METODOLOGIA PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION CON LAS NORMAS ISO 9001, ISO 20000 e ISO 27001.

Preparado por:

DIANA MARCELA CORTES R.

ALIX VICTORIA ARDILA.

Trabajo presentado como requisito para obtener el título de

Especialista en Gerencia de Procesos y Calidad.

TUTOR

ING. JAIRO BUSTAMANTE.

UNIVERSIDAD EAN

FACULTAD DE POSGRADOS

ESPECILIZACION GERENCIA DE PROCESOS Y CALIDAD

BOGOTA, COLOMBIA

JUNIO, 2012

CONTENIDO

LISTA DE GRAFICOS

..

LISTA DE TABLAS

HOJA DE APROBACION.

METODOLOGIA PARA LA IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION CON LAS NORMAS ISO 9001, ISO 20000 e ISO 27001.

OBSERVACIONES:_____

_____

_____

_____

_____

_____

_____

IFI APROBADO POR: _____

FECHA: _____

AUTORES: DIANA MARCELA CORTES R.

ALIX VICTORIA ARDILA.

RESUMEN.

Generalmente las empresas desarrollan los procesos de calidad y seguridad de una manera independiente, muchas organizaciones están certificadas con ISO 9001 y desconocen que por el simple hecho de tener esta certificación, ya llevan recorrido un camino bastante largo para el logro de nuevas certificaciones y la implementación de nuevos estándares de calidad dentro de sus procesos.

Aunque las tres normas abordadas en este trabajo han tenido un origen diferente, todas tienen en común una misma filosofía de gestión; la calidad (ISO 9001) se ha desarrollado impulsada por la competencia y la necesidad de sobresalir en el ámbito empresarial, mientras que la seguridad (ISO 20000 y 27000) ha sido impulsada por el rápido crecimiento de las tecnologías de la información y en algunos casos por el establecimiento de algunas regulaciones propias del mercado. Aun así en los tres casos encontramos que la mejora continua se convierte en un objetivo común el cual se puede aprovechar para el establecimiento de un sistema integrado de gestión.

Así mismo, sí se aplica un paralelo entre los requisitos de las normas, la organización podrá disminuir el volumen de documentación, se agilizaran las acciones para el cumplimiento de requisitos en común entre éstas y las empresas podrán tener un sistema de gestión acorde a la realidad organizacional, no será un sistema de gestión estático ni sobrecargado de documentación.

La organización implementara sistemas de gestión aplicables a su realidad, los cuales mejoraran continuamente el desempeño de los procesos mediante un cambio en la cultura organizacional y la participación activa de todos los niveles jerárquicos de la organización.

1. INTRODUCCION

La implementación de un sistema de gestión es una decisión estratégica que debe involucrar a toda la organización y que debe ser dirigida y apoyada desde la dirección. El diseño dependerá de los objetivos y necesidades de la empresa así como de la estructura, estos elementos son los que van e definir el alcance del sistema, es decir las áreas que van a verse involucradas en el cambio; en ocasiones no es necesario un sistema que implique a toda la organización, puede ser que solo sea necesario en un departamento, una sede en concreto o una unidad de negocio.

El tiempo de implementación de un sistema integral de gestión varía en función del tamaño de la empresa, su estado inicial y los recursos destinados, pero podríamos estimar que su duración es entre seis meses y un año para evitar que quede obsoleto nada mas acabando de implementarlo. Antes de entrar mas en detalle sobre cómo debe hacerse la implementación del sistema hay algo muy importante que siempre debe tenerse en cuenta: la solución más sencilla de implementar y mantener suele ser la más acertada.

La metodología que utilizaremos para la implementación es el modelo PHVA, es un modelo dividido en 4 fases en el que finalizada la última y analizados sus resultados se vuelve a comenzar la primera. Las siglas PHVA son traducidas como Planear, Hacer, Verificar y Actuar, en la primera fase de planear se realiza un estudio de la situación actual de la organización, para

estimar las medidas que se van a implementar en función de las necesidades detectadas. En la fase de hacer se lleva a cabo la implementación de los diferentes controles, así como la concientización y formación para dar a conocer que se está haciendo y por qué al personal de la organización. La tercera fase de Verificar corresponde al seguimiento, en ella se evalúa la eficacia y el éxito de los controles implementados, por ello es importante contar con registros e indicadores que provengan de estos controles. La cuarta fase corresponde al Actuar en la que se llevará a cabo una labor de mantenimiento del sistema; si durante la fase anterior de seguimiento se ha detectado un punto débil este es momento de mejorarlo o corregirlo, para ello se cuenta con tres tipos de medidas: medidas correctivas, medidas preventivas y medidas de mejora. Si el objetivo de la implementación de estos sistemas de gestión es para certificación el ciclo completo tendrá la duración de un año, coincidiendo con las realizaciones de las auditorías de certificación que se realizan cada año.

2. DESARROLLO DEL PROBLEMA

La ISO es la Organización Internacional de Normalización y se encarga de elaborar normas internacionales que el mercado requiere y necesita dando los lineamientos para que las organizaciones lleguen a sus clientes con productos y servicios de calidad. Las normas son de carácter voluntario, nadie obliga o vigila su cumplimiento, sin embargo su uso por millones de empresas facilita el entendimiento entre países y organizaciones y agregan un factor diferenciador a las organizaciones que se encuentran certificadas.

Para asegurar competitividad y sobresalir en el mercado, una organización debe demostrar que sus servicios son gestionados de forma segura, eficiente y eficaz, esto se logra implementando dentro de la organización sistemas de gestión, que permitan un enfoque práctico y seguro de las actividades que se llevan a cabo en su interior.

Al igual que lo sucedido con la norma ISO 9001(Gestión de Calidad), las normas ISO 27001 (Seguridad de la Información) e ISO 20000 (Gestión de Servicios IT), se están convirtiendo en una necesidad de las empresas para sobresalir en el panorama actual, además son consideradas como necesarias en algunos procesos de contratación de la gestión publica y para el cierre de algunos convenios o acuerdos entre empresas. Estas tres normas tienen grandes similitudes, y sucede que al implementar las tres normas, las empresas duplican y repiten mucha

documentación, en el afán de cumplir los requisitos; esto se puede agilizar, si se realiza un paralelo entre los requisitos de las tres normas, sus concordancias y también sus diferencias, para así, ayudar a las empresas a que realicen una implementación mas ágil y efectiva de estas normas.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar un paralelo entre las normas ISO 9001, 20000 e ISO 27001, con el fin de documentar semejanzas y diferencias en los requisitos de cada una, para brindar una herramienta práctica y eficaz a las empresas que estén en proceso de certificación con las tres.

3.2. OBJETIVOS ESPECIFICOS

Realizar un diagnóstico para determinar qué tipo de organizaciones se certifican con las normas ISO 20000, 270001 y 9001 y establecer los beneficios que estas certificaciones significan para cada empresa.

Identificar posibles concordancias, semejanzas y diferencias entre los requisitos de las normas ISO 9001, 20000 e ISO 27001, con el fin de agilizar su implementación y certificación.

Definir una metodología que permita la implementación de dichas normas en cualquier tipo de organización, destacando las fortalezas de cada una, para justificar su implementación paralela y el beneficio que esto puede traer a la organización.

Determinar los factores críticos de éxito para la implementación de estas normas, de manera que si son satisfactorios aseguren un funcionamiento competitivo y exitoso para la organización.

4. JUSTIFICACION

Los beneficios que puede tener una empresa al implementar las normas ISO 9000, ISO 20000 e ISO 27001 dentro de un sistema integrado de gestión se verán reflejados en:

- Posicionamiento de la organización en el mercado.
- Confianza y satisfacción de los clientes.
- Seguridad, eficiencia y productividad en la gestión organizacional.
- Aumento de la eficiencia de la gestión de los sistemas IT y de la consecución de los objetivos y metas de la organización.
- Mejora en la capacidad de reacción de la organización frente a posibles amenazas contra sus sistemas documentales e información confidencial.
- Reducción de recursos y de tiempo empleado en la realización de los procesos integrados.
- Reducción de costos en el mantenimiento del sistema y de evaluación externa, simplificación del proceso de auditoría.
- Menos costos en consultoría de implementación.
- Menos horas de trabajo interno por parte de la organización.

Lo anterior debido a que los clientes al saber que una empresa está certificada en cualquiera de estas normas o en las tres, sienten confianza y respaldo en que los servicios y productos ofrecidos cuentan con procedimientos y controles basados en estándares internacionales que permiten minimizar los riesgos y buscar la excelencia.

5. MARCO TEORICO CONCEPTUAL

5.1. ISO 9001

Especifica los requisitos para un sistema de gestión de calidad que puede utilizarse para su aplicación interna por las organizaciones. Es la base del sistema de gestión de la calidad ya que es una norma internacional certificable y se centra en todos los elementos de administración de calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios.

5.2. ISO 20000

Es el estándar reconocido internacionalmente en gestión de servicios de TI. La norma ISO 20000 se concentra en la gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia, los problemas se clasifican, lo que ayuda a identificar problemas continuados o interrelaciones. La norma considera también la capacidad del sistema, los niveles de gestión necesarios cuando cambia el sistema, la asignación de presupuestos financieros y el control y distribución del software.

La norma ISO 20000 consta de dos partes:

a.) ISO 20000-1 es la especificación formal y define los requisitos que tiene que cumplir una organización para proporcionar servicios gestionados de una calidad aceptable a los clientes. Su alcance incluye:

- Requisitos para un sistema de gestión
- Planificación e implantación de la gestión del servicio
- Planificación e implantación de servicios nuevos o cambiados
- Proceso de prestación de servicios
- Procesos de relaciones
- Procesos de resolución
- Procesos de control y liberación

b.) ISO 20000-2 por otra parte, es el código de procedimiento y describe los mejores procedimientos para procesos de gestión de servicios dentro del ámbito de la norma BS 15000-1. El Código de procedimiento resulta especialmente útil para organizaciones que se preparan para someterse a una auditoría según la norma ISO 20000-1 o para planificar mejoras del servicio.

5.3. ISO 27001

La norma ISO 27001, es un estándar internacional publicado en 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). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI. Es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información (TI).

5.4. DIAGNOSTICO DE LAS ORGANIZACIONES QUE SE CERTIFICAN CON ISO 20000 Y 270001

5.4.1. ORGANIZACIONES QUE SE CERTIFICAN CON ISO 20000

Las empresas que optan por este tipo de certificación son empresas dedicadas a prestar servicios de IT, como centros de procesamiento de datos o data center, organizaciones

dedicadas a realizar monitoreo, soporte y mantenimiento de infraestructura de tecnologías de la información, plataforma de hardware y software, telecomunicaciones, automatización y control, servicios de administración, operación y mantenimiento de aplicaciones, soporte IT entre otros.

Esta certificación, tiene una validez de tres años, es de gran valor para el mercado de las TI pues enmarca las principales exigencias que un proveedor debe cumplir para ofrecer servicios TI alineados con las demandas de sus clientes, agregando seguridad, valor y calidad, mientras asegura la optimización de los costos y garantiza un proceso de mejoramiento continuo en la gestión.

5.4.2. ORGANIZACIONES QUE SE CERTIFICAN CON ISO 27001

El estándar se puede adoptar por la mayoría de los sectores comerciales, industriales y de servicios de pequeñas, medianas o grandes entidades y organizaciones: finanzas, aseguradoras, telecomunicaciones, servicios públicos, minoristas, sectores de manufactura, industrias de servicios diversos, sector del transporte y gobiernos entre otros. Organizaciones donde la información y su manejo son el activo más importante para la operación.

En la actualidad destaca su presencia en empresas dedicadas a servicios de tecnologías de la información, como prueba del compromiso con la seguridad de los datos de sus clientes. La información crítica de una empresa está presente en los sistemas informáticos, pero también en papel, en diferentes tipos de archivos y soportes, se transmite a terceros, se muestra en diversos

formatos audiovisuales, se comparte en conversaciones telefónicas y reuniones y está presente en el propio conocimiento y experiencia de los trabajadores. ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa en donde su objetivo principal es minimizar los riesgos para la empresa en cuanto a pérdida de dinero, pérdida de imagen, pérdida de clientes, pérdida de la confidencialidad, integridad y disponibilidad de la información.

La presencia masiva de sistemas informáticos en el tratamiento de la información lleva a menudo a centrar la atención sólo en la seguridad informática, dejando así expuesta información esencial que no fluye por los sistemas de información y que se enmarca en lo que es la seguridad de la información que abarca los procesos, las personas y la demás documentación física. Por ende La aplicación posterior de controles considera temas como los aspectos organizativos, la clasificación de la información, la inclusión de la seguridad en las responsabilidades laborales, la formación en seguridad de la información, la conformidad con los requisitos legales o la seguridad física, además de controles propiamente técnicos.

Con el rápido avance de la ciencia y la tecnología, cada día las organizaciones están dando mayor importancia al control en la seguridad de la información, una empresa no puede pensar en ser competitiva sin satisfacer a sus clientes entregándole cumplimiento en sus requisitos, calidad en los procesos y en la gestión del cumplimiento de sus necesidades.

Uno de los aspectos que ha ganado más relevancia en las últimas décadas dentro de la calidad es el área de tecnología, que es donde cada organización se basa en sus procesos y sistemas. En muchos países, se han promulgado leyes de protección y privacidad de la

información, haciendo que las empresas tengan como requisito legal implementar servicios de control y protección de la información, y para esto existen varias normas internacionales cuya certificación está tomando mucha importancia en empresas de todos los tamaños para implementar la protección de datos y obtener privacidad de la información, no solo por cumplir con los requisitos legales, sino porque los datos de los clientes y la información de las organizaciones son unos de los principales activos de estas empresas, y si se implementan estas normas, la seguridad cuidará de estos activos.

5.5. VENTAJAS Y BENEFICIOS DE LA IMPLEMENTACION DE ISO 27001, ISO 20000 E ISO 9001

La globalización está despertando una tendencia bien definida hacia la estandarización de los procesos, que ha sugerido la adopción de mejores prácticas en el área de IT, esto es especialmente cierto en organizaciones altamente dependientes de la tecnología informática y se aplica al observar el tipo de organizaciones que tienen las certificaciones ISO 27001 e ISO 20000 en Colombia.

Las certificaciones internacionales, en el entorno de negocios actual, se ven como factores diferenciadores de competitividad global, que definitivamente las empresas que quieran estar a la vanguardia necesitan implementar, y si bien es conocido que hoy este tipo de certificaciones internacionales representan muchas ventajas competitivas, en algunos años serán

los requisitos mínimos para poder sobrevivir en el cambiante mundo de los negocios y la globalización mundial.

A continuación, se describen las ventajas de estas certificaciones, basados en 5 factores básicos para el éxito aplicables a cualquier tipo de organización:

- COMPETITIVIDAD:

Este es el primer factor que le interesa a cualquier empresa, como se menciono 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.

- CALIDAD A LA SEGURIDAD:

Con la implementación de un verdadero sistema de gestión de seguridad de la información SGSI, la seguridad se transformara en una actividad de gestión. Esta se convertirá en una actividad trascendente en la organización, ya que transformará un conjunto de actividades técnicas, en un ciclo de vida metódico y controlado, protegiendo uno de los activos más valiosos de las organizaciones: la información.

- REDUCCION DE RIESGOS:

Con la implementación de los controles y la mejora continua que proponen estas normas, se reducirá al mínimo todo riesgo por robo, fraude, error humano intencionado o no, mal uso de instalaciones y equipo a los cuales esta expuesto el manejo de la información.

- CONCIENTIZACION Y COMPROMISO:

La implementación de e este tipo de estándares crea conciencia y compromiso de seguridad en todos los niveles de la empresa, creando conciencia colectiva de calidad y seguridad, que se ve reflejada en la calidad de los servicios y productos entregados al cliente.

- 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. Además llegado el momento de la visita del organismo certificador, los auditores darán una visión externa y objetiva de la situación de la organización, la cual aporta muchos elementos aplicables a la mejora continua. A continuación otras de las ventajas que traen consigo las certificaciones ISO 27001, ISO 20000 e ISO 9001.

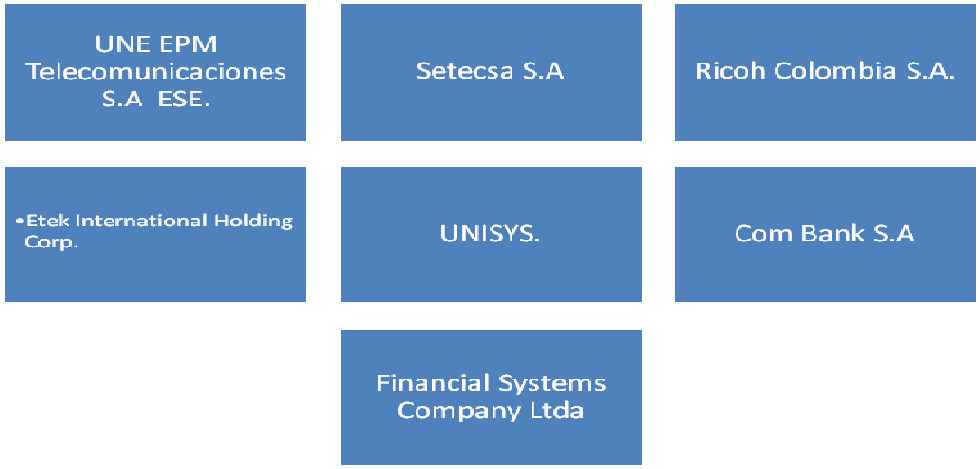
Tabla 1. Ventajas de un sistema integrado de gestión de la información.

Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
Reducción del riesgo de pérdida, robo o corrupción de información.
Los clientes tienen acceso a la información a través medidas de seguridad.
Los riesgos y sus controles son continuamente revisados.
Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
Confianza y reglas claras para las personas de la organización.
Reducción de costes y mejora de los procesos y servicio.
Aumento de la motivación y satisfacción del personal.
Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.
Definitivamente calidad en los productos y servicios prestados.

Fuente: Elaboración propia.

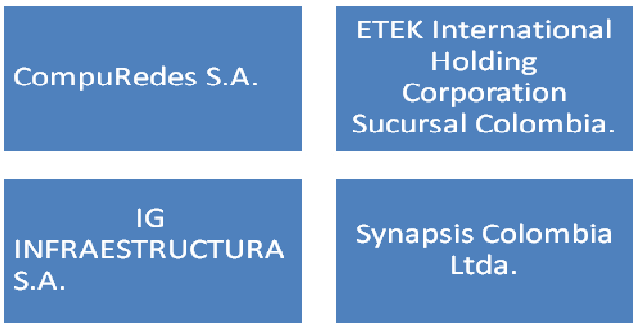
5.6. EMPRESAS QUE HAN ADQUIRIDO LAS CERTIFICACIONES ISO 27001, E ISO 20000 EN COLOMBIA:

Grafica 1. Empresas certificadas ISO 27001 en Colombia



Fuente: adaptada de http://www.iso27001certificates.com/

Grafica 2. Empresas certificadas con ISO 20000 en Colombia



Fuente. Adaptada

http://www.isoiec20000certification.com/home/ISOCertifiedOrganizations/SynapsisColumbia.aspx

Con respecto a las empresas certificadas en ISO 9001 no son mencionadas ya que conforman hoy en día un gran número de organizaciones certificadas en Colombia.

5.7. COMPARATIVO DE LAS NORMAS ISO 9001, 27001 Y 20000

A continuación se presentan los requisitos comunes entre las normas ISO 9001, ISO 20000 e ISO 27001.

Tabla 2. Requisitos comunes entre ISO 9001, 20000 y 27001.

DESCRIPCION	ISO9001	ISO 27001	ISO 20000
Enfoque basado en procesos	X	X	X
Modelo PHVA	X	X	X
Responsabilidad de la Dirección	X	X	X
Control de documentación	X	X	X
Competencia y Formación	X	X	
Auditorías	X	X	X
Seguimiento y Medición	X	X	
Acciones Correctivas	X	X	
Acciones Preventivas	X	X	

Gestión de proveedores	X	X	X
Gestión de cambios		X	X
Continuidad del negocio		X	X
Gestión del riesgos		X	X
Gestión de incidentes		X	X
Gestión de problemas		X	X
Gestión de la capacidad		X	X
Gestión de la configuración		X	X

Fuente: elaboración propia.

Durante esta investigación se ha podido observar que, debido al gran número de elementos comunes entre los tres sistemas de gestión, el esfuerzo necesario para implantar el sistema de gestión integrado propuesto, sería mucho menor que el esfuerzo que supondría implantar las tres normas de manera independiente.

Desde el punto de vista documental pueden aprovecharse los mismos procedimientos para los tres sistemas de gestión. En primer lugar, tanto la ISO 27001 como la ISO 20000 y la ISO 9001, definen un sistema de gestión completo. Como tal, las tres normas siguen un modelo PDCA o HPVA, y por tanto van a requerir el desarrollo de un ciclo de revisión y mejora

continua en el que existan recursos dedicados a la gestión, monitorización, seguimiento, revisión, auditoría y optimización de estos sistemas.

Sin embargo, nada impide que estos recursos sean los mismos, y que en ambos casos el ciclo de revisión y mejora continua se desarrolle bajo las mismas estructuras organizativas. Además, estas normas exigen que el ciclo de revisión sea liderado desde la alta dirección, en base a unas responsabilidades coincidentes que pasan por la definición de políticas y objetivos, la provisión de los recursos necesarios, la difusión del sistema de gestión y la garantía de cumplimiento de lo establecido.

En segundo lugar, estas tres normas centran parte de sus objetivos en el desarrollo de una documentación completa que regule y formalice las actividades desarrolladas bajo estos sistemas de gestión. Y en esa línea, todos los tres sistemas exigen el desarrollo de una gestión documental completa, que cubra todo lo relativo a la gestión de cambios y versiones y estandarice el proceso de revisión y validación formal de la misma, garantizando su viabilidad y operatividad.

Otro de los principales elementos que encontramos en común es el referido a la gestión de terceras partes. Ambas exigen una adecuada gestión de los servicios proporcionados por los distintos proveedores, así como su correcta evaluación y selección. La ISO 20000 se centra más

en la óptima integración de las terceras partes en la cadena de prestación del servicio, mientras que la ISO 27001 profundiza más en los riesgos asociados al intercambio de información que se lleva a cabo con ellos y la ISO 9001 va enfocada a que la organización debe hacer monitoreo y control de los servicios ofrecidos por terceras partes con el fin de ofrecer calidad al cliente final.

A partir de este punto podemos descubrir una gran cantidad de coincidencias entre controles de ISO 27001, ISO 9001 y procesos de ISO 20000. De hecho, algunos de los controles más importantes a la hora de implementar un SGSI están desarrollados en forma de procesos dentro de ISO 20000. Por tanto, podríamos considerar que la ISO 20000 amplía la definición de dichos controles, planteando no sólo los requisitos que se deben cumplir sino la forma en la que se deben llevar a cabo.

Uno de estos controles es el relativo a la gestión de cambios. Gestión de cambios no sólo a nivel documental, como ya se ha indicado anteriormente, sino a nivel global. Las normas exigen una correcta gestión de cambios en las características de los servicios prestados, en las infraestructuras de soporte, en los procedimientos, en los sistemas de información o en el propio sistema de gestión.

Como ya se ha señalado, la ISO 20000 es más exhaustiva a la hora de definir los requisitos en este ámbito, definiendo un proceso específico para ello, pero ambas normas exigen el desarrollo de un ciclo completo de autorización, análisis, evaluación, pruebas, validación,

verificación y aceptación para cualquier cambio significativo que se lleve a cabo dentro de cualquiera de los elementos contemplados en el alcance.

A la hora de garantizar la continuidad de los servicios, las normas se integran y complementan a la perfección. Por un lado, la ISO 20000 se centra en la disponibilidad de los servicios, exigiendo el desarrollo de planes de contingencia y recuperación que garanticen su continuidad a corto plazo. Por otro, la ISO 27001 amplía estas consideraciones y extiende el concepto de disponibilidad hasta los planes de continuidad de negocio, exigiendo su existencia como garantía de la continuidad de los servicios a largo plazo. De este modo, la ISO 20000 permite una aproximación más concreta a los planes de contingencia mientras que la ISO 27001 define el marco de gestión de la continuidad en el que se deben incluir todos los planes desarrollados.

Uno de los apartados en los que la ISO 27001 es más exhaustiva y exigente que la ISO 20000 es el relativo al análisis de riesgos. La segunda únicamente señala que se analicen los riesgos asociados a la prestación de servicios TI de forma genérica, mientras que la ISO 27001 define con mayor profundidad los requisitos y condiciones que debe cumplir dicho análisis. Además, la ISO 27001 es más extensa a la hora de definir el modo en el que debe desarrollarse la gestión de los riesgos, llegando a proponer una serie de controles (el conocido Anexo A) que deben implementarse para garantizar un nivel de seguridad adecuado dentro del alcance en el que nos encontramos, los sistemas de información.

Uno de los aspectos en los que ISO 27001 e ISO 20000 son bastante similares es en lo relativo a la gestión de incidentes. Ambas normas llevan a cabo un importante esfuerzo a la hora de definir una metodología de gestión de incidentes, que contemple no sólo las propias incidencias sino también los problemas. En ambos casos se contemplan los incidentes dentro del sistema de gestión, y se especifican en mayor o menor medida tanto las estructuras organizativas que deben garantizar esta gestión como los pasos que se deben seguir para llevar a cabo esta gestión de forma correcta y los resultados mínimos que deben obtenerse.

Por último, otro de los elementos más destacables respecto a las coincidencias entre ambas normas es el relativo a la planificación de la capacidad. En este caso, la ISO 20000 vuelve a ser más exhaustiva a la hora de definir requisitos, ya que define un proceso completo cuyo objetivo principal es garantizar la suficiente capacidad de los sistemas para prestar los servicios, pero la ISO 27001 también hace referencia a este hecho al definir un control específico a tal efecto, que exige que se garantice el rendimiento futuro de los sistemas a través de monitorizaciones y proyecciones que permitan predecir dichas necesidades. Por tanto, una adecuada gestión de la capacidad de los sistemas va a permitir el cumplimiento simultáneo de ambas normas, en lo que a este respecto se refiere.

Se podría seguir enumerando, a más bajo nivel, otra serie de aspectos en los que la implementación de los tres sistemas de gestión presenta coincidencias. Tanto la ISO 20000 como la ISO 27001 e ISO 9001 proponen sistemas de gestión que, aunque con objetivos

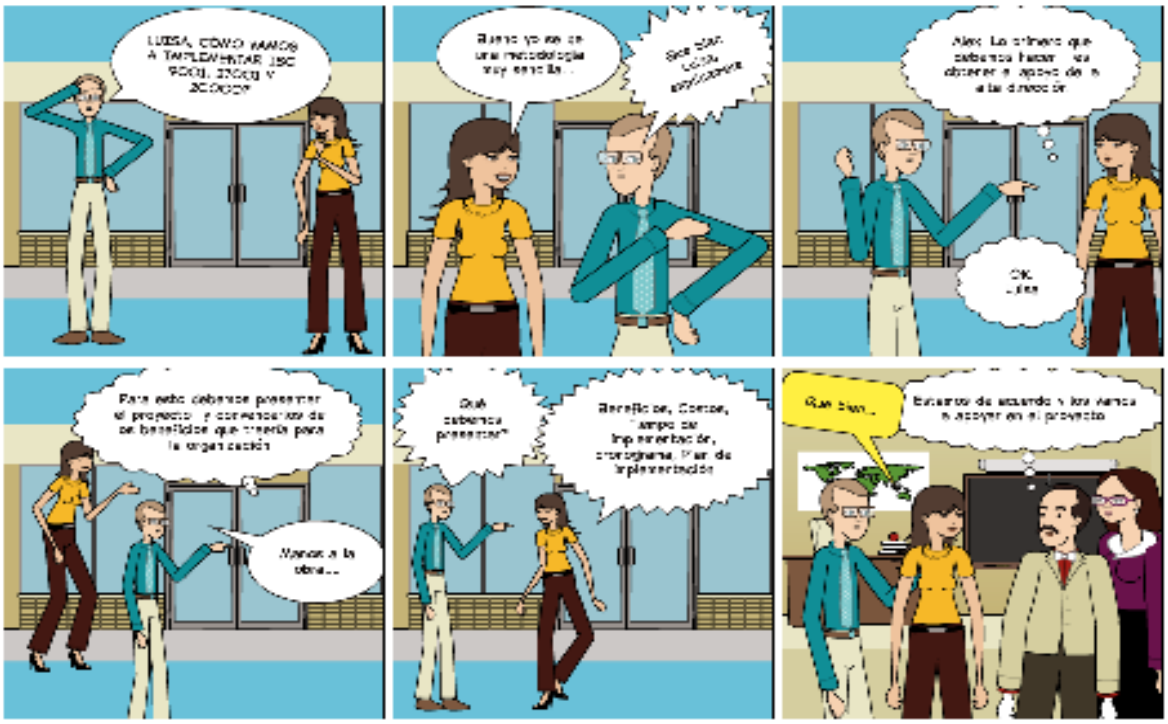
distintos, exigen la implementación de medidas coincidentes, en muchos casos. La implementación integrada nos va a permitir el desarrollo de un único sistema de gestión integral que cumpla simultáneamente con los requisitos de los tres estándares.

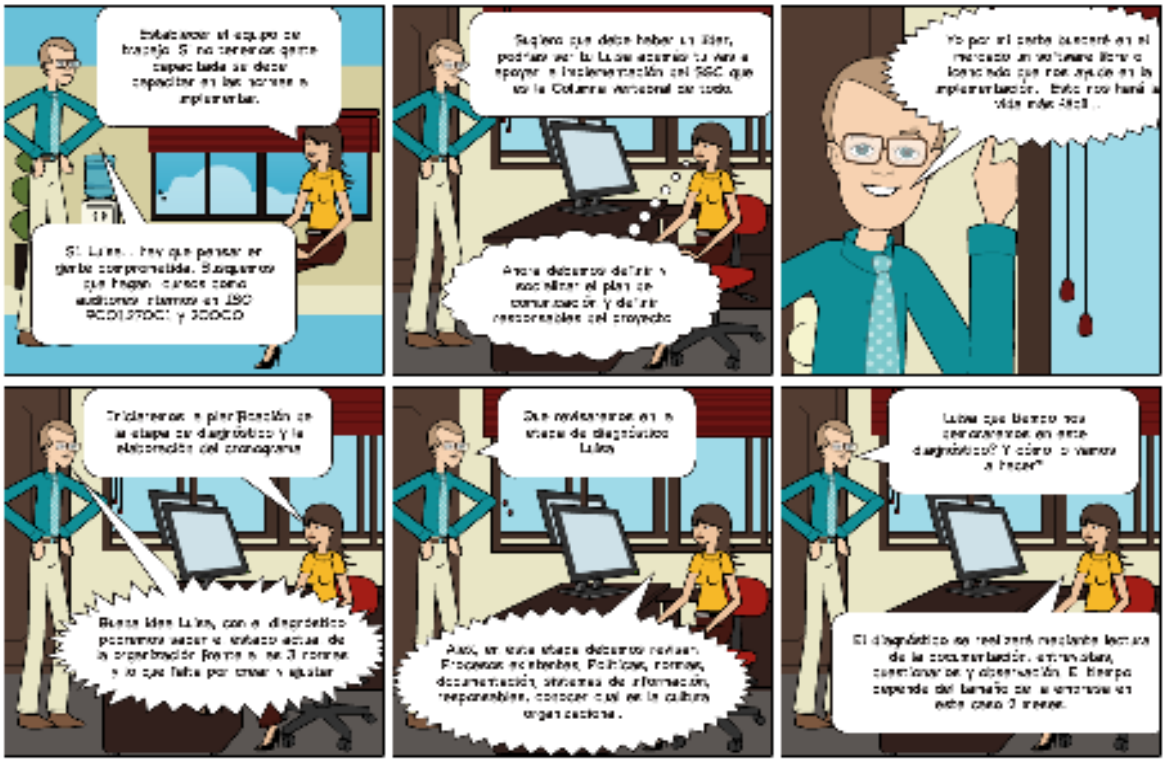
Este hecho, además de aportar todas las ventajas que supone la adopción de un único sistema de gestión, nos va a permitir desarrollar una infraestructura de gestión técnica que garantice de forma global, tanto a nivel de prestación de servicios como de seguridad de todos sus elementos, la necesaria calidad de las actividades desarrolladas en este entorno. Esta triple certificación se puede logar gracias al cumplimiento de estándares internacionalmente reconocidos, una infraestructura de gestión que permita garantizar la óptima adecuación del núcleo tecnológico de nuestras organizaciones a las exigencias y requisitos, tanto propios como de nuestros clientes con el fin de ofrecer unos servicios seguros y de óptima calidad.

6. METODOLOGIA

Se sabe que hablar de implementación y certificación de normas se torna un tema aburrido y difícil, el aporte expuesto en este trabajo es plantear una metodología de manera creativa con la utilización de comics, para ayudar a las organizaciones a implementar sistemas de gestión integrados. En este caso puntual hablamos de 3 referentes ISO 9001, ISO 27001 e ISO 20000. En esta historieta contextualizamos los pasos a seguir en un ejercicio real de implementación de un sistema de gestión integral. El referente principal es la norma ISO 9001 la cual es la columna vertebral para realizar la implementación de las otras dos normas.

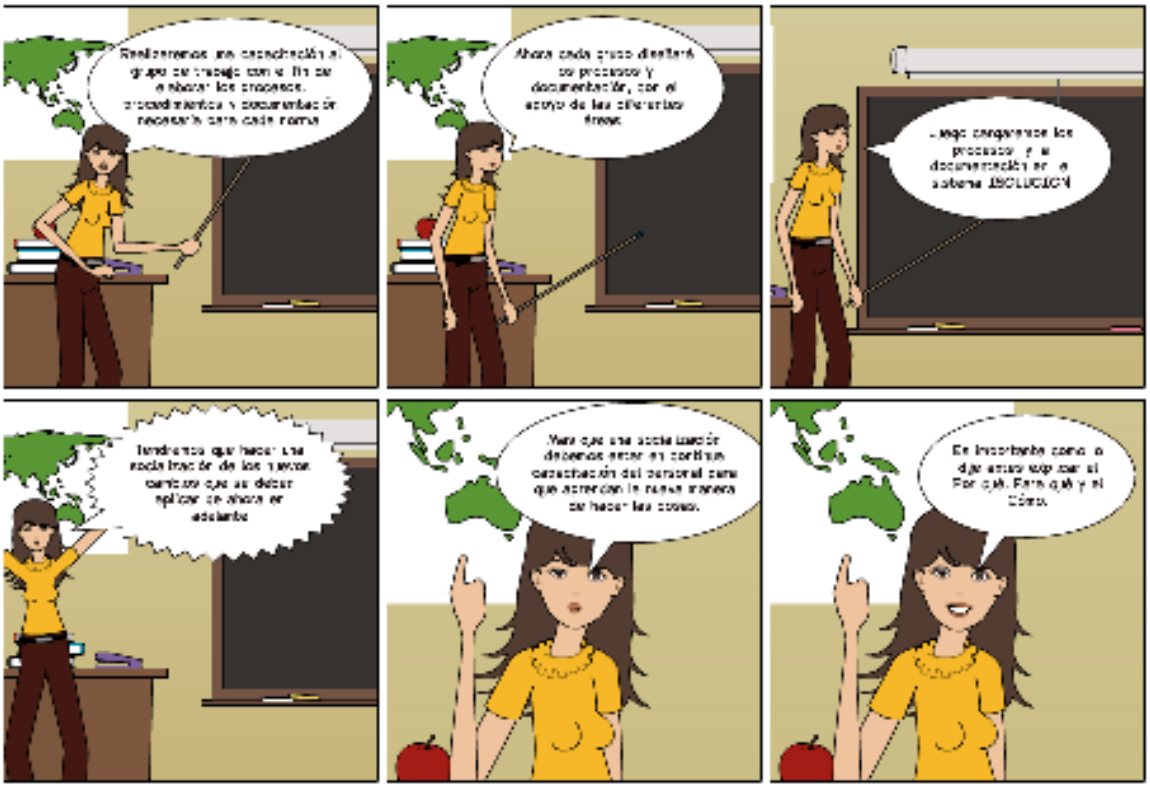
Grafica 3. Comics metodología para la implantación de un sistema integrado.



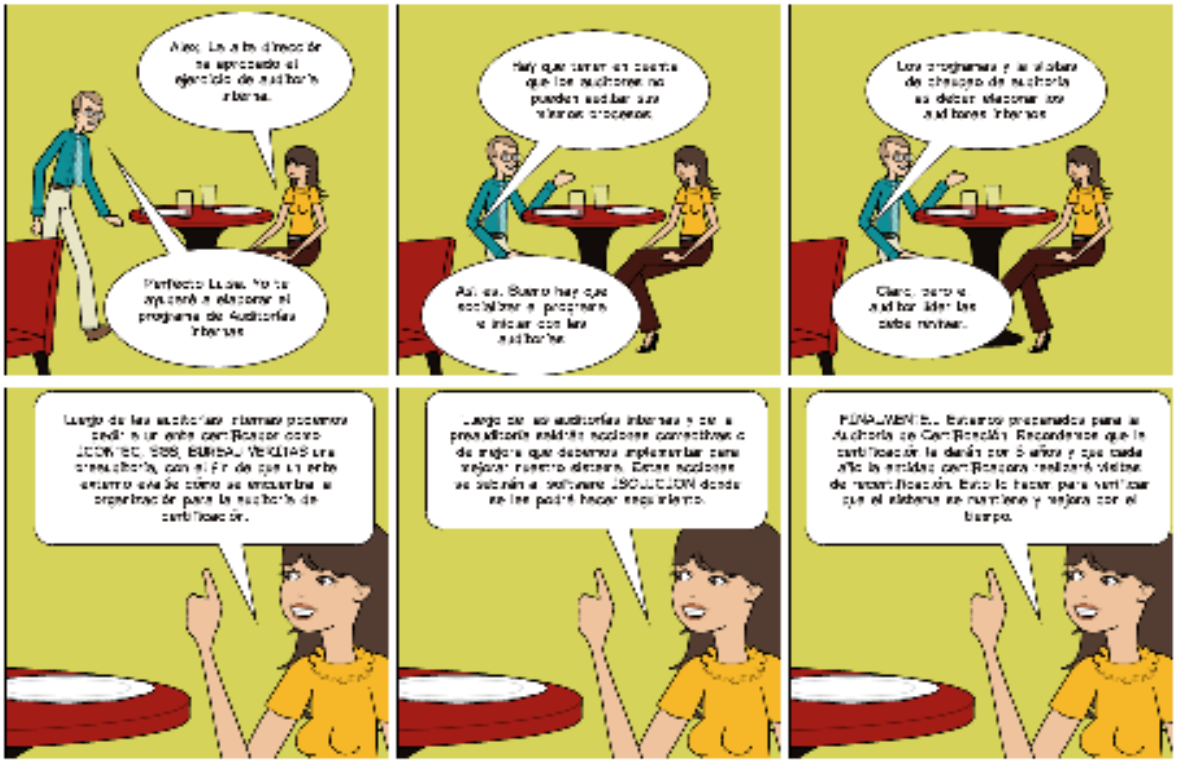

Estableceremos el equipo de trabajo. Si no tenemos gente capacitada se debe capacitar en las normas a implementar.
Si Lucía... hay que pensar en gente comprometida. Busquemos que tengan cursos como auditores internos en ISO 9001:2008 y 22000.
Sugiero que debe haber un líder, podrías ser tú Lucía además tu vas a apoyar a implementación del SGC que es la Columna vertebral de todo.
Ahora debemos definir y socializar el plan de comunicación y definir responsables del proyecto
Yo por mi parte buscaré en el mercado un software libre o licenciado que nos ayude en la implementación. Esto nos hará a más rápidos.
Tuvimos a pier[illegible]ción de la etapa de diagnóstico y la elaboración del cronograma
Buena idea Lucía, con el diagnóstico podremos saber el estado actual de la organización [illegible] las 3 normas y lo que falta por crear y ajustar
Que realizamos en la etapa de diagnóstico Lucía
Así, en esta etapa debemos revisar: Procesos existentes, Políticas, normas, documentación, sistemas de información, responsables, conocer cual es la cultura organizacional.
Lucía que hemos realizado en esta diagnóstico? Y cómo lo vamos a hacer?
El diagnóstico se realizará mediante lectura de la documentación, entrevistas, cuestionarios y observación. El tiempo depende del tamaño de la empresa en este caso 2 meses.


