REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO
ESPECIALIZACIÓN EN PLANIFICACIÓN,
DESARROLLO Y GESTIÓN DE PROYECTOS

PLAN MAESTRO PARA IMPLEMENTACIÓN DE PROYECTOS APLICANDO LA NORMA ISO/IEC 27001:2013 EN CERTIFICACION DE EMPRESAS CONSULTORAS DE SOFTWARE

Trabajo Especial de Grado, para optar al Título de Especialista en Planificación, Desarrollo y Gestión de Proyectos, presentado por:

Marquina Morandy, Argelys Betsabe, CI: 15.759.322

Asesorado por:

Guillén Guédez, Ana Julia

Caracas, abril de 2018

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO

ESPECIALIZACIÓN EN PLANIFICACIÓN, DESARROLLO Y GESTIÓN DE PROYECTOS

PLAN MAESTRO PARA IMPLEMENTACIÓN DE PROYECTOS APLICANDO LA NORMA ISO/IEC 27001:2013 EN CERTIFICACION DE EMPRESAS CONSULTORAS DE SOFTWARE

Trabajo Especial de Grado, para optar al Título de Especialista en Planificación, Desarrollo y Gestión de Proyectos, presentado por:

Marquina Morandy, Argelys Betsabe, CI: 15.759.322

Asesorado por:

Guillén Guédez, Ana Julia

Caracas, abril de 2018

REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO
ESPECIALIZACIÓN EN PLANIFICACIÓN, DESARROLLO Y GESTIÓN DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

PLAN MAESTRO PARA IMPLEMENTACIÓN DE PROYECTOS APLICANDO LA NORMA ISO/IEC 27001:2013 EN CERTIFICACION DE EMPRESAS CONSULTORAS DE SOFTWARE

Autora: Marquina Morandy, Argelys Betsabe
Asesora: Guillén Guédez, Ana Julia
Año: 2018

RESUMEN

La propuesta presentada en el trabajo de investigación busca identificar causas, y soluciones a problemas en los Sistemas de Gestión de Seguridad de la Información (SGSI), que pudiesen perjudicar las operaciones y estrategias en la aplicación de certificación de la norma ISO/IEC en empresas consultoras de software; así como tomar acciones preventivas y correctivas necesarias para mantener a los sistemas de información confiables y disponibles, es por eso que se propone diseñar un plan maestro para implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en certificación de empresas consultoras de software. Para desarrollar la investigación se utilizaron fundamentos teóricos establecidos en los estándares de la norma ISO/IEC 27001:2013, áreas del conocimiento y procesos gerenciales conformes al Project Management Institute PMI (2017), bibliografía pertinente con el trabajo especial de grado e investigaciones previas utilizadas como antecedentes. Para establecer las bases funcionales se plantearon los objetivos específicos que consisten en determinar los requisitos que exige la norma ISO/IEC 27001:2013 para la implementación de proyectos aplicada en certificación de empresas desarrolladoras de software, Elaboración de plan de auditoria y plan maestro para aplicar la norma ISO/IEC 27001:2013 en empresas consultoras de software. El tipo de investigación utilizada fue investigación aplicada, documental y no experimental, presentando un carácter descriptivo y explicativo. El tipo de investigación utilizada fue investigación aplicada, documental y no experimental, presentando un carácter descriptivo y explicativo. . En cuanto a la metodología seleccionada para realizar el trabajo especial de grado se utilizó un modelo para proyectos de investigación, donde se ejecutaron las etapas del ciclo de vida del estudio, partiendo desde su fase de inicio, planificación, la ejecución y finalmente la etapa de cierre del proyecto. Se recomienda implementar las actividades y documentos diseñados en este proyecto para la certificación correcta del SGSI en cualquier momento que la organización decida, este material contribuirá para la acreditación o certificación del modelo implantado. Finalmente, el objetivo del TEG es alcanzado con el desarrollo del Plan Maestro para empresas consultoras de software aplicando la norma ISO/IEC 27001:2013.

Palabras Clave: Proyecto, ISO/IEC 27001, Gerencia de Proyectos, Sistemas de Información, Norma, Certificación.

Línea de Trabajo: Plan de Implementación, migración y plan estratégico.

Nomenclatura UNESCO: (5311) Organización y Dirección de empresas, (5304) Actividad económica.

INDICE GENERAL

INDICE DE FIGURAS

Figura **Página**

INDICE DE TABLAS

Tabla **Página**

LISTA DE ACRONIMOS Y SIGLAS

EDT/WBS: Estructura Desagregada de Trabajo/Work Breakdown Structure.

IEC: Comisión Electrotécnica Internacional.

IPMA: International Project Management Association.

ISO: Organización Internacional de Normalización.

PDCA: Planificar, hacer, verificar, actual.

PMI: Project Management Institute.

SGSI: Sistema de Gestión de la Seguridad de la Información.

TEG: Trabajo Especial de Grado.

TI: Tecnología de la Información.

INTRODUCCIÓN

La problemática actual de las empresas que desean incursionar en el ámbito de la ingeniería de software es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a las compañías a pérdidas no solo de información, si no también económica.

Es por ello que se ve la necesidad de implantar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información, para garantizar que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

Un Sistema de Gestión de Seguridad de la Información (SGSI), en términos generales es entendida como un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización. Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada.

La característica principal de un SGSI es resguardar la confidencialidad e integridad de los activos de información en una empresa; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudaran a proteger estos activos.

En el presente Trabajo Especial de Grado se realiza un Plan Maestro Para Implementación De Proyectos Aplicando La Norma ISO/IEC 27001:2013 En Certificación De Empresas Consultoras De Software.

El presente trabajo especial de grado está constituido por capítulos, en el Capítulo I se presenta el planteamiento de la investigación, la interrogante, los objetivos, la justificación y las limitaciones.

El capítulo II se establecen los antecedentes de la investigación, de igual manera se muestra el marco teórico, en el que están planteadas las bases teóricas relacionadas con un sistema de gestión de seguridad de la información (SGSI), definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y las bases legales.

En el capítulo III, se especifican el marco metodológico, se detalla el tipo de investigación, las técnicas y herramientas de recolección de datos, las fases de la investigación, Operacionalización de las variables y aspectos éticos. En el capítulo IV, se describe el Marco referencial, En el capítulo V, se desarrollan los objetivos de la investigación y se describen los resultados por cada objetivo específico.

En el capítulo VI, se analizan los resultados, en el capítulo VII, se detallan las lecciones aprendidas. Finalmente se presenta el capítulo VIII, donde se describen las conclusiones por cada objetivo y se detallan las recomendaciones relacionadas al objetivo general y las Referencias Bibliográficas.

CAPITULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1. PLANTEAMIENTO DE LA INVESTIGACIÓN

Sabiendo que los datos que posee una organización es uno de sus más grandes activos por la cantidad de datos contables, financieros, comerciales, procesos de producción, datos de clientes y proveedores, entre otros. Se debe garantizar la seguridad de la información, se hace necesario una asesoría y seguimiento para la gestión de la seguridad de la información.

Es de suma importancia asegurar la confidencialidad, integridad y disponibilidad de sus datos, atributos que son inherentes a un Sistema de Gestión de la seguridad de la Información (SGSI). De forma que, se pueden establecer políticas, procedimientos, normas y controles relacionados a los objetivos del negocio de la organización contribuyendo a la mejora continua de sus procesos y la consecución de sus metas.

Por lo anteriormente expuesto es necesaria la implementación de herramientas, procedimientos, normas, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información, con ellos garantizar a que acceden a la información quienes estén designados para su uso, este disponible cuando se requiera permanezca tal como fue creada por sus propietarios y asegurar también la actualización de la misma a través de un Plan maestro para implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en empresas consultoras de software.

2. INTERROGANTE Y SISTEMIZACIÓN DE LA INVESTIGACIÓN

a. Interrogante de la Investigación

Sobre la base de lo expuesto anteriormente se formula la siguiente interrogante: ¿Cómo debe conformarse un plan maestro para implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en certificación de empresas consultoras de software empleando las buenas prácticas de planificación, desarrollo y gestión de proyectos?

b. Sistematización de la Investigación

Del Planteamiento del Problema surgen las siguientes interrogantes:

¿Cuáles son los requisitos que exige la norma ISO/IES 27001 para la certificación de empresas desarrolladoras de software?

¿Cómo elaborar un plan de auditoria para aplicar la norma ISO/IES 27001 en la certificación de empresas desarrolladoras de software?

¿Cuál es la factibilidad técnica y operacional al aplicar la norma ISO/IEC a empresas desarrolladoras de software?

¿Cómo debe estar estructurado un plan maestro del proyecto para la implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en certificación de empresas consultoras de Software., basado en las buenas prácticas de la Gerencia de Proyectos?

3. OBJETIVOS DE LA INVESTIGACIÓN

a. Objetivo General:

Diseñar el plan maestro para implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en certificación de empresas consultoras de software.

b. Objetivos Específicos

- Determinar los requisitos que exige la norma ISO/IEC 27001:2013 para la implementación de proyectos aplicada en certificación de empresas desarrolladoras de software.
- Elaborar plan de auditoria para aplicar la norma ISO/IEC 27001:2013 en empresas consultoras de software.
- Elaborar el plan maestro para la implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en empresas desarrolladoras de software.

4. JUSTIFICACIÓN E IMPORTANCIA

Debido a los riesgos a los que están expuestos los activos de información, el impacto que la interrupción de estos puede causar, es preponderante a la definición de una metodología y el uso de herramientas que ayuden a reducir y mitigar estos riesgos.

El establecimiento de un sistema de gestión de seguridad de la información (SGSI) en empresas desarrolladoras de software, permitirá asegurar la confidencialidad, disponibilidad e integridad de la los datos, protegiendo de esta forma la información de todas las partes interesadas, adicional a esto el cumplimiento de la norma ISO 27001 permitirá demostrar a sus clientes y socios principal la seguridad con que se abordan todos los temas relacionados con la seguridad de la información, la cual es la base para la gestión de riesgos de seguridad y así mismo la determinación de los niveles de protección que se requieran.

A través del SGSI en empresas desarrolladoras de software se lograrán optimizar todas las áreas dentro de las organizaciones, relacionadas con la información, logrando de esta forma realizar mejor las tareas, de manera mucho más rápida y segura; además de lograr obtener una certificación bajo la norma ISO/IEC 27001:2013, facilitando de esta forma la

comercialización de los diferentes productos y/o servicios, valorando los diferentes riesgos, así como los procedimientos de gestión necesarios.

5. ALCANCE Y DELIMITACIÓN DE LA INVESTIGACIÓN

El alcance de esta investigación es el diseño de un plan maestro para implementación de proyectos para certificación de empresas consultoras de software aplicando la norma ISO/IEC 27001:2013.

CAPITULO II. MARCO TEÓRICO

ANTECEDENTES

Los antecedentes son estudios previos relacionados con el problema planteado. En los antecedentes se trata de hacer una síntesis conceptual de las investigaciones o trabajos realizados sobre el problema formulado, con el fin de determinar el enfoque metodológico de la misma investigación.

Disterer, Journal of Information Security (2013). "ISO / IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información" El siguiente articulo expresa que Con la creciente importancia de la tecnología de la información, existe una necesidad urgente de medidas adecuadas de seguridad de la información. La gestión sistemática de la seguridad de la información es una de las iniciativas más importantes para la gestión de TI. Al menos desde que los informes sobre violaciones de privacidad y seguridad, prácticas contables fraudulentas y ataques a sistemas de TI aparecieron en público, las organizaciones han reconocido sus responsabilidades para salvaguardar los activos físicos y de información. Los estándares de seguridad se pueden usar como pauta o marco para desarrollar y mantener un sistema adecuado de gestión de la seguridad de la información (ISMS). Los estándares ISO / IEC 27000, 27001 y 27002 son estándares internacionales que están recibiendo un creciente reconocimiento y adopción. Se los conoce como "lenguaje común de organizaciones de todo el mundo" para la seguridad de la información. Con ISO / IEC 27001, las empresas pueden obtener su ISMS certificado por una organización externa y así mostrar a sus clientes evidencia de sus medidas de seguridad.

Gernot (2013) 13th IEEE International Symposium "Fortificación de la seguridad de la información por mapeo ontológico de ISO / IEC 27001Standard" Este documento presento un marco basado en la ontología para

mejorar la preparación de las auditorías ISO / IEC 27001 y para fortalecer el estado de seguridad de la empresa, respectivamente. Construyendo un extenso trabajo previo en las ciencias de la seguridad, desarrollamos cómo los artefactos ISO / IEC 27001 se pueden integrar en esta ontología. Una introducción básica a las ontologías de seguridad se da primero. Los ejemplos específicos muestran cómo ciertos requisitos de ISO / IEC 27001 deben integrarse en la ontología; además, nuestro motor basado en reglas se usa para consultar la base de conocimiento para verificar si se cumplen los requisitos de seguridad específicos. El objetivo de este documento es explicar cómo se pueden utilizar las ontologías de seguridad para una herramienta que respalde la certificación ISO / IEC 27001, proporcionando información fundamental para la preparación de auditorías y la creación y el mantenimiento de directrices y políticas de seguridad.

Arroyo (2017). "Formulación de estrategias para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (pci-dss) de Bancaribe banco universal" El siguiente trabajo de investigación plantea la implementación del estándar de seguridad de datos en la industria de tarjetas de pago de una institución bancaria, con normativas que permiten aumentar la seguridad en los sistemas de procesamiento de la información de las transacciones, para con ello se incrementar la confianza de los clientes y por consiguiente su fidelidad y aumento de las ventas del negocio. Presenta una propuesta de Plan de implementación para un proyecto de formulación de estrategias para implantar el estándar de seguridad de datos en la industria de tarjetas de pago, específicamente la versión 3.2 del estándar PCI-DSS, en el mismo se toman en cuenta las Mejores Prácticas de la Gerencia de Proyectos. Con la finalidad de desarrollar un Plan de implementación del estándar de seguridad de datos en la industria de tarjetas de pago de pago (PCI-DSS), el cual sirvió de modelo a aquellas instituciones bancarias que deseen apostar por la certificación PCI-DSS. Se utilizarán como referencias destacadas el Estándar PCI-DSS y las Buenas Prácticas en Gerencia de Proyectos.

León (2017). "Plan maestro del proyecto "migración de la norma iso 9001:2008 a la 9001:2015 caso: empresas de servicio en Venezuela" El presente trabajo de investigación presento una propuesta de Plan Maestro para un proyecto de migración por cambio o actualización de norma, específicamente el cambio de la Norma ISO 9001 a la versión 2015, en el mismo se tomó en cuenta las Mejores Prácticas de la Gerencia de Proyectos. Esta metodología tomó en cuenta todos los factores que las empresas consideraron a la hora de plantearse una migración (alcance, tiempo, costos, calidad, riesgos e involucrados, con la finalidad de desarrollar un Plan Maestro para la migración de la Norma ISO 9001:2008 a la ISO 9001:2015, el cual sirve de modelo a aquellas empresas que deseen apostar por la migración. Se utilizaron como referencias destacadas las Normas ISO 9001:2008, ISO 9001:20015 e ISO 21500:2012 y las Buenas Prácticas en Gerencia de Proyectos.

Kliem (1999) "Usando la Gerencia de Proyectos para Certificarse ISO 9000". El autor explica de una manera sistemática cómo las organizaciones pueden utilizar la gestión de proyectos para certificarse ISO 9000 y como las funciones básicas de la gestión de proyectos: planificación; estructura de desagregada de trabajo, estimación, programación, asignación de recursos; presupuestos, riesgo, organización, organización del equipo de trabajo; seguimiento de los progresos; planificación de contingencias; comunicación y la construcción de un ambiente de trabajo en equipo son aplicables, ya que la certificación ISO 9000 cumple con los tres criterios para considerarse un proyecto, tiene una duración fija, requiere realizar una secuencia de tareas y produce algo una vez que las tareas son completadas. El aporte a la presente investigación viene dado por la vigencia de la aplicabilidad de los elementos de la Gerencia de Proyectos en la Implementación de un Sistema de Gestión de la Calidad basados en el cumplimiento de la Norma ISO 9001:2015. Palabras clave: gerencia, gerencia de proyectos, ISO 9000.

Nieto (2013) "Plan de implementación de la ISO/IEC 27001:2005" Dentro de esta implementación de la norma ISO/IEC27001:2005, se contempla el estado de madurez, análisis y definición de riesgos. Las conclusiones generadas arrojaron como resultado que las amenazas y riesgos más representativos se encuentran en el factor humano, mostrando un resultado del 73%, además se hallan amenazas relacionadas con la infraestructura de la empresa y errores de programación; para reducir estas amenazas y riesgos, el autor sugiere unas salvaguardas para mitigar estos riesgos, adicionalmente presenta una serie de proyectos que permitirán reducir el riesgo a su nivel mínimo. La exploración realizada por el autor, aporta mucho al desarrollo del presente trabajo, puesto que despliega la investigación apoyada de la norma ISO/IEC 27001:2005 y se utiliza MAGERIT como metodología de análisis de riesgo.

Salcedo, (2015) "plan de implementación del SGSI basado en la norma ISO/IEC 27001:2013". La investigación se centra en la implementación de un SGSI en la empresa ISAG para solucionar problemas de seguridad en los servicios de información con la finalidad de llevar el riesgo a un nivel tolerable.
El autor concluye que el apoyo de la gerencia es vital para el desarrollo de proyecto y que se deben realizar auditorías periódicamente, por otro lado es necesario aumentar el presupuesto para la implementación de estrategias de seguridad informática en la organización.

BASES TEÓRICAS

A continuación se exponen los conceptos fundamentales que soportan la investigación.

Proyecto:

Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. (PMI, 2017, p. 4).

Kerzner (2003), define proyecto como “aquel conjunto de actividades… que además de caracterizarse por un alcance especifico y tener definido un inicio y final contempla un presupuesto limitado, consume recursos humanos y no humanos, y finalmente es multifuncional por naturaleza, dado que conjuga múltiples disciplinas durante su desarrollo”

La definición de ISO 21500:2012 Orientación sobre la Gestión de Proyectos es “conjunto único de procesos que consta de actividades coordinadas y controladas, con fechas de inicio y fin, que se llevan a cabo para lograr objetivos del proyecto.

Gerencia o Dirección de Proyectos:

La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo. Se logra mediante la aplicación e integración adecuadas de los procesos de dirección de proyectos identificados para el proyecto. La dirección de proyectos permite a las organizaciones ejecutar proyectos de manera eficaz y eficiente. (PMI, 2017. p.10).

Kerzner (2003), establece que la dirección de proyectos consiste en la planificación, organización, dirección y control de los recursos con el fin de alcanzar un objetivo relativo a corto plazo, haciendo énfasis lo anterior a la temporalidad y alcance único de cada proyecto. (p.4)

Las técnica de dirección de proyecto permiten coordinar eficiente los recursos, con el de alcanzar los resultados previstos. Pero es importante entender que la gerencia de proyectos no es una ciencia exacta y que, de ninguna manera, existe garantía de éxito; pues sobre cada proyecto pesan diferentes elementos de riesgo e incertidumbre, que nunca pueden ser controlados en su totalidad.

Ciclo de Vida de un Proyecto: El Project Management Institute (PMI;2017) define el Ciclo de Vida de un Proyecto como la serie de fases que atraviesa un proyecto desde su inicio hasta su conclusión. Proporciona el marco de referencia básico para dirigir el proyecto. Este marco de referencia básico se aplica

independientemente del trabajo específico del proyecto involucrado. Las fases pueden ser secuenciales, iterativas o superpuestas. Todos los proyectos pueden configurarse dentro del ciclo de vida genérico que muestra la figura 1.

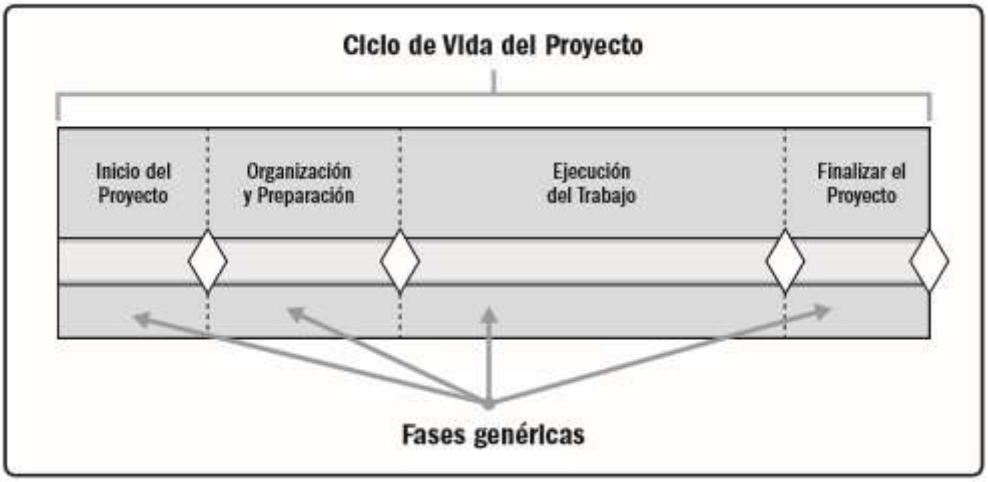


Figura 1. Representación Genérica del Ciclo de Vida de un Proyecto
Fuente: PMI (2017)

Procesos de la Dirección de Proyectos: De acuerdo con la PMI (2017), la Dirección de Proyectos se logra mediante la aplicación e integración adecuada de los 47 procesos de la dirección de proyectos agrupados en 5 grupos de procesos.

Grupos de Procesos de la Dirección de Proyectos: A continuación se presentan los cinco grupos de la Dirección de Proyectos descritos por la PMI (2017).

- **Grupo de Procesos de Inicio.**

  Proceso(s) realizado(s) para definir un nuevo proyecto o nueva fase de un proyecto existente al obtener la autorización para iniciar el proyecto o fase.

- **Grupo de Procesos de Planificación.**

  Proceso(s) requerido(s) para establecer el alcance del proyecto, refinar los objetivos y definir el curso de acción requerido para alcanzar los objetivos propuestos del proyecto.

- **Grupo de Procesos de Ejecución.**

Proceso(s) realizado(s) para completar el trabajo definido en el plan para la dirección del proyecto a fin de satisfacer los requisitos del proyecto.

- **Grupo de Procesos de Monitoreo y Control.**

Proceso(s) requerido(s) para hacer seguimiento, analizar y regular el progreso y el desempeño del proyecto, para identificar áreas en las que el plan requiera cambios y para iniciar los cambios correspondientes.

- **Grupo de Procesos de Cierre.**

Proceso(s) llevado(s) a cabo para completar o cerrar formalmente un proyecto, fase o contrato.

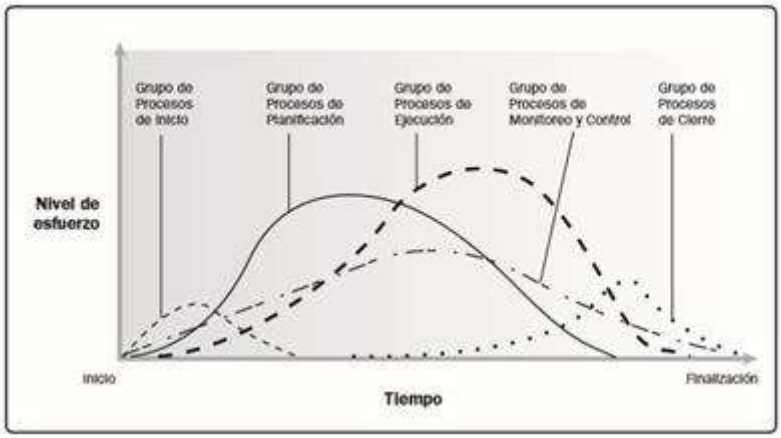


Figura 2 .Ejemplo de interacción entre los grupos de procesos dentro de un proyecto o Fase

Fuente: PMI (2017)

Áreas de Conocimiento de la Gerencia de Proyectos:

Según la PMI (2017) en su publicación internacional PMBOK Las Áreas de Conocimiento de la Dirección de Proyectos son campos o áreas de especialización que se emplean comúnmente al dirigir proyectos. Un Área de Conocimiento es un conjunto de procesos asociados a un tema particular de la dirección de proyectos. Estas 10 Áreas de Conocimiento se utilizan en la mayoría de los proyectos, la mayoría de las veces. Las necesidades de un proyecto

específico pueden requerir Áreas de Conocimiento adicionales. Las 10 Áreas de Conocimiento son:

- **Gestión de la Integración del Proyecto.**

La Gestión de la Integración del Proyecto incluye los procesos y actividades para identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de dirección del proyecto dentro de los Grupos de Procesos de la Dirección de Proyectos.

- **Gestión del Alcance del Proyecto.**

La Gestión del Alcance del Proyecto incluye los procesos requeridos para garantizar que el proyecto incluya todo el trabajo requerido, y únicamente el trabajo requerido, para completar el proyecto con éxito.

- **Gestión del Cronograma del Proyecto.**

La Gestión del Cronograma del Proyecto incluye los procesos requeridos para administrar la finalización del proyecto a tiempo.

- **Gestión de los Costos del Proyecto.**

La Gestión de los Costos del Proyecto incluye los procesos involucrados en planificar, estimar, presupuestar, financiar, obtener financiamiento, gestionar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado.

- **Gestión de la Calidad del Proyecto.**

La Gestión de la Calidad del Proyecto incluye los procesos para incorporar la política de calidad de la organización en cuanto a la planificación, gestión y control de los requisitos de calidad del proyecto y el producto, a fin de satisfacer las expectativas de los interesados.

- **Gestión de los Recursos del Proyecto.**

La Gestión de los Recursos del Proyecto incluye los procesos para identificar, adquirir y gestionar los recursos necesarios para la conclusión exitosa del proyecto.

- **Gestión de las Comunicaciones del Proyecto.**

La Gestión de las Comunicaciones del Proyecto incluye los procesos requeridos para garantizar que la planificación, recopilación, creación,

distribución, almacenamiento, recuperación, gestión, control, monitoreo y disposición final de la información del proyecto sean oportunos y adecuados.

- **Gestión de los Riesgos del Proyecto.**

La Gestión de los Riesgos del Proyecto incluye los procesos para llevar a cabo la planificación de la gestión, identificación, análisis, planificación de respuesta, implementación de respuesta y monitoreo de los riesgos de un proyecto.

- **Gestión de las Adquisiciones del Proyecto.**

La Gestión de las Adquisiciones del Proyecto incluye los procesos necesarios para comprar o adquirir productos, servicios o resultados que es preciso obtener fuera del equipo del proyecto.

- **Gestión de los Interesados del Proyecto.**

La Gestión de los Interesados del Proyecto incluye los procesos requeridos para identificar a las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto, para analizar las expectativas de los interesados y su impacto en el proyecto, y para desarrollar estrategias de gestión adecuadas a fin de lograr la participación eficaz de los interesados en las decisiones y en la ejecución del proyecto.

Estándar:

Un estándar es una publicación que recoge el trabajo en común de los comités de fabricantes, usuario, organizaciones, departamentos de gobierno y consumidores y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional, con el objetivo de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología. Los estándares ayudan a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan todas las partes interesadas (productores, vendedores, compradores, usuarios y reguladores).

En principio, son de uso voluntario, aunque la legislación y las reglamentaciones nacionales pueden hacer referencia a ellos.

Organización Internacional de Normalización (ISO):

La Organización Internacional de Normalización (ISO), es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 157 países, uno por cada país.

La ISO es una organización no gubernamental, establecida en 1947 cuya misión es promover el desarrollo de la estandarización y las actividades relacionadas, con el fin de facilitar el intercambio de servicios y bienes y promover la cooperación en la esfera de lo intelectual, científico, tecnológico y económico.

Todos los trabajos realizados por la ISO resultan en acuerdos internacionales, los cuales son publicados como Estándares Internacionales.

ISO 27001

Desde 1901 y como primera entidad de normalización a nivel mundial, BSI (*British Standards Institution*) es responsable de la publicación de importantes normas Como: BS 5750 publicada en 1979, origen de ISO 9001; BS 7750 publicada en 1992, origen de ISO 14001. La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, estableció los requisitos de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En el 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el así como el año de publicación formal de la revisión.

Esta norma, está constituida por 8 cláusulas y Anexos, de los cuales la parte principal del sistema son desde la cláusula 4 a la 8 y el Anexo A. Las cláusulas indican los procedimientos que deben ser implementados, los documentos que deben ser elaborados y los registros que deben ser mantenidos dentro de la organización. El anexo A indica los controles y objetivos de control a implementar con el fin de ser salvaguardas, los mismos que se encuentran distribuidos en 11 dominios que son:

- A.1 Política de seguridad.
- A.2 Organización de la seguridad de la información.
- A.3 Gestión de activos.
- A.4 Seguridad de los recursos humanos.
- A.5 Seguridad física y ambiental.
- A.6 Gestión de las comunicaciones y operaciones.
- A.7 Control de acceso.
- A.7 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.9 Gestión de incidentes en seguridad de la información.
- A.10 Gestión de la continuidad del negocio.
- A.11 Cumplimiento.

Por lo tanto, ISO 27001, es un estándar que proporciona un modelo para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (del inglés Plan-Do-Check-Act, cuyo significado en español es Planear, Hacer, Verificar y Actuar; o ciclo de Deming) de mejora continua, al igual que otros sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

Fases de un SGSI basado en la norma ISO 27001

En base a este sistema PDCA, la norma ISO 27001 establece las siguientes fases para elaborar un SGSI.

1. Análisis y evaluación de riesgos.
2. Implementación de controles.
3. Definición de un plan de tratamiento de los riesgos o esquema de mejora.
4. Alcance de la gestión.
5. Contexto de organización.
6. Partes interesadas.
7. Fijación y medición de objetivos.
8. Proceso documental.
9. Auditorías internas y externas.

Seguridad de la información

Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Entendiéndose por confidencialidad a la propiedad que impide la divulgación de información a personas o sistemas no autorizados, es decir asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización; así mismo, cuando nos referimos a integridad, es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, es decir trata de mantener la información tal cual fue generada y al hablar de disponibilidad, nos referimos a la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Modelo PDCA (Plan – Do – Check – Act)

El modelo PDCA (Plan, Do, Check, Act), en su equivalencia en español: Planificar, hacer, verificar y actuar (PHVA), es una estrategia de mejora continua.

Este modelo es muy usado para la implantación de sistemas de gestión, en este caso un Sistema de Gestión de Seguridad de Información, ya que permite una efectiva organización y documentación, lo cual es requerido en este proceso.

Figura 3 Modelo PDCA.

Fuente: Swartch Implementation Guideline ISO/IEC 27001:2013

En la figura Modelo PDCA, se muestra este modelo basado en los procedimientos esenciales para un SGSI.

El modelo PDCA es una estrategia de mejora continua, implementada en cuatro pasos detallados a continuación:

- **Planificar**

  1. Planificación de la gestión del servicio.
  2. Definir el alcance del SGSI en la empresa.
  3. Identificar los activos de información y tasarlos.
  4. Hacer el análisis y evaluación del riesgo.
  5. Determinar opciones para el tratamiento del riesgo.

6. Definir los procesos.

7. Definir los recursos, equipamiento, presupuestos, herramientas.

- **Hacer**

Implementar la gestión y provisión del servicio.

1. Elaborar el plan de tratamiento del riesgo, detallando las acciones que deben emprenderse para implantar las opciones de tratamiento del riesgo escogidas.

- **Verificar**

1. Monitorear, medir y verificar.
2. Desarrollar procedimientos de monitoreo.
3. Revisar regularmente el SGSI.
4. Revisar objetivos y plan de gestión del servicio.
5. Auditar internamente el SGSI.

- **Actuar**

Mantener el SGSI y desarrollar la mejora continua.

1. Identificar e implantar las mejoras.
2. Adoptar acciones correctivas y preventivas.
3. Verificar que las mejoras cumplen su objetivo.

BASES LEGALES

Según Constitución de la república bolivariana de Venezuela (Gaceta oficial N°5.908 Extraordinario, de fecha 19/02/2009) se mencionan los artículos con relación a esta investigación:

Existen diversas leyes y normativas relativas a la Seguridad de la Información y al uso de las tecnologías de la información (TI) que aplican a todo tipo de organizaciones. A continuación se presentan las leyes nacionales y normas internacionales, que tienen correspondencia con la presente investigación.

Constitución Bolivariana de Venezuela: Según gaceta oficial de la República Bolivariana de Venezuela, 5.908. (Extraordinaria), febrero 19, 2.009, regula en su Título VI de manera programática y general el sistema socio económico de la nación. El artículo 117 consagra, entre otros aspectos, que todas las personas tendrán derecho a disponer de bienes y servicios de calidad; así como, a una información adecuada y no engañosa sobre el contenido y características de los productos y servicios que consumen. Visto que este Ente Regulador, debe velar por un desarrollo armónico y ordenado de la red de distribución de los servicios bancarios a los fines que éstos cubran racionalmente las expectativas de crecimiento de la demanda de tales servicios.

Ley Orgánica de Ciencia, Tecnología e Innovación: Promulgada en Gaceta Oficial Nro. 38.242 de fecha 03 de Agosto de 2005.

Titulo 1: Disposiciones fundamentales

Artículo 1: Objeto del Decreto-Ley: El presente Decreto-Ley tiene por objeto desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para la generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional.

Ley cuyo objetivo fundamental de estructurar el Sistema Nacional de Ciencia, Tecnología e Innovación (SNCTI). En este Sistema se integran las instituciones, organismos, entidades y organizaciones universitarias estadales del sector público y privado para que realicen actividades vinculadas al desarrollo científico, tecnológico e innovativo, y adelanten la formación del personal que hace vida en los diferentes entes que lo conforman.

Ley Orgánica de Telecomunicaciones: Promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001 por Decreto N° 1.024 - 10 de febrero de 2001

Título I. Disposiciones Generales.

Artículo 1.- Esta Ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes.

Se excluye del objeto de esta Ley la regulación del contenido de las transmisiones y comunicaciones cursadas a través de los distintos medios de telecomunicaciones, la cual se regirá por las disposiciones constitucionales, legales y reglamentarias correspondientes.

Ley que da soporte legal al área de las telecomunicaciones, regulando la transferencia de información entre los diferentes organismos, incluyendo las redes de datos.

Ley Especial Contra los Delitos Informáticos: Promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001 por la Asamblea Nacional.

Título I. Disposiciones Generales.

Artículo 1. Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Este instrumento legal concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Cuyo objetivo es proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra o mediante el uso de tales tecnologías.

Ley Sobre Mensajes De Datos y Firmas Electrónicas: Promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001, por Decreto N° 1.024 – 10 de febrero de 2001.

Capítulo I. Objeto y Aplicabilidad Del Decreto -Ley

Artículo 1°: El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas. La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Esta ley sienta las bases para la regulación del comercio electrónico. Apoyando las transacciones a través de formatos digitales, las transferencias de datos entre organizaciones, el establecimiento de redes inter empresariales, así como la comunicación efectiva entre organismos públicos y privados.

ISO/IEC 27000:2014 Tecnología de Información, Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información-Requerimientos. Aprobado y publicado como estándar internacional el 15 de enero de 2014, por la Organización Internacional de Estándares y la Comisión Electrónica Internacional.

ISO 21500:2012 Guía de Dirección de Proyectos. Publicado el año 2012 por el Organismo Internacional de Normalización. Proporciona una guía para la gestión de proyectos y puede ser utilizado por cualquier tipo de organización, incluidas las organizaciones públicas, privadas u organizaciones comunitarias, y para cualquier tipo de proyecto, independientemente de la complejidad, tamaño o duración.

CAPITULO III: MARCO METODOLOGICO

3.1 Tipo de Investigación

El presente proyecto corresponde al tipo de investigación Aplicada y Documental, de acuerdo con Arias (2006): “La investigación documental “es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por los otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos”.

Este tipo de investigación estudia los factores internos y busca dar respuesta en corto plazo a empresas consultoras de software aplicando la norma ISO/IEC 27001:2013.

3.2. Diseño de la Investigación

El diseño se elaborará basado en la norma ISO/IEC 27001:2013, la cual provee practicas apropiadas para el desarrollo e implementación de cada uno de sus componentes, estableciendo las fases de documentación y procedimientos requeridos y exigidos en el estándar para continuar con el diseño y ejecución del SGSI de manera adecuada. En consecuencia se debe realizar un análisis de los riesgos, vulnerabilidades y amenazas que se presentan en las empresas consultoras de software las cuales no siempre implementan sistemas de seguridad de información robustos, utilizando el siglo Deming proporcionando una realimentación constante de cada uno de los procesos.

3.3 Unidad De Análisis

De acuerdo a lo anteriormente planteado la unidad de análisis en la que fue desarrollada la investigación, fue en la Dirección de Seguridad de la Información de empresas desarrolladoras de software.

3.4 Técnicas Y Herramientas De Recolección e Interpretación

Un instrumento de recolección de datos es cualquier recurso del cual pueda valerse el investigador para aproximarse a los fenómenos y extraer de ellos información.

> Según Hernández, Fernández y Baptista (2010), "La recolección de los datos se fundamenta en la medición (se miden las variables o conceptos contenidos en las hipótesis). Esta recolección se lleva a cabo al utilizar procedimientos estandarizados y aceptados por una comunidad científica. Para que una investigación sea creíble y aceptada por otros investigadores, debe demostrarse que se siguieron tales procedimientos. Como en este enfoque se pretende medir, los fenómenos estudiados deben poder observarse o referirse en el mundo real". (p.5).

Para la recolección de datos del presente trabajo se usarán las siguientes técnicas:

Revisión Bibliográfica: La revisión bibliográfica fue un procedimiento estructurado cuyo objetivo es la localización y recuperación de información relevante, dando como ventaja marcar pautas teóricas sobre el tema, facilitando el entendimiento del mismo. En el caso de esta investigación fue utilizada para la búsqueda de datos históricos, información relacionada a la implementación del estándar de seguridad de datos, así como información para desarrollar las bases teóricas.

Para esta técnica se usaran:

- Bibliografía de Gerencia de Proyectos
- Procedimiento para Planes de Ejecución de Proyectos (PEP)
- Norma ISO/IEC 27001:2013.
- Implementación de Plan Maestro.

Juicio de Expertos: La evaluación mediante el juicio de expertos, método de validación cada vez más utilizado en la investigación, “consiste, básicamente, en solicitar a una serie de personas la demanda de un juicio hacia un objeto, un instrumento, un material de enseñanza, o su opinión respecto a un aspecto concreto” (Cabero y Llorente, 2013:14). Se trata de una técnica cuya realización adecuada desde un punto de vista metodológico constituye a veces el único indicador de validez de contenido del instrumento de recogida de datos o de información (Escobar Pérez, 2008); de ahí que resulte de gran utilidad en la valoración de aspectos de orden radicalmente cualitativo.

Para esta técnica, se usó información del personal gerencial y técnico especializado del área de IT de cada empresa.

El análisis de brechas El análisis de brechas es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado, respecto a uno o más puntos de referencia seleccionados de orden local, regional, nacional y/o internacional. El resultado esperado es la generación de estrategias y acciones para llegar al referente u objetivo futuro deseado.

Metodología Magerit

Magerit es una metodología de análisis y gestión de riesgos que proporciona un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para así poder implementar las medidas de control más adecuadas que permitan mitigar los riesgos.

Magerit se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser aprovechadas por estas amenazas, obteniendo una identificación clara de las medidas preventivas y correctivas más apropiadas.

Metodología PDCA – Ciclo Deming

La metodología PDCA o ciclo Planificación – Ejecución – Evaluación – Actuación o secuencia Planificación – Ejecución – Evaluación – Actuación (en inglés, PDCA, de Plan-Do-Check-Act) es una secuencia cíclica de actuaciones que se hacen a lo largo del ciclo de vida de un servicio o producto para planificar su calidad, en particular en la mejora continua.

3.5 Fases De La Investigación

Estas fases de la investigación fueron realizadas con la finalidad de obtener un Plan de Gestión del Proyecto para el "Plan maestro para Implementación de proyectos y certificación de empresas consultoras de software aplicando la norma ISO/IEC 27001:2013", el estudio se realizó bajo un conjunto de fases contiguas, las cuales se presentan a continuación:

Fase I: Inicio de la investigación.

Esta fase alcanzó la investigación documental que sirvió de base para el planteamiento del problema, definición de objetivo general y objetivos específicos, marco teórico, marco metodológico, antecedentes.

Fase II: Planificación de la investigación: La segunda fase consistió en establecer las políticas, procedimientos y la documentación utilizando el Metodología PDCA para planificar, hacer, verificar y actuar con el cronograma del proyecto.

Fase III: Ejecución de la investigación: Esta etapa será la más larga en tiempo, y haciendo uso de las técnicas serán respondidas las interrogantes planteadas, y en consecuencia se cumplirá con lo establecido en los objetivos específicos de la investigación.

Fase IV: Cierre de la investigación: La última fase corresponde a la evaluación, conclusiones y recomendaciones del proceso investigativo y a la entrega final del Trabajo Especial de Grado (TEG).

3.6 Estructura Desagregada de Trabajo: En la figura 4 se presenta la Estructura Desagregada de Trabajo (EDT/WBS) que se utilizará en esta investigación.

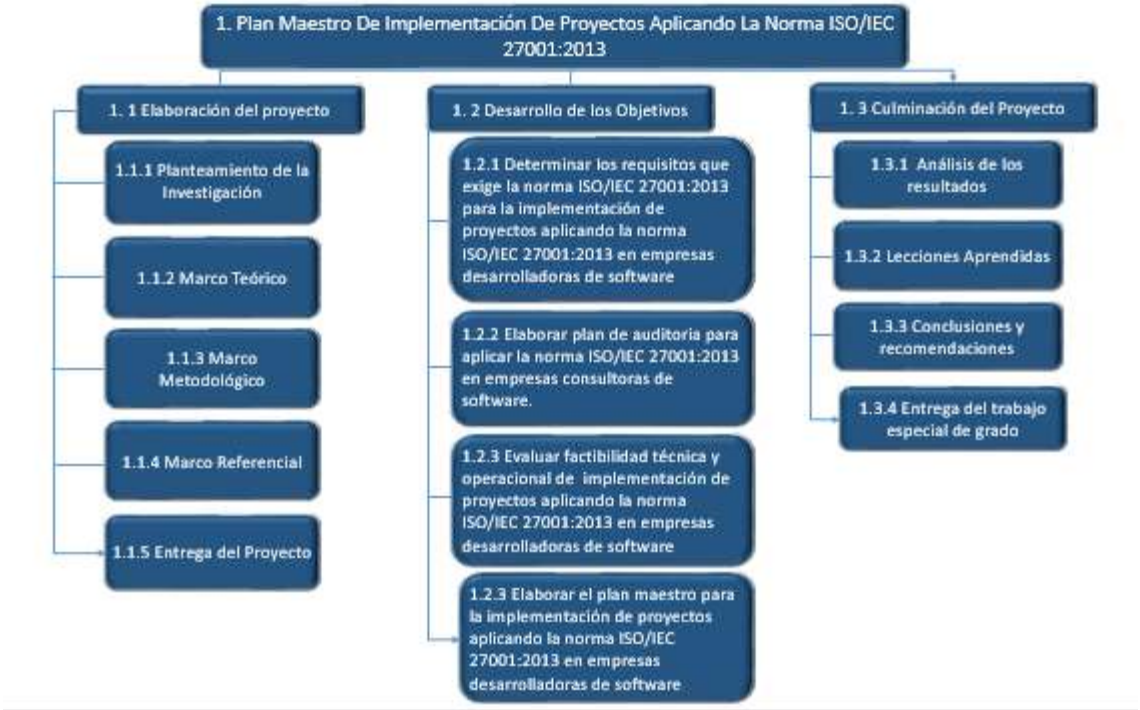


Figura 4. EDT/WBS Trabajo Especial de Grado
FUENTE: Adaptación PMI (2017)

3.7 Procedimiento por Objetivos: A continuación se presenta el procedimiento que será aplicado a cada uno de los objetivos específicos planteados en esta investigación y cuyo fin último será formular las estrategias para implementar Proyectos de Certificación de Empresas Consultoras De Software aplicando La norma ISO/IEC 27001:2013.

Objetivo 1. Determinar los requisitos que exige la norma ISO/IEC 27001:2013 para la implementación de proyectos en certificación de empresas desarrolladoras de software

Actividades:

- Revisión de los requisitos que exige la norma ISO/IEC 27001:2013 para la aplicación de la misma.

Técnicas y herramientas: Revisión bibliográfica, revisión documental.

Entregable: Requisitos exigidos por la norma ISO/IEC 27001:2013 en empresas consultoras de software.

Objetivo 2. Elaborar plan de auditoria para aplicar la norma ISO/IEC 27001:2013 en empresas consultoras de software.

Actividades:

- Análisis de la información recopilada
- Redacción del informe de análisis
- Aplicar PDCA Deming
- Evaluación de los riesgos.

Técnicas y Herramientas: Revisión documental, aplicación de metodología Magerit y PHVA, evaluación e impacto de riesgos, matriz de probabilidad e impacto, categorización de riesgos, evaluación de la urgencia de los riesgos, estrategias para riesgos positivos y negativos.

Entregable: Documento a ser implementado en las empresas aplicando la norma ISO/IEC 27001:2013 en el SGSI.

Objetivo 3. Elaborar el plan maestro para la implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en empresas desarrolladoras de software.

Actividades:

- Revisión de las áreas del conocimiento según el PMI que apliquen a la investigación
- Revisión de las normas ISO 27001, ISO/IEC 27001:2013
- Aplicación del estándar para la elaboración del plan maestro
- **Técnicas y Herramientas:** Juico de expertos, Revisión documental

Entregable: Plan maestro para la implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en empresas desarrolladoras de software.

3.8 OPERACIONALIZACIÓN DE LAS VARIABLES:

A continuación la tabla N° 1 presenta de manera resumida la operacionalización de las variables.

Tabla N° 1 Operacionalización de las variables.

EVENTO	SINERGIA	VARIABLE	INDICADOR	TÉCNICAS / HERRAMIENTAS	FUENTE
Plan Maestro Para Implementación De Proyectos Aplicando La Norma ISO/IEC 27001:2013 En Empresas Consultoras De Software.	Determinar los requisitos que exige la norma ISO/IEC 27001:2013 para la implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en empresas desarrolladoras de software	Requisitos	Informe de Requisitos	Consulta de expertos Revisión documental	Información de campo PMI(2017)
	Elaborar plan de auditoria para aplicar la norma ISO/IEC 27001:2013 en empresas consultoras de software.	Plan de Auditoria	Informe sobre los riesgos detectados	Metodología Magerit Revisión documental Evaluación e impacto de riesgos Matriz de probabilidad e impacto Evaluación de la urgencia de los riesgos Estrategias para riesgos positivos y negativos	
	Elaboración de plan maestro para la implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en empresas desarrolladoras de software.	Alcance Tiempo Costos Calidad Riesgos Involucrados	Plan maestro para la Implementación de proyectos aplicando La norma ISO/IEC 27001:2013 en empresas consultoras de software.	Juicio de expertos Revisión documental	Bases de datos Académicas PMI(2017)

3.9 Aspectos Éticos De La Investigación

Los Aspectos Éticos para esta investigación se sostienen de dos códigos específicos, el primero el Código de Ética Profesional del CIV (1.996) y en segundo lugar el Código de ética y conducta profesional del PMI (2.006).

Código de Ética Profesional del CIV **(1.996),** donde se considera "contrario a la ética" (p. 1) para profesionales de la ingeniería, las siguientes situaciones:

- "Actuar en cualquier forma que tienda a menoscabar el honor, la responsabilidad y aquellas virtudes de honestidad, integridad y veracidad que deben servir de base a un ejercicio cabal de la profesión." (p. 1).
- "Descuidar el mantenimiento y mejora de sus conocimientos técnicos, desmereciendo así la confianza que al ejercicio profesional concede la sociedad." (p. 1).
- "Atentar contra la reputación o los legítimos intereses de otros profesionales, o intentar atribuir injustificadamente la comisión de errores profesionales a otros colegas." (p. 2).
- "Utilizar estudios, proyectos, planos, informes u otros documentos, que no sean el dominio público, sin la autorización de sus autores y/o propietarios." (p. 2).
- "Revelar datos reservados de índole técnico, financiero o profesionales, así como divulgar sin la debida autorización, procedimientos, procesos o características de equipos protegido por patentes o contratos que establezcan las obligaciones de guardas de secreto profesional. Así como utilizar programas, discos, cintas u otros medios de información, que no sea de dominio público, sin la debida autorización de sus autores y/o propietarios, o utilizar sin autorización de códigos de acceso de otras personas, en provecho propio." (p.2).

Código de Ética y Conducta Profesional del PMI **(2.006),** donde destacan las siguientes expectativas entre profesionales de la Gerencia de Proyectos:

- "Únicamente aceptamos aquellas asignaciones que se condicen con nuestros antecedentes, experiencia, habilidades y preparación profesional." (p. 3).

- “Cumplimos los compromisos que se asumen: hacer lo que se dice que se va a hacer.” (p. 3).
- “Cuando cometemos errores u omisiones, se responsabilizan por ellos y los corrigen de inmediato.” (p. 3).
- “Protegemos la información confidencial o de propiedad exclusiva que se les haya confiado.” (p. 3).
- “Nos informamos sobre las normas y costumbres de los demás, y evitar involucrarse en comportamientos que ellos podrían considerar irrespetuosos.” (p. 4).
- “Escuchamos los puntos de vista de los demás y procurar comprenderlos.” (p. 4).
- “Nos comportamos de manera profesional, incluso cuando no se es correspondido de la misma forma.” (p. 4).
- “No nos aprovechamos de nuestra experiencia o posición para influir en las decisiones o los actos de otras personas a fin de obtener beneficios personales a costa de ellas.” (p. 4).
- “Respetamos los derechos de propiedad de los demás.” (p. 4).
- “Demostramos transparencia en el proceso de toma de decisiones.” (p. 5).
- “Revisar constantemente los criterios de imparcialidad y objetividad, y realizar las acciones correctivas pertinentes.” (p. 5).
- “Brindar acceso equitativo a la información a quienes están autorizados a contar con dicha información.” (p. 5).

“Procuramos que haya igualdad de acceso a oportunidades para aquellos candidatos que sean idóneos.” (p. 5).

CAPITULO IV. MARCO REFERENCIAL

Reseña

La información obtenida sobre CