones
4 Cláusula	Contexto de la organización
5 Cláusula	Liderazgo
6 Cláusula	Planificación
7 Cláusula	Soporte
8 Cláusula	Operación
9 Cláusula	Evaluación del desempeño
10 Cláusula	Mejora

Fuente:basado en INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN [ICONTEC].

En la tabla 17, se describe cada una de las cláusulas que componen la estructura de alto nivel, y cada descripción, esta estructura la contiene la norma ISO9001 y la norma ISO/IEC: 27001:2013.

4.4 FASES PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO

La verificación de las similitudes de los requisitos entre las normas ISO9001:2015, e ISO/IEC: 27001:2013 está conformado por 4 fases las cuales son detalladas a continuación.

4.4.1 Fase de diagnóstico. En esta etapa se realiza el levantamiento de información con el fin de conocer las posibles tareas a realizar**.**

- "Lo primero y lo más importante al iniciar un proyecto de implementación de un sistema de gestión es contar con el apoyo de la alta dirección.
- El segundo paso tiene que ver con la definición del alcance.
- El tercer paso es establecer los objetivos de la etapa de diagnóstico
- El cuarto paso es establecer el equipo de trabajo
- El quinto paso es realizar el cronograma con las actividades a ejecutar"[38]

En esta fase es importante conocer la cultura organizacional de la empresa a la cual se le realizara la posible integración.

Es importante conocer la misión, visión, políticas, procesos, manuales de la compañía; es trascendental hablar con los líderes de cada proceso, observar cómo funciona cada proceso, de esa forma se puede realizar un diagnóstico, para al final conocer que se tiene y que hace falta al interior de la organización, para poder implementar un Sistema Integrado de Gestión.

4.4.2 Fase de planeación. "Para llevar a cabo esta etapa es necesaria la elaboración de un plan de trabajo detallado, donde se enumeren las actividades que se llevaran a cabo para poder implementar estas normas desde el punto de vista de la documentación"[39]

El desarrollo de una metodología para la implementación simultánea de las normas ISO 9001:2015, e ISO/IEC 27001:2013 es necesario que se conforme un grupo de trabajo y poner en marcha este proceso.

[38] CALDER,Alan.Nueve claves para el éxito una Visión general de la implementación de la norma NTC-ISO /IEC27001

[39] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

En la etapa de planeación se identifica los siguientes aspectos

- Identificación y evaluación de aspectos, impactos y riesgos**.**
- Identificación de requisitos legales y de cualquier otro tipo
- Planificación de contingencias
- Objetivos y sus programas para su cumplimiento
- Una estructura organizativa,funciones,responsabilidades y autoridades

Para poder ejecutar esta etapa es significativo articular un plan de trabajo para poder generar la documentación.

En la etapa de planeación, se identifica y evalúan los "riesgos", tema de gran interés, ya que interviene en cada parte de este trabajo.

- **Gestión del riesgo:** según Lopez[40], la organización debe estar al tanto de que existe riesgo en todos y cada uno de los procesos, por lo cual deben ser tratados, la gestión del riesgo nos permite gestionarlo antes de que este ocurra, el proceso de análisis de riesgos facilita a las organizaciones a identificar eventos adversos.

La gestión del riesgo forma parte de las fases de planificación e implementación y debe ser tenido en cuenta en todas las fases; de esta forma es necesario tener claro que no todos los procesos de sistema de gestión tengan los mismos riesgos.

Al aplicar un enfoque racional en el riesgo, tiene efectos positivos para las organizaciones, ya que permiten mejorar la capacidad para lograr los objetivos propuestos.

La norma ISO 31000:2010 Gestión del riesgo que trata de Principios y directrices**,** plantea una serie de directrices para el trato del riesgo, la cual se puede aplicar a cualquier organización, la norma propone unos principios, para tener una gestión del riesgo eficaz:

- Crea valor
- Forma parte de la toma de decisiones
- Trata la incertidumbre
- Es sistemática, estructurada y adecuada
- Se basa en la mejor información disponible
- Está hecha a la medida de la organización
- Es transparente e inclusiva
- Facilita la mejora continua de la organización

[40] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

- **Grupos de trabajo:** como dice Cortes[41], las personas que estén seleccionados en los grupos de trabajo deben tener un gran conocimiento de la organización, deben estar comprometidas con la compañía, por tal razón al momento de elegir este personal debe ser cuidadoso, ya que el éxito depende del grupo y tipo de personas que lo conforman.

- **Asignación de responsabilidades:** es importante asignar responsabilidades claras, ya que es la única forma de poder evaluar el desempeño de manera efectiva de cada uno de los grupos que se conforman

- **Asignación de recursos:** la asignación de recursos es clave, para poder llevar a feliz término nuestra implementación, es importante tener en cuenta los recursos físicos, técnicos, humanos, financieros

- **Capacitación:** la capacitación es fundamental para poder cumplir todos y cada uno de los objetivos propuestos, estas capacitaciones se deben realizar en todos los niveles de la organización, directivos, técnicos, supervisores, ya que es importante dar a conocer a todo el personal los beneficios, costos, consecuencias al implementar estos estándares

4.4.3 Fase de desarrollo. ‘‘Las personas deben evaluar la situación actual, y establecer qué le falta a la organización para que sus destrezas de trabajo estén conformes a las normas ISO 9001:2015 e ISO/IEC 27001:2015”.
Las normas nos brindan la oportunidad de decidir de acuerdo a la organización, su tamaño, actividad que desempeña, complejidad en cada uno de sus procesos que la componen.

Para que nuestro sistema de gestión integrado cumpla el objetivo por el cual está siendo implementado, las normas requieren de la presencia de documentos como:

- Objetivos de calidad
- Manual de calidad
- Control de riesgos de calidad
- Auditorías Internas
- Acciones correctivas
- Acciones preventivas
- Revisión de los requisitos

[41] CORTÉS R., Diana Marcela y ARDILA, Alix Victoria. Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001 [en línea]. Trabajo de grado Especialista en Gerencia de Procesos y Calidad. Bogotá: Universidad EAN, 2012 [consulta: 10 de diciembre de 2016]. Disponible en internet: <http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2>.

- Elementos de Entrada, diseño y desarrollo
- Auditorías internas
- Tratamiento de las no conformidades
- Revisiones por la dirección del sistema de gestión de calidad

Cuando se tenga toda la documentación, se debe verificar con que archivo cuenta la organización para determinar que tiene y que falta; de esta forma se determina que se puede eliminar, actualizar, y crear; para el cumplimiento de las normas, toda la información es necesario que la alta dirección tenga conocimiento, ya que el proceso de certificación debe ser de conocimiento de todos.

Después del análisis que realiza la alta gerencia, deben dar una serie de observaciones y luego el visto bueno para poder continuar

4.4.4 Fase de implementación. Como dice Lopez[42], en esta etapa se debe realizar la adecuación del sistema documental de la organización, contando con el visto bueno de la alta dirección y teniendo en cuenta las observaciones resultantes de la revisión gerencial.

Es importante que todo el personal de la organización tenga en mente que trabajar con este sistema integrado ISO 9001 y 27001, es un proceso cíclico de mejora continua y no va a ser culminado en un solo gran paso, se necesita compromiso y entrega por parte de toda la organización.

Para esto se requiere de:

- Personal competente sobre la base de su formación capacitación, habilidades de relevancia e importancia de sus actividades y de cómo contribuyen al logro de los objetivo.
- Los recursos y la infraestructura que es necesaria para poder lograr los objetivos
- Una excelente comunicación interna y externa

Según Cortes[43], ya implementado el sistema integrado, es necesario efectuar un sistema de auditoria interna del sistema documental, con base a los requisitos de las normas ISO9001:2015 y ISO/IEC/27001:2013, es importante que los requisitos

[42] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

[43] CORTÉS R., Diana Marcela y ARDILA, Alix Victoria. Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001 [en línea]. Trabajo de grado Especialista en Gerencia de Procesos y Calidad. Bogotá: Universidad EAN, 2012 [consulta: 10 de diciembre de 2016]. Disponible en internet: <http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2>.

de la documentación del sistema integrado este de acuerdo con los requisitos de calidad de las normas que deseamos implementar.

Luego de implementado nuestro Sistema Integrado de Gestión, la organización puede escalar al tema de certificación.

4.5 HERRAMIENTAS.

Algunas de las herramientas que se pueden validar para su utilización, al momento de hacer la implementación del sistema integrado de gestión son:

4.5.1 ACURITY STREAM. Un paquete de software muy completo, sencillo de utilizar que automatiza los complejos procesos necesarios para gestionar el cumplimiento normativo y realizar la gestión del riesgo de una manera eficaz**.**

4.5.2 CALLIO. Callio Secura 17799, producto basado en la web, permite al usuario realizar tareas necesarias para implementar, gestionar y poder certificar un Sistema de Gestión de Seguridad de la Información, gestiona el cuerpo documental del SGSI.

4.5.3 EAR/PILAR. Esta herramienta brinda soporte, el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit, está diseñada para apoyar el proceso de gestión del riesgo a lo largo de periodos prolongados.

4.5.4 ECIJA I SGSI. Es una herramienta web, esta nos permite la gestión integral de la seguridad de la información basado en un ciclo de mejora continua (PDCA) y el seguimiento centralizado de las obligaciones que establecen los estándares internacionales.

4.5.5 GLOBALSGSI. Es una herramienta de gestión integral de la norma ISO 27001, desarrollada por Audisec Seguridad de la información S.L. que cumple con el ciclo completo de la misma, ayuda a acompañar al proyecto de realización de un SGSI desde su nacimiento.

4.5.6 GStool. Desarrollada por Bundesamt für Sicherheit in der informationstechnik (BSI) del gobierno alemán, para dar soporte a los usuarios del manual básico de protección de las TI, los usuarios tienen a su disposición un sistema de generación de informes.

4.5.7 ISAMM. Esta herramienta está alineada con el conjunto de controles de las mejores prácticas en seguridad de la información de la ISO/IEC 27002, un análisis de gestión del riesgo según esta herramienta está basado en determinación del alcance, análisis de riesgo e informes.

4.5.8 S²SGSI. Ha sido diseñada por el grupo SIA, para dar soporte a la gestión eficiente de las principales actividades derivadas de la implementación de un SGSI, esta facilita los procesos de implementación y el mantenimiento de la misma.

4.5.9 SECURIA SGSI. Es una herramienta integral, desarrollada bajo licencia GNU, por el centro europeo de empresas e innovación de Albacete, esta herramienta cubre el proceso automático de implementación, puesta en marcha, mantenimiento y mejora continua de un SGSI, según la norma ISO 27001.

4.6 METODOLOGÍAS PARA LA GESTIÓN DEL RIESGO.

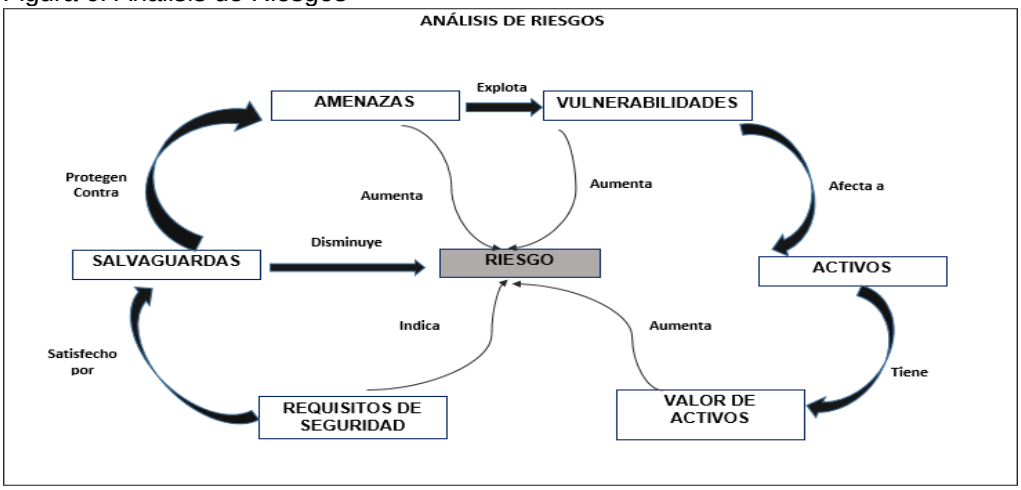
La metodología debe ser capaz de analizar procesos complejos y reducir los mismos, para que a partir de esto sea posible describir y entender dichos procesos, la metodología debe ser consistente y repetible, la metodología deberá reunir los siguientes características.

- Objetiva.
- Fiable.
- Medible
- Repetible.
- Permitir la medición continua.
- Enfocada en términos entendibles por la organización.
- Estar soportada por una herramienta de gestión.

Por lo tanto la elección de la metodología debe estar fundada en las mejores prácticas, existen muchas metodologías de evaluación del riesgo las cuales son aceptadas internacionalmente, la ISO27001, no especifica que metodología utilizar, pero la más reciente publicada ISO/IEC 27005:2011 (Information technology-security techniques-information security risk management, proporciona algunas pautas para la gestión del riesgo en la seguridad de la información.

En la figura 6, se describe todos los factores que intervienen en el Riesgo, lo que es importante dar a conocer

Figura 6. Análisis de Riesgos



Fuente: basado en Merino Bada Cristina y Cañizares Ricardo Implantación de un Sistema de gestión de seguridad de la información según ISO 27001

Según Paloma López[44], las metodologías más conocidas para la gestión del riesgo en el ámbito de la seguridad de la información son las siguientes:

4.6.1 Magerit. Tiene un uso muy amplio en España, en las organizaciones públicas, al haber sido desarrollada por el Consejo Superior de la Administración Electrónica. No es muy conocida a nivel internacional.

4.6.2 Cramm. Origen Británico, fue desarrollada por CCTA "Central Computer and Telecommunications Agency" es reconocida a nivel internacional y es muy simple, identificación y valoración de activos, valoración de amenazas, vulnerabilidades.

4.6.3 Octave. Desarrollada en Estados Unidos, por SEI "Software Engineering Institute", es un poco compleja de aplicar, pero es reconocida internacionalmente.

4.6.4 NIST800-30. De origen Norte Americano desarrollada por NIST (National Institute of Standards and Techhnology), el uso prácticamente limitado a las administraciones publicar norteamericanas.es muy simple de manejar.

4.6.5 ISO 31000. Norma internacional de referencia para la gestión de los riesgos, se puede aplicar cualquier tipo de riesgo; Metodologías para el análisis del riesgo en la seguridad de la información.

[44] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

López[45], también indica que las vulnerabilidades más comunes de los activos están asociadas con:

- Fallos en la seguridad de las instalaciones (protección física del edificio)
- Desastres naturales (incontrolables)
- Amenazas internas (sabotajes)
- Robos (destrucción de activos por parte del personal)
- Intrusiones externas (virus, troyanos)
- Fallos (con los procedimientos de control o controles de acceso no definidos, ejemplo claves, contraseñas)
- Defectos de configuración de hardware (poca memoria, no capacidad en los discos duros)
- Software mal configurado
- Perdida de los activos

Es necesario poder medir, ya que como se dice lo que no se mide no es posible mejorar, por tal motivo es preciso conocer la evolución de nuestro sistema de gestión, ya que demandamos saber si los controles que tenemos implantados están funcionando correctamente, y para ello debemos definir una serie de indicadores para poder lograr esto.

Los indicadores deben proporcionar resultados comparables y reproducibles, la persona o responsables de la seguridad son los encargados de controlar los indicadores y objetivos de seguridad.

Software de apoyo para la ejecución del sistema de gestión:

Isolution: software licenciado, ofrece un software para la gestión integral de las normas ISO, se puede parametrizar de acuerdo a las necesidades de cada compañía, se adquiere por suscripción, Isolution es una empresa colombiana

Esta herramienta está compuesta por módulos como:

- Gestión documental
- Indicadores
- Sistema de mejora
- MECI
- Riesgos
- Proveedores
- Talento Humano
- Tareas pendientes

[45] LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7

- Divulgación y comunicación
- Clientes

ITS Gestión: este software es licenciado, nos sirve como apoyo para implementar sistemas de gestión, consta de los siguientes módulos[46]

- Administración documental
- Auditorías internas de calidad
- Acciones de mejora
- Indicadores
- Administración de riesgos
- PQR
- Revisión por la dirección
- Actas y seguimiento a tareas

EGAM: esta herramienta es española, es un software licenciado y nos brinda apoyo en los siguientes aspectos

- Auto gestionar evidencias y registros
- Gestionar en tiempo real requisitos de certificación y auditoria
- Eliminar toda la documentación en papel
- Está integrado con Microsoft Outlook
- Se configura a la medida de los procesos
- Supervisa en tiempo real tareas y responsabilidades

ISO TOOLS: es una herramienta web, es licenciada, es una herramienta que permite personalizar según a la norma que se requiera, solo se necesita de usuario y password, lo práctico de esta herramienta es que se utiliza en la nube no necesita de comprar hardware, ya que adquirir el paquete todo viene incluido

OpenKM: es una herramienta de software libre, nos permite controlar toda la documentación que se genere en los procesos de implementación, tiene un sistema de seguridad, si se borrara los datos el guarda una copia del sistema, este software obtendrá todas las comunicaciones que se hagan las clasificara y almacena para una revisión, tiene un control de versiones.

[46] ITS Gestión – Software Gestión de Calidad,ITS Soluciones, http://www.its-solutions.net/software-gestion-de-calidad-its-gestion/

KMKEY Quality: software libre, es un software que nos permite hacer gestión a la calidad, es muy fácil de usar, es una herramienta que brinda un entorno colaborativo, este software nos permite:

- Organización
- Gestionar la documentación
- Indicadores
- Revisiones por la dirección
- Acciones correctivas
- No conformidades
- Acciones preventivas
- Mejoras
- Auditorias
- Seguimiento
- Reclamaciones

4.7 COMPONENTES PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO DEGESTIÓN

Cuadro 2. Componentes para implementar un sistema integrado de gestión

Responsabilidad y Liderazgo de la Dirección	En este componente identificamos las partes del sistema de gestión integrado, en la cual la alta dirección desempeña una función clave.
Liderazgo Eficaz	Un sistema de gestión eficaz requiere de la participación de todas las partes de la organización, la dirección requiere que todos tengan conciencia de cómo sus acciones o la misma ausencia de estas pueden influir directamente en la eficacia del sistema. El liderazgo eficaz requiere de: • Pertenencia, la cual se demuestra por el compromiso • Planificación de tareas y recursos dentro de la estructura • Asignación de recursos • Asignación de las responsabilidades a través de la organización y deberes acordados • Determinar la eficacia del sistema • Identificar, planear oportunidades de mejora
Política y Objetivos	la organización debería tener declaraciones que reflejen sus políticas, la alta dirección es responsable de las entradas para la formulación y modificación de las políticas, se debería fundar objetivos para poder dar el cumplimiento a las políticas
Gestión del Cambio	Un sistema de Gestión puede facilitar la gestión del cambio y los factores claves de este son las prioridades para el cambio y los riesgos que este puede tener, todo cambio debe estar alineado con los objetivos establecidos por la organización.
Organización	La dirección necesita establecer una estructura definida, esto permite que las personas comprendan su función dentro de la organización
Identificación y Suministros de Recursos	La alta dirección debe identificar los recursos con los que cuenta, recurso humano, físico, financieros
Participación de los Empleados	Es el compromiso de las personas individuales, en el contexto de los valores compartidos, el que transforma un sistema de Gestión documentado en una red de procesos eficaz. Los empleados deben estar en el establecimiento de las metas
Planificación	La planeación debe incluir metas a corto y a largo plazo y la mejora continua
Implementación	La implementación de un sistema de Gestión, se puede emprender por etapas y se debe basar en el nivel de toma de conciencia sobre los requisitos, aspectos y beneficios
Seguimiento	La dirección debe asegurar que estas actividades brindan la información necesaria para que la organización pueda decidir si su desempeño está de acuerdo con si política, objetivos y metas

Cuadro 2 (Continuación)

Mejora	la mejora continua se logra mediante la evaluación regular del desempeño del sistema de gestión contra las políticas, objetivos, metas y criterios de desempeño
Participación de las Partes Interesadas	La alta dirección debería asegurar que todas las partes interesadas pertinentes están identificadas, las opiniones de las partes interesadas deben ser tenidas en cuenta
Identificación y Análisis de Necesidades	Todas las empresas tienen varias partes interesas, clientes, proveedores, propietarios, empleados, gobierno, la comunidad. Las necesidades y expectativas de las partes interesadas se deben tener en cuenta ya que brindan entradas al desarrollo de un Sistema de Gestión Integrado. Cuando se establece un Sistema de Gestión Integrado, la posición actual de una organización en relación al sistema de gestión, se puede determinar por medio de una revisión inicial, los resultados de la revisión se deben documentar y deberían proporcionar los elementos de entrada para el "desarrollo de la estructura y objetivos de la integración" La revisión inicial puede implicar lo siguiente: • Identificación de todos los requisitos legislativos y regulatorios aplicables • Identificar los aspectos de las actividades, productos o servicios, para poder así determinar aquellos que tienen o pueden tener impactos y responsabilidades. • Las prácticas y procedimientos de Gestión existentes • Identificación de las políticas y procedimientos existentes que tratan sobre actividades de compra y contratación • Las oportunidades de ventajas competitivas • Las opiniones de las partes interesadas Las funciones o actividades de otros sistemas organizacionales puedan impedir o posibilitar el desempeño
Política y Objetivos	La alta dirección debe establecer la política global de la organización, se pueden desarrollar varias políticas secundarias aplicables a actividades específicas, las políticas envían un mensaje claro que la organización tiene una visión y un compromiso que aplicaran de principio a fin. Objetivos y metas: se debe establecer objetivos para poder cumplir con la políticas de la organización, estas se deben revisar y actualizar periódicamente, teniendo en cuenta las consideraciones de las partes interesadas, cuando se tiene esto la organización debe establecer "indicadores de desempeño" los cuales se pueden usar como base para la evaluación del desempeño de los sistemas de Gestión

Cuadro 2 (continuación)

Planificación e Implementación del Sistema	Un sistema de Gestión es la estructura, procedimientos, procesos y recursos que la organización necesita para lograr sus políticas y objetivos Para poder cumplir con estos objetivos, la organización debe asegurar que los factores técnicos, administrativos y humanos que afectan las actividades de la organización estén controlados, para lograr la eficacia máxima y satisfacer las expectativas de los clientes y partes involucradas, es esencial que el sistema de gestión sea apropiado para el tipo de actividad, para los productos o servicios que se ofrecen y para las expectativas de las partes interesadas
Documentación del Sistema de Gestión	La documentación es parte clave de cualquier sistema de gestión y se debe ajustar a las necesidades de la organización y de los individuos que usan el sistema. Los procesos y procedimientos operacionales se deben definir, documentar y actualizar apropiadamente según las necesidades, la cantidad y grado de documentación variara dependiendo del tamaño de la organización, la documentación se puede usar para: • Introducir o desarrollar nuevas tecnologías • Divulgar las políticas, objetivos, metas, programas y logros de la organización • Informar sobre nuevos competidores que entran al mercado Introducir nuevos productos o servicios
Asignación de Recursos	La dirección debe identificar, brindar y priorizar los recursos humanos apropiados, de infraestructura, información, financieros adecuados, lo cual es esencial para la implementación de las políticas de una organización y el logro de los objetivos. Para poder suministrar estos recursos puede ser necesario: • Entrenar personal, para que adquiera las habilidades necesarias. • Buscar personal adicional, ya sea temporal o permanente • Desarrollar o mejorar el ambiente de trabajo para todos los empleados • Desarrollar nuevos procesos o nuevos métodos de trabajo
Gestión de Procesos y Actividades	El sistema de Gestión se aplica a todos los procesos y actividades dentro de la organización e interactúa con ellos, la gestión de los procesos es fundamental para la fabricación de productos o servicios de la calidad requerida. Es conveniente verificar que los procesos están en capacidad de lograr el resultado requerido de acuerdo con las especificaciones, los procesos son importantes para la calidad, seguridad o impacto ambiental del producto o servicio, se debe planificar, aprobar hacer seguimiento y controlarlos

Cuadro 2 (continuación)

Medición y Seguimiento	Es importante medir, hacer seguimiento y evaluar ya que es clave para que la organización pueda determinar si el sistema tiene un desempeño de acuerdo con las políticas, metas y objetivos de gestión. Para ser eficaz se debe establecer procesos apropiados para poder asegurar la confiabilidad de los datos, las personas que realicen las mediciones deben ser competentes en estas actividades, la organización necesita establecer los criterios y procedimientos de verificación que demostraran que se ha cumplido los requisitos específicos, esto incluye todos los aspectos de las actividades de la organización, cuando esta verificación indica una falla en el cumplimiento de estos requisitos, la organización debe contar con los procedimientos para tratar los incidentes, quejas o cualquier otra no conformidad, estos procedimientos deben ser oportunos para poder posibilitar la solución de los mismos. Se debe llevar a cabo evaluaciones periódicas del Sistema de Gestión y el status organizacional, para poder determinar si el sistema ha sido implementado y mantenido apropiadamente

Nota: la información del cuadro 2, se genera por la investigación generada al documento ICONTEC 9000, Guía Internacional para una mejor práctica comercial, Integración de sistemas de Gestión, Guía para las empresas, el gobierno y las organizaciones de la comunidad, Bogotá D.C. Colombia 2003 ISBN:9383-33-5

5. CONCLUSIONES

- La seguridad de la información debe intervenir en cada uno de los procesos de la estructura, ya que nos permite proteger el activo más importante que tiene una organización que es la información.

- Un sistema de gestión de calidad es entrar a la cultura de la calidad, y esta aplicación necesita de un análisis de los beneficios y costos de esta implementación.

- La implementación de un sistema integrado de gestión de calidad se hace posible en la medida, que se identifican todos los requisitos de las normas a integrar.

- Se considera que esta guía desarrollada, satisface todas aquellas ideas planteadas al inicio, y puede servir como una referencia para el desarrollo de otras guías que tengan que ver con el tema de sistemas integrados de gestión.

- Para la implementación exitosa de un sistema de gestión integrado, debe estar toda la organización comprometida desde el área operativa hasta la alta gerencia.

- Para que las organizaciones tengan una competitividad en el mercado, se requiere de estándares de calidad.

- La elaboración de esta monografía, aporto académicamente al aprendizaje de temas de calidad, que no se tenían claros, como conceptos, identificación de algunos requisitos de las normas y su contexto

- Mediante el sistema integrado de gestión se puede tener una mejora continua mucho más eficiente, si la organización cuenta con uno o más sistema de gestión.

- Un sistema integrado de gestión, permite tener menos esfuerzo de trabajo, que implementando normas por separado.

- Para poder acoplar un sistema integrado de gestión, es importante que las normas a implementar tengan una estructura de alto nivel, ya que de esta forma es más sencillo y fácil la implementación

- El éxito de una organización, está en poder evaluar claramente sus procesos y esto se logra por medio de estándares de calidad.

- Es importante la capacitación y compromiso de aquellas personas que intervienen en el desarrollo del sistema integrado de gestión.

6. RECOMENDACIONES

Para la implementación del sistema integrado de gestión es importante tener una serie de recomendaciones.

- Para verificar la implementación del sistema integrado de gestión, se recomienda las diferentes herramientas existentes en el mercado.
- Es importante realizar revisiones periódicas de nuestro sistema integrado de gestión, para verificar su correcto funcionamiento
- Las personas que diseñen el sistema integrado de gestión deben estar capacitados.
- No implementar un sistema integrado de gestión porque si, se debe tener claro él porque es necesario el sistema integrado.
- Cuando se tenga implementado el sistema, se deben hacer actualizaciones periódicas de la documentación.
- Tener claro todos los elementos que intervienen en el sistema de seguridad de la información.
- La calidad no tiene precio, la calidad nos lleva al éxito.
- El trabajo en equipo, es un factor determinante para la eficiencia colectiva de la compañía.
- Implementar las actividades que sean necesarias para mantener el sistema integrado de gestión.
- La alta gerencia de la organización, debe estar comprometida con el sistema de gestión de la organización.

7. BIBLIOGRAFÍA

CORLETTI ESTRADA, Alejandro. Seguridad por niveles. Madrid: DarFE Learning Consulting, 2011.

CORTÉS R., Diana Marcela y ARDILA, Alix Victoria. Metodología para la implementación de un sistema integrado de gestión con las normas ISO 9001, ISO 20000 e ISO 27001 [en línea]. Trabajo de grado Especialista en Gerencia de Procesos y Calidad. Bogotá: Universidad EAN, 2012 [consulta: 10 de diciembre de 2016]. Disponible en internet: <http://repository.ean.edu.co/bitstream/handle/10882/2779/CortesDiana2012.pdf?sequence=2>.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN [ICONTEC]. NTC-ISO 9000, Sistemas de gestión de la calidad -- Fundamentos y vocabulario, 2.a actualización. Bogotá: El Instituto, 2015. 56 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN [ICONTEC]. NTC-ISO 9001, Sistemas de gestión de la calidad. Requisitos, 4.a actualización. Bogotá: El Instituto, 2015. 33 p.

ISO. The ISO Survey of Management System Standard Certifications (1993-2015) [base de datos en línea]. [Consulta: 27 de febrero de 2017]. Disponible en internet: <https://www.iso.org/files/live/sites/isoorg/files/standards/conformity_assessment/certification/doc/Survey-data/iso_9001_iso_survey2015.xls>.

LABOUCHEIX, Vincent. Tratado de la calidad total. México: Limusa, 2001, p. 14.

LÓPEZ LEMOS, Paloma. Novedades de ISO: 2015. Madrid: Fundación confemetal, 2016. ISBN 978-84-16671-00-7.

MANTILLA GUERRA, Anibal Ruben. Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base a la norma ISO 27001. 17 [en línea]. Tesis Máster en Gestión de las Comunicaciones y Tecnologías de la Información, MSC. Quito: Escuela Politécnica Nacional, 2009 [consulta: 11 de enero de 2017]. Disponible en internet: <http://bibdigital.epn.edu.ec/retrieve/30968/CD-2254.pdf>.

ZUBIETA GUILLÉN, José M.a y ALFARO LARRAGUETA, Eduardo Alfaro. Soluciones en las empresas de TI mediante la aplicación de un sistema de gestión ISO 20000 parte 1 integrado a un sistema ISO 27001 e ISO 9001 [en línea]. Trabajo de grado Ingeniero Técnico Industrial Eléctrico. Pamplona (España): Universidad Pública de Navarra, 2010 [consulta: 20 de noviembre de 2016], p. 5. Disponible en internet <http://docplayer.es/4468561-Escuela-tecnica-superior-de-ingenieros-industriales-y-de-telecomunicacion.html>.

ZUCCARDI, Giiovanni y GUTIÉRREZ, Juan David. ISO-27001:2005 [en línea]. [consulta: 2 de octubre de 2016]. Disponible en internet: <http://pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001v0.1.pdf>.

Bada Merino, Cristina. Implantación de un Sistema de Gestión de Seguridad de la Informacion Segun ISO27001. Madrid : FUNDACION COMFEMETAL. 74-28006.

COLOMBIANA, NORMA TECNICA. 2015. sistemas de gestion de la calidad. Bogota : icontec, 2015.

MESQUILE C., Luis, Modelo para facilitar la interacción de estándares de gestión de TI en entornos maduros. Tesis doctoral para optar el grado en Doctor en informática. España: Universitat de les Illes Balears, 2012