Teniendo el diagnóstico de la situación actual nos servirá para elaborar el plan de implementación
El resultado del diagnóstico debe ser presentado a la alta dirección.
La primera etapa será la de planeación del sistema integrado
Definiremos el alcance del sistema
Definiremos los objetivos
Definiremos el grupo de trabajo.
Definiremos el plan de comunicaciones para la implementación
Definiremos el cronograma o plan de trabajo
Uno de los errores mas comunes es no decirle a las personas Qué se va a hacer, Porqué, Para qué y Cómo se va a realizar el proyecto
Así que haremos una sensibilización con todo el personal de la organización de forma participativa y creativa, empezaremos a cambiar la cultura organizacional
Alex. Cómo te fue con la investigación del software que nos ayudará a la implementación?
Listo ya hice el estudio y el mas completo que me parecio se llama ISOLUCION, creo es el que vamos a adquirir, el contrato va este listo.
Bien. Vamos a realizar una sesión de trabajo con el equipo donde miraremos las semejanzas dentro de las 3 normas y la forma de implementarlas lo mas sencillo que podamos.
Perfecto. El software nos apoyará en implementar las tres normas.
Las 3 normas tienen requisitos obligatorios y algunos son los mismos.
1. Control de documentos
2. Control de Registros
3. Auditorías Internas
4. Producto no conforme
5. Acciones Correctivas
6. Acciones Preventivas


Es decir que ambos procesos nos servirán para las 3 normas?
Así es Alex. Yo diría que realizarlos juntos. De esta manera no hay que duplicar procesos ni documentación.
Claro, pero también hay unos requisitos propios de la norma ISO 20000 o ISO 27001 que los podemos usar para las dos normas.
Casi es así. Luis?
Alex, son algunos: Gestión de proveedores Gestión del Cambio Continuidad de negocio Gestión de riesgos Gestión de Incidentes Gestión de la Capacidad Gestión de problemas Gestión de la configuración Gestión de la seguridad
Teniendo esta claridad Alex. La siguiente etapa es la etapa de desarrollo o ejecución
Cómo lo vamos a hacer?
Cada grupo de trabajo establecido, deberá evaluar la situación actual y determinar qué le falta a la organización para que sus prácticas de trabajo estén conformes a cada norma. ISO 9001, 20000 y 27001.
Luego de esto qué debe hacer?
Luego nos vamos a capacitación en el manejo del software ISOLUCION, con el fin de elaborar los procesos
De acuerdo Luis, yo coordinaré la capacitación


Realizaremos una capacitación al grupo de trabajo con el fin de elaborar los procesos, procedimientos y documentación necesaria para cada norma
Ahora cada grupo diseñará su procesos y documentación, con el apoyo de las diferentes áreas
Luego cargaremos los procesos y la documentación en el sistema ISOLUCION
Tendremos que hacer una socialización de los nuevos cambios que se deben aplicar de ahora en adelante
Para que esta socialización debemos iniciar en cortísima capacitación del personal para que aprendan la nueva manera de hacer las cosas.
Es importante como lo dije antes explicar el Por qué, Para qué y el Cómo.


Ahora tenemos que dedicarnos a realizar ajustes. Diseñar los indicadores que nos permitan verificar si los sistemas implementados son eficaces y efectivos
PHVA
De acuerdo Alex. Lo que no se mide no se puede controlar y lo que no se puede controlar no se puede mejorar.
Hemos logrado un trabajo muy importante. Pienso que es hora de hacer el ejercicio de auditoría interna, qué dices?
Felicitaciones vemos que han realizado un buen trabajo. Hagan lo que tengan que hacer. Buscamos buscar la certificación.
Alta Dirección
Estoy de acuerdo Alex. Vamos a realizar el plan de auditoría y a coordinar el grupo de auditores que ya fueron formados. Pero primero debemos contar con la alta dirección para contar el aval. Voy corriendo a hablar con ellos..


Alex, La alta dirección ha aprobado el ejercicio de auditoría interna.
Perfecto Luisa. Ya te ayudaré a elaborar el programa de Auditorías Internas
Hay que tener en cuenta que los auditores no pueden auditar sus propios procesos
Así es. Bueno hay que socializar el programa e iniciar con las auditorías.
Los programas y el plan de trabajo de auditoría se deben elaborar por auditores internos
Claro, pero el auditor líder los debe revisar.
Luego de las auditorías internas procederá realizar la auditoría de certificación por parte de ICONTEC, BUREAU VERITAS o alguna otra entidad, con el fin de que la alta dirección sepa cómo se encuentra la organización para la auditoría de certificación.
Luego de las auditorías internas y de la preauditoría existirán acciones correctivas o de mejora que deberán implementar para mejorar nuestro sistema. Estas acciones se subirán al software ISOLUCION donde se les podrá hacer seguimiento.
FINALMENTE... Estamos preparados para la Auditoría de Certificación. Recuerden que la certificación la dará por 3 años y que cada año la entidad certificadora realizará visitas de recertificación. Esto lo hacen para verificar que el sistema se mantiene y mejora con el tiempo.

La metodología propuesta para la verificación de las similitudes entre los requisitos entre las normas ISO 9001, ISO 20000 e ISO 27001, se compone de 4 fases, las cuales están descritas y explicadas en detalle una a una en las siguientes secciones del informe:

6.1. ETAPA DE DIAGNÓSTICO

- 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, este punto es clave y es el primer paso que se debe tener en nuestra lista de actividades dentro de la metodología propuesta.
- El segundo paso tiene que ver con la definición del alcance, el cual debe describir los procesos y el cubrimiento geográfico que tendrá la etapa de diagnóstico.
- 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
- El sexto paso es la ejecución de las actividades descritas en el cronograma.

En la etapa de diagnóstico se realiza un levantamiento de información de la organización con el fin de conocer la cultura organizacional; esto se realiza mediante las siguientes técnicas:

a) Lectura de la documentación existente (misión, visión, objetivos organizacionales, planeación estratégica, políticas, procesos, procedimientos, instructivos, manuales, normatividad entre otros).
b) Entrevistas a los líderes de proceso para conocer el clima organizacional y el estilo de liderazgo de la organización y de cada proceso.
c) Entrevistas a los líderes de proceso, mediante cuestionarios a los colaboradores de todos los niveles con el fin de conocer el grado de difusión del sistema de calidad y el nivel de empoderamiento de cada cargo.
d) Observación de procesos con el fin de hacer un diagnostico organizacional del funcionamiento transversal de la estructura del mapa de procesos.
e) Se continúa con el seguimiento a las actividades del cronograma.
f) Y se termina con un informe final de diagnóstico donde se determina con que documentación y procesos cuenta la organización y que hace falta para llegar a implementar las 3 normas que se desea, dando inicio a la siguiente etapa de planeación.

6.2. ETAPA DE PLANEACION

Una vez el grupo directivo de la entidad establezca dentro de sus propósitos el desarrollo de una metodología para la implementación simultanea de las normas ISO 9001, 20000 y 27001, es necesario que se conforme un grupo de trabajo, cuya responsabilidad sea liderar y poner en marcha este proceso.

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.

- Grupos de trabajo

Los empleados que hagan parte de los grupos de trabajo se deben caracterizar por un gran conocimiento de la organización, del proceso donde se desempeñan y del área donde trabajan. Deben ser personas visionarias, lideres con capacidad de hacer las cosas bien y de inspirar a los demás integrantes de la organización para el logro de los objetivos y metas propuestas en el diseño de esta metodología para la evaluación del sistema documental. La selección de este personal debe ser cuidadosa y deben recibir capacitación y asistencia técnica en los temas que van a trabajar y en la forma de realizar tareas.

Adicionalmente, los grupos de trabajo deben tener claro su propósito y este debe ser común entre todos los integrantes, cada grupo de trabajo debe tener autonomía para poder solucionar sus problemas y tomar decisiones claves para el logro de los objetivos y tener claras las metas para cada periodo de tiempo.

El éxito de estos grupos de trabajo depende de los miembros que lo conforman, de la armonía que se logre entre los integrantes y del apoyo que brinde la alta dirección.

- Plan de trabajo

Al desarrollar el plan de trabajo para desarrollar esta metodología, es importante que:

a) Se identifiquen las tareas necesarias por realizar.
b) Se especifique un plazo para completar cada tarea.
c) Se indiquen claramente las relaciones de interdependencia entre las tareas establecidas.
d) Se designen personas o equipos específicos para llevar a cabo cada tarea.

- Asignación de responsabilidades

Uno de los mayores problemas en el desarrollo de cualquier metodología, es la asignación de responsabilidades, que con frecuencia se asigna en un nivel en donde no se pueden llevar a cabo.

Una clara asignación de actividades permitirá un monitoreo efectivo del desempeño de los equipos de trabajo, es importante que las personas a las que se les asigne una responsabilidad estén plenamente conscientes de ella y de cómo se relaciona con otras actividades.

- Cronograma de actividades

Una vez establecidas las actividades claves y los responsables. El grupo de trabajo elabora un cronograma, donde se debe relacionar cada una de las actividades, teniendo en cuenta el orden de ejecución, fechas de inicio, y finalización, y el responsable de cada tarea. Adicionalmente es recomendable que a su vez, para cada uno de los responsables sea elaborado un cronograma individual, que indique las actividades que están a su cargo.

- Definición de recursos:

Toda metodología requiere para su realización una serie de recursos, los cuales se clasifican en 4 tipos:

a) Humanos: como se menciono en los puntos anteriores, la selección de los grupos de trabajo es un punto clave, ya que este recurso con sus competencias, permitirá el logro de los objetivos propuestos de el desarrollo de la metodología.
b) Físicos: comprenden varios aspectos como infraestructura, maquinaria, equipos y documentos.
c) Técnicos: se deben definir qué tipo de insumos técnicos se van a necesitar para el desarrollo de la metodología, en este caso sería necesario contar con las normas ISO 9001, 20000 y 27001.

d) Financieros: se hace referencia al presupuesto necesario para el desarrollo del proyecto.

- Capacitación del grupo de trabajo directivo y técnico

En este momento ya deben estar definidos los objetivos, las actividades, responsables y recursos necesarios para el desarrollo de la metodología, y el grupo directivo debe definir las necesidades de capacitación para poder cumplir con los objetivos propuestos, esta capacitación debe ser impartida a todos los niveles de la organización y dar a conocer los objetivos, justificación y acciones necesarias para poner en marcha el proyecto con las normas ISO 9001, ISO 20000 e ISO 27001.

Familiarice a sus empleados con los documentos pertinentes: Lo primero que el personal de la organización debe hacer es conocer y entender lo mejor posible todos los aspectos que hay detrás de los estándares ISO 9001, 20000 y 27001. ¿Cuáles son sus beneficios?, ¿Cuáles son sus costos?, fundamentos, entre otros.

6.3. ETAPA DE DESARROLLO

Evalúe la situación actual. El personal debe evaluar la situación actual y determinar qué le falta a la organización para que sus prácticas de trabajo estén conformes a ISO 9001, 20000 y 27001.

Todo sistema de gestión tiene sus soportes en el sistema documental, ya que este tiene una importancia vital en el logro de la calidad.

La mayoría de las normas ISO dan la posibilidad de aplicar el sentido común y decidir de acuerdo a las características de la organización en cuanto a tamaño, tipo de actividad que realiza complejidad de los procesos y sus interacciones, y la competencia del personal, la extensión de la documentación del sistema de gestión de la calidad. No obstante, la mayoría de normas exigen la existencia de los siguientes documentos:

- Declaraciones documentadas de una política de calidad.
- Objetivos de la calidad.
- Manual de Calidad.
- Control de documentos.
- Control de los registros de calidad.
- Auditorías internas.
- Control de productos no conformes.

- Acciones correctivas.
- Acciones preventivas.
- Los documentos requeridos por la organización para asegurar el control, funcionamiento y planificación efectivos de sus procesos.
- Revisiones efectuadas por la dirección al sistema de gestión de la calidad.
- Educación, formación, habilidades y experiencia del personal.
- Procesos de realización del producto y cumplimiento de los requisitos del producto.
- Revisión de los requisitos relacionados con el producto.
- Elementos de entrada del diseño y desarrollo.
- Resultados de la verificación del diseño y desarrollo.
- Resultados de la validación del diseño y desarrollo.
- Control de cambios del diseño y desarrollo.
- Evaluación de proveedores.
- Control de los equipos de medición y seguimiento cuando no existen patrones nacionales o internacionales.
- Resultados de la verificación y calibración de los instrumentos de medición.
- Auditorías internas.
- Autoridad responsable de la puesta en uso del producto.

- Tratamiento de las no conformidades.

Una vez se listen los documentos pertinentes a la organización, se debe realizar un diagnóstico de la situación de la documentación, comparando lo que existe con las necesidades determinadas en la etapa anterior, generando un informe donde se listen los documentos existentes por proceso, su adecuación a las normas según los requisitos, y si es un documento único o si la información contenida esta duplicada o triplicada en documentos similares. El resultado de este diagnóstico nos debe arrojar datos como:

a) El número de documentos con los que cuenta la organización.
b) La información contenida en cada documento
c) Información duplicada.
d) Información omitida.
e) Información obsoleta.

El paso a seguir es realizar el procesamiento y análisis de la información recolectada. Se deben definir que documentación es útil para el propósito de las certificaciones, eliminar los que estén duplicados y actualizar los que estén desactualizados o ayuden al cumplimiento de los requisitos de las normas.

Es importante presentar un informe de resultados y avances de la revisión documental a la alta gerencia, con el fin de hacer este proceso de certificación una actividad transversal, en la que cada miembro de la organización esté involucrado e informado de los avances y cambios que se van a ir dando dentro de la cultura y el manejo de la información dentro de la organización. Una

vez que la alta gerencia de sus observaciones y el visto bueno, se debe iniciar la etapa de implementación.

6.4. ETAPA DE IMPLANTACION Y PUESTA EN MARCHA DE LA IMPLEMENTACION

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.

Se recomienda la utilización de un software de apoyo para el manejo de la documentación, los cuales son de fácil aplicación y en algunos casos de acceso libre. (Vea numeral 5 Software de acceso libre).

Una vez implantados los procesos requeridos en los requisitos de las normas, se debe implantar un programa de auditoría interna del sistema documental, con base a los requisitos de la documentación de las normas ISO 9001, 20000 y 27001.

Previamente se deben haber formado a los colaboradores como auditores internos de cada norma, con el fin de instaurar un grupo de auditores multidisciplinario, capaz de detectar incumplimientos de los requisitos de cualquiera de las normas a certificar. Cabe recordar que la gestión documental será el soporte principal de nuestro sistema de gestión integrado ISO 9001, 20000 y 27001, ya que es la base y el soporte del propio sistema, es importante que los requisitos y el contenido de la documentación del sistema integrado se orienten de acuerdo con los requisitos de calidad de las normas que se pretenden certificar.

Con base a los resultados del programa de auditoría se deben iniciar ciclos de mejora continua hasta alcanzar la adecuación completa de la documentación necesaria, usar la información obtenida en las auditorias para identificar las áreas que tengan más potencial para mejorar, realizar ciclos PHVA en cada proceso con el fin de establecer una cultura de mejora continua.

Es importante que todo el personal de la organización tenga en mente que trabajar con este sistema integrado ISO 9001, 20000 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 lograr la certificación.

Una vez implantado el sistema de gestión integrado, la organización puede escalar a la fase de auditoría y certificación, la cual generalmente se lleva a cabo de la siguiente manera:

a) Solicitud de la auditoria por parte de la organización.

b) Respuesta y compromiso de la organización.

c) Designación de auditores, determinación de fechas y desarrollo del plan de auditoría.

d) Programación de una pre auditoria: Una vez han culminado varios ciclos de mejora continua, es recomendable que la organización se enfrente a una pre auditoria por parte de alguno de los organismos certificadores como Icontec, CGC o Bureau Veritas; aunque esta auditoría no es obligatoria, el informe de los hallazgos de esta es muy importante para el proceso de mejora continua dentro de la organización y para garantizar el cumplimiento de los requisitos requeridos para la auditoria de certificación.

e) Fase 1 de la auditoria de certificación: donde se revisa el sistema documental del SGSI, y del SGC.

f) Fase 2 de la auditoria: es la fase en la que se revisan las políticas, implantación de controles de seguridad y eficacia del sistema integrado y se evalúan los hallazgos de

la fase 1, si se descubren no conformidades graves, se deben implementar acciones correctivas para corregir la causa y el origen de los incumplimientos a las normas.

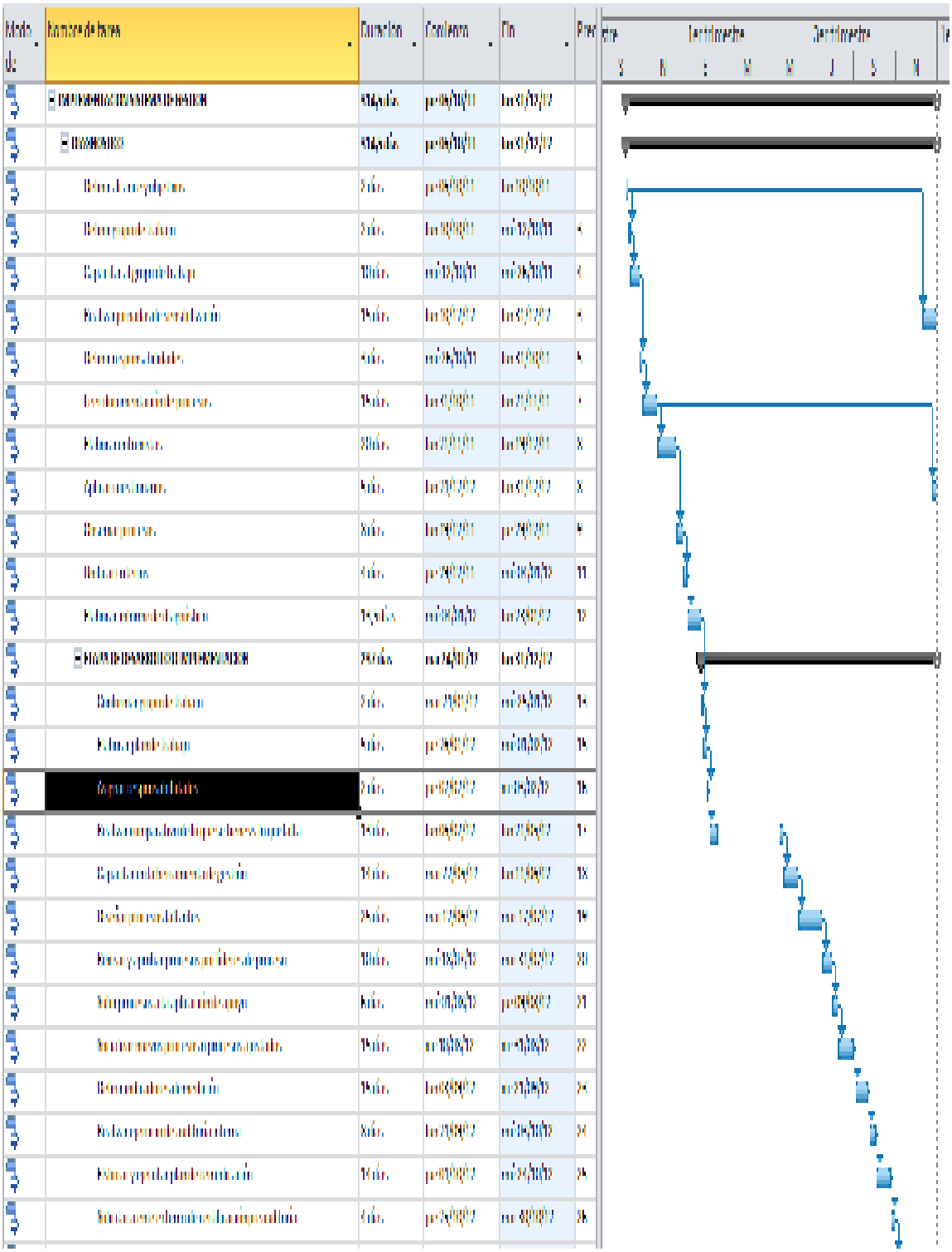
g) Certificación: en caso de cumplir con los requisitos, el auditor dará un concepto favorable y la organización será certificada.

h) Auditoría de seguimiento: cada seis meses o un año se debe realizar una auditoría interna de mantenimiento, con el fin de garantizar el correcto funcionamiento del sistema certificado, fomentar y verificar que la mejora continua del sistema se esté llevando a cabo dentro de la organización.

i) Auditoría de re certificación: es necesario que cada tres años se supere una auditoría de certificación completa como la descrita anteriormente.

Para llevar a cabo esta metodología, se ha diseñado un cronograma de tareas, cuyo tiempo estimado de ejecución es de 10 meses 3 días. Este cronograma es solo una sugerencia dentro del trabajo de investigación, ya que el tiempo, y los avances que se presenten en la implementación de un sistema integrado de gestión con las normas ISO 9001, 20000 y 27001, deberán depender del tipo de organización que se pretenda certificar, su tamaño y tipo de estructura de trabajo que quiera adoptar.

Grafica 4. Cronograma de actividades



6.5. SOFTWARE DE APOYO A LA IMPLEMENTACION DE SISTEMAS DE GESTION

6.5.1. SOFTWARE LIBRE

El OpenKM: es una aplicación mediante la cual las empresas podrán tener un control sobre toda la documentación digital que se genere en el proceso de implementación. Las últimas tecnologías han hecho que la gran mayoría de las comunicaciones se realicen mediante esta vía y, como en las empresas, hay muchos trabajadores, a menudo es imposible gestionar toda la documentación. Para ello, esta aplicación obtendrá todas las comunicaciones que se hagan y las clasificará y almacenará por si se requiere de una posterior revisión. Además, actúa como sistema de seguridad, ya que aunque se borren algunas de estas comunicaciones de los ordenadores, esta aplicación mantendrá una copia en su sistema. Esta aplicación tiene características tan importantes como la capacidad de arrastrar y soltar, control de versiones, motor de búsqueda para que podemos encontrar lo que estamos buscando, integración LDAP o DBMS, API para su utilización en webservices de empresas de gran tamaño, almacenamiento en DBMS y Workflow.

KMKey Quality: es el software de gestión de calidad (SGC) ideal para la implantación y la gestión de la calidad en su empresa u organización. Mediante su uso sencillo e intuitivo, su acceso universal, y su entorno colaborativo, hará más fácil la tarea de gestionar la calidad de una forma eficiente. Las funcionalidades de esta herramienta se describen a continuación:

- Organización: Permite definir la organización indicando qué personas están dentro del SGC y los cargos que ocupan dentro de la institución.

- Gestión de la documentación: Permite conocer los documentos del SGC en vigor, el histórico de los mismos y su distribución dejando registro de la misma. Además el gestor de expedientes le permitirá la elaboración colaborativa de documentos, gestionando la edición, la revisión y la aprobación de los mismos, integrando además un sistema de notificaciones digitales por e-mail que facilita la comunicación a los diferentes usuarios.

- Objetivos: Permite conocer los objetivos de la organización aprobados y dejar registro del seguimiento de los mismos.

- Indicadores: Permite conocer los indicadores definidos para los procesos de la organización y dejar registro del seguimiento de los mismos.

- Revisiones por la dirección: permite enviar las convocatorias, registrar los resultados de las mismas y realizar el seguimiento de los acuerdos tomados.

- No conformidades: Permite registrar y realizar el tratamiento, seguimiento y cierre de las no conformidades
- 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.

- Acciones de mejora: Permite registrar y realizar el tratamiento de las acciones de mejora recibidas, así como el seguimiento y cierre de las aprobadas.

- Auditorias: Generar planes de auditoría. Lanzar programación de las auditorías. Gestionar y controlar su realización. Relacionar con las No Conformidades que se detecten.

- Calibraciones: permite registrar las acciones efectuadas para verificar el correcto funcionamiento de los diferentes aparatos de medida. Permite planificar, registrar y consultar las diferentes calibraciones.

- Seguimiento satisfacción del cliente: permite generar y lanzar encuestas a una lista de personas para evaluar cualquier acontecimiento. En concreto, se puede lanzar una encuesta para evaluar la satisfacción de los clientes sobre un producto y servicio. Se pueden generar estadísticas de forma automática.

- Satisfacción de los usuarios de los servicios: permite acceder a los registros de las mediciones de la satisfacción de los usuarios de los servicios y seguir su evolución, así como realizar el seguimiento de las acciones definidas en función del análisis de los resultados obtenidos.

- Reclamaciones: Permite registrar y realizar el tratamiento, seguimiento y cierre de las reclamaciones y quejas recibidas.

6.5.2. SOFTWARE LICENCIADO

EGAM

Es un software web de origen español, tiene como ventajas:

- Autogenerar evidencias y registros
- Ejecutar automáticamente procedimientos
- Delegar automáticamente tareas, instrucciones y plazos
- Supervisar en tiempo real tareas y responsables
- Gestionar en tiempo real requisitos de certificación y auditoría
- Eliminar no conformidades a causa de despistes
- Eliminar toda la documentación en papel
- Integrado con Microsoft Outlook
- Configurable 100% a la medida de sus propios procesos
- Plataforma tecnológica BPM (Business Process Management)
- Comercializado mediante modelo de "pago por uso" (SaaS)
- Apoyado sobre comunidad abierta de documentación y conocimiento.

ITS GESTION

Es software colombiano para la implementación de sistemas de gestión. A continuación se describen los módulos de esta aplicación.

- Administración Documental
- Auditorías Internas y de Calidad
- Acciones de mejora
- Producto no conforme
- Indicadores
- Proveedores
- Administración de riesgos
- PQR
- Revisión por la dirección
- Encuestas
- Evaluación por competencias
- Actas y seguimiento de tareas
- Planes y proyectos
- MECI

ISO TOOLS

Es una Plataforma 100% Web altamente personalizable con la que puede integrar fácilmente sus Sistemas de Gestión ISO y OHSAS, así como Normas específicas según su país.

La Plataforma Online ISOTools se basa en la idea de Cloud Computing, es decir, para usar esta potente aplicación, el cliente no necesita de centros de datos, energía, refrigeración, ancho de banda, servidores, redes, software complejo, espacio, y expertos que instalen, configuren y ejecuten la aplicación. Cloud Computing es una manera más cómoda y rentable de explotar su negocio.

En vez de ejecutar ISOTools usted mismo, la aplicación se ejecuta en un centro de datos compartido, que dispone de todas las medidas de seguridad necesarias y de un servicio técnico 24horas.

Para utilizar ISOTools en la nube, sólo hay que iniciar sesión y empezar a trabajar. La Plataforma Online ISOTools sólo requiere de un paso previo para personalizar su entorno y configurar los usuarios que podrán acceder a ella. En pocos días usted tiene a disposición una herramienta de gestión ISO lista para rentabilizar su negocio, sin necesidad de pagar a una plantilla de expertos en sistemas software, instalaciones, seguridad, hardware y personal de apoyo. El Cloud Computing de ISOTools soporta actualizaciones automáticas, y puede ampliarse de forma más segura y fiable.

El método de pago de ISOTools con base de Cloud Computing posee grandes ventajas. Cuando ISOTools se ejecuta en la nube, no tiene que comprar servidores ni software, todo se incluye en una suscripción mensual predecible, de modo que sólo paga por lo que realmente utiliza y cuando lo utiliza. ISOTools se adquiere en modalidad SaaS (Software como un Servicio) es el modelo de distribución de software basado en Cloud Computing, el cual se presenta como

un servicio alojado y accedido a través de Internet, con soporte de ASP (Application Service Provider).

ISOLUTION

Es una empresa Colombiana con presencia a nivel latinoamericano que ofrece un software de gestión integral para normas ISO, totalmente parametrizable a las necesidades de la organización, se puede adquirir mediante suscripción, es decir con solo una cuenta de usuario y clave la compañía podría iniciar a utilizarlo sin necesidad de adquirir infraestructura de hardware. Este software de apoyo se compone de los siguientes módulos:

- Gestión Documental
- Sistema de Mejora
- Indicadores
- Planeación Estratégica
- MECI
- Riesgos
- S&SO y Ambiental
- Proveedores
- Talento Humano
- Calibración de equipos
- Tareas Pendientes
- Divulgación y Comunicación
- Clientes

7. CONCLUSIONES Y FACTORES CRITICOS DE ÉXITO.

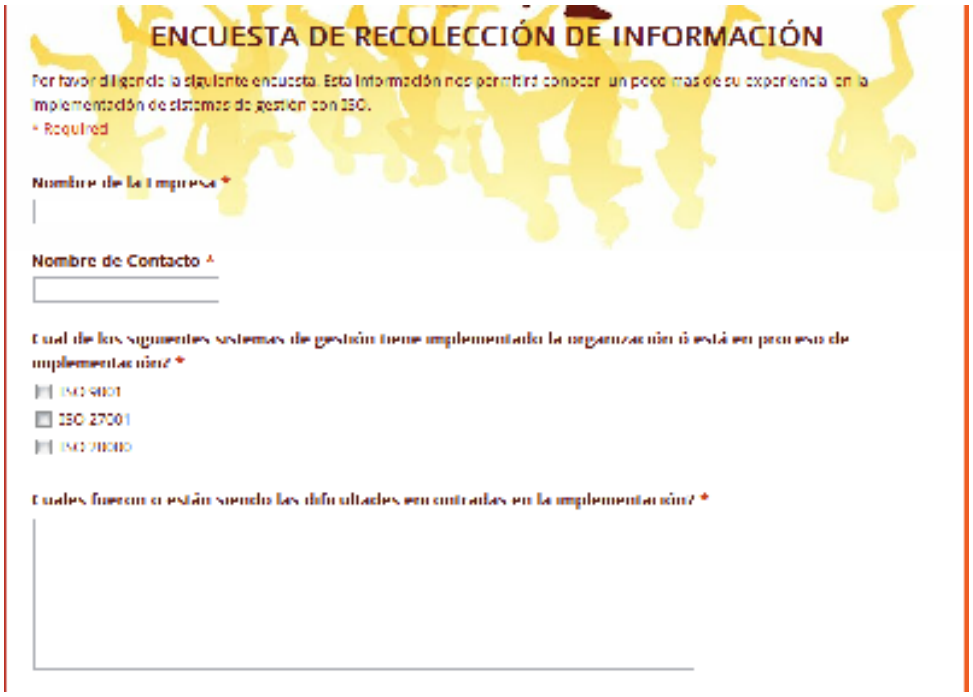
"La concienciación del empleado. Principal objetivo a conseguir."

Para hablar de factores críticos de éxito en la implementación de un sistema integrado de gestión, hemos ideado una metodología basada en la evidencia.

7.1. ENCUESTA FACTORES CRITICOS DE ÉXITO

Se diseñó una encuesta cuyo fin es de obtener información de algunas empresas que ya han pasado o están actualmente pasando por el proceso de implementación de los referentes estudiados en este trabajo ISO 9001, ISO 20000 o ISO 27001, para extraer de las experiencias reales, información valiosa sobre los factores críticos de éxito que estas empresas aplicaron y que definitivamente fueron la clave de su certificación.

Grafica 5. Encuesta factores críticos de éxito.



Cuales han sido los beneficios que la organización obtuvo o piensa que puede obtener con la implementación de esta (s) norma (s)? *

Cuales fueron o cuales son los puntos claves de éxito identificados dentro de la implementación del proyecto? *

Cuanto tiempo duró o estima dure la implementación? *

- 3 Meses
- 6 Meses
- 12 meses
- 24 meses

Cuantas personas participaron o están participando en la implementación? *

- 1-3
- 3-6
- 6 - 12
- 12 - 24
- Mas de 24

Se utilizó o se piensa utilizar algún tipo de software para la implementación? *

- Si
- No

Cual?

Considera que implementar estas 3 normas al tiempo puede tener algunas ventajas? *

- Si
- No

Puede mencionar algunas?

Submit

Se aplico la encuesta a 5 diferentes personas que han participado o están participando en proceso de implementación de los referentes de ISO tratados a lo largo de este trabajo, observando los siguientes factores clave en el momento de la implementación:

a) En todos los casos se evidencio que el equipo encargado de la implementación debe ser un equipo multidisciplinario, no menos de 5 personas participan en el proceso.
b) El tiempo promedio para la implementación de alguna de las normas por las que se indago en la encuesta en ningún caso fue menos de 6 meses.
c) Definitivamente, uno de los factores claves para el éxito del proceso de implementación es el compromiso de la alta dirección, y la asignación de recursos suficientes para llevar a cabo todas las tareas.
d) Los altos directivos aún sub estiman la fuerza que puede alcanzar un equipo motivado y empoderado, esa es una de las dificultades nombrada por nuestros encuestados, ya que en ocasiones no se motiva ni capacita al personal de la empresa y se toman las certificaciones como cuestiones simplemente asuntos documentales.
e) Uno de los beneficios más importantes de la implementación ISO 20000 y 27001, y respuesta común entre todos los encuestados, es el aumento de la confiabilidad del cliente y mejora de la imagen corporativa.

Grafica 6. Dificultades en la implementación de un sistema integrado de gestión.

Grafica 7. Factores críticos de éxito

Así mismo, durante la realización de este trabajo, se detectaron varios factores, que aplicados a una correcta planeación y metodología pueden ser considerados factores claves de éxito en la implementación de un sistema integrado de gestión con ISO 9001, 20000 y 27001, a continuación los presentamos, cada uno con una breve explicación de por que el grupo de trabajo considera vital su priorización en el momento de aplicar a una certificación con los referentes estudiados.

- La autoridad y compromiso decidido de la Dirección de la empresa, evitarán la aparición de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales, asegurando también continuidad en el proyecto de implementación. La

comunicación, capacitación y empoderamiento del personal de todos los niveles de la organización, es también un factor clave de éxito.

- Mantener siempre en claro la visión, misión objetivos y la razón de ser de la organización, alinear los objetivos estratégicos con el objetivo de la certificación.

- Trabajo en equipo, este resulta ser un factor determinante para un eficiente esfuerzo colectivo de la empresa, destinado a alcanzar las metas y objetivos planificados.

- Realizar gestión del cambio dentro de la organización, desarrollar estrategias para saber cómo manejar o modificar los planes sobre la marcha sin afectar los objetivos estratégicos.

- Asegurarse que se está realizando una gestión adecuada de competencias, estar seguros de que el personal que participara en forma activa en la puesta en marcha de la implementación tiene los conocimientos, experiencia aptitudes y actitudes necesarias para desarrollar dicha tarea.

- Determinación clara de los límites, especificaciones y alcances de los objetivos en cada fase de la implantación de la metodología para llevar a cabo las certificaciones anheladas.

- Lograr un manejo adecuado de los recursos, definir responsables en la administración y disponibilidad de los mismos.

- Administrar y controlar los tiempos de ejecución de las tareas, no convertir la certificación en un logro inalcanzable por causa de la falta de planeación.

- Comprender en detalle el proceso de implantación de las normas: iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación, se debe aplicar la experiencia adquirida, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.

- Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo y un único centro de proceso de datos. Una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance a otros procesos de la organización.

- Servirse de lo ya implementado: otros sistemas de gestión ya implantados en la organización son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a responsables y auditores internos de otros sistemas de gestión, no tratar de “reinventar la rueda”, es importante apoyarse en métodos y guías ya existentes y así mismo sacar provecho de las experiencias de otras organizaciones.

- La certificación como objetivo: aunque se puede alcanzar la conformidad con las normas sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito. Eso sí, la certificación es el "trofeo anhelado", pero, no es bueno que sea la meta en sí misma. “El objetivo principal es la gestión de la seguridad de la información alineada con el negocio.”

7.2. FACTORES CRITICOS DE ÉXITO DEL PERSONAL IT.

Los siguientes fueron los factores críticos de éxito, específicos para procesos IT detectados durante el proceso de investigación.

El personal que trabaje en procesos IT, deberá tener en cuenta los siguientes aspectos claves sobre la seguridad:

- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.
- Se debe crear un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).

8. REFERENCIAS

Icontec internacional. NTC- ISO 9000. SISTEMAS DE GESTION DE LA CALIDAD. FUNDAMENTOS Y VOCABULARIO. Editada por el Instituto de Normas Técnicas y Certificación (ICONTEC). 2006.

Icontec internacional. NTC- ISO 9001. SISTEMAS DE GESTION DE LA CALIDAD. REQUISITOS. Editada por el Instituto de Normas Técnicas y Certificación (ICONTEC). 2009.

Icontec internacional. NTC- ISO 20000. GESTION DE SERVICIOS DE TECNOLOGIA DE LA INFORMACION. Editada por el Instituto de Normas Técnicas y Certificación (ICONTEC). 2011.

Icontec internacional. NTC- ISO 27001. SISTEMAS DE GESTION DE LA INFORMACION. Editada por el Instituto de Normas Técnicas y Certificación (ICONTEC). 2005.

López Neira A. (2005). iso27000.es EL PORTAL DE ISO 27001 EN ESPAÑOL. Recuperado el 17 de mayo de 2012, de *www.iso27000.es*

Zapata C. Proceso Certificación 27001. Recuperado del 17 de mayo de 2012, de *http://certificacion27001.blogspot.com/2010/09/empresas-certificadas-de-colombia.html*

Santiago J. (2003). Problemática, ventajas y desventajas de ISO27001 en las Pymes. Recuperado el 17 de mayo de 2012, de *http://www.laflecha.net/canales/seguridad/articulos/problematica-ventajas-y-desventajas-de-iso27001-en-las-pymes/*

Nieto Lucio T. (2003). ISO 20000 en español. Recuperado el 17 de abril de 2012, de *http://iso20000enespanol.com/index.php?option=com_content&task=view&id=12&Itemid=27*

Earcon, S.L. Kmkey Knowledge Manager. Recuperado el 12 de abril de 2012, de *http://www.kmkey.com/productos/software_gestion_calidad*

Clive Goodinson (2003). Pixton para divertirse. Recuperado el 17 de mayo de 2012, de *http://www.pixton.com/es*

LICENCIA DE USO – AUTORIZACIÓN DE LOS AUTORES

Actuando en nombre propio identificado (s) de la siguiente forma:

Nombre Completo Dialia Marcela Cortés Rugeles

Tipo de documento de identidad: C.C. [X] T.I. [ ] C.E. [ ] Número: 52.704 957

Nombre Completo Alix Victoria Ardila Guzmán

Tipo de documento de identidad: C.C. [X] T.I. [ ] C.E. [ ] Número: 37.706.728

Nombre Completo _____

Tipo de documento de identidad: C.C. [ ] T.I. [ ] C.E. [ ] Número: _____

Nombre Completo _____

Tipo de documento de identidad: C.C. [ ] T.I. [ ] C.E. [ ] Número: _____

El (Los) suscrito(s) en calidad de autor (es) del trabajo de tesis, monografía o trabajo de grado, documento de investigación, denominado:

Metodología para la implementación de un Sistema Integrado de Gestión con las normas ISO9001, ISO20000 e ISO 27001.

Dejo (dejamos) constancia que la obra contiene información confidencial, secreta o similar: SI [ ] NO [X]
(Si marqué (marcamos) SI, en un documento adjunto explicaremos tal condición, para que la Universidad EAN mantenga restricción de acceso sobre la obra).

Por medio del presente escrito autorizo (autorizamos) a la Universidad EAN, a los usuarios de la Biblioteca de la Universidad EAN y a los usuarios de bases de datos y sitios webs con los cuales la Institución tenga convenio, a ejercer las siguientes atribuciones sobre la obra anteriormente mencionada:

A. Conservación de los ejemplares en la Biblioteca de la Universidad EAN.
B. Comunicación pública de la obra por cualquier medio, incluyendo Internet
C. Reproducción bajo cualquier formato que se conozca actualmente o que se conozca en el futuro
D. Que los ejemplares sean consultados en medio electrónico
E. Inclusión en bases de datos o redes o sitios web con los cuales la Universidad EAN tenga convenio con las mismas facultades y limitaciones que se expresan en este documento
F. Distribución y consulta de la obra a las entidades con las cuales la Universidad EAN tenga convenio

Con el debido respeto de los derechos patrimoniales y morales de la obra, la presente licencia se otorga a título gratuito, de conformidad con la normatividad vigente en la materia y teniendo en cuenta que la Universidad EAN busca difundir y promover la formación académica, la enseñanza y el espíritu investigativo y emprendedor.

Manifiesto (manifestamos) que la obra objeto de la presente autorización es original, el (los) suscritos es (son) el (los) autor (es) exclusivo (s), fue producto de mi (nuestro) ingenio y esfuerzo personal y la realizó (zamos) sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de exclusiva autoría y tengo (tenemos) la titularidad sobre la misma. En vista de lo expuesto, asumo (asumimos) la total responsabilidad sobre la elaboración, presentación y contenidos de la obra, eximiendo de cualquier responsabilidad a la Universidad EAN por estos aspectos.

En constancia suscribimos el presente documento en la ciudad de Bogotá D.C.,

NOMBRE COMPLETO: Diana Marcela Cortés R.
FIRMA: _____
DOCUMENTO DE IDENTIDAD: 52.704957.
FACULTAD: Post Grados
PROGRAMA ACADÉMICO: Esp. Gerencia de Procesos y Calidad.

NOMBRE COMPLETO: _____
FIRMA: _____
DOCUMENTO DE IDENTIDAD: _____
FACULTAD: _____
PROGRAMA ACADÉMICO: _____

NOMBRE COMPLETO: Alix Victoria Ardila Guzmán
FIRMA: _____
DOCUMENTO DE IDENTIDAD: 37706728
FACULTAD: Postgrados
PROGRAMA ACADÉMICO: Especialización en Gerencia de procesos y calidad

NOMBRE COMPLETO: _____
FIRMA: _____
DOCUMENTO DE IDENTIDAD: _____
FACULTAD: _____
PROGRAMA ACADÉMICO: _____

Fecha de firma: 12 Julio / 2012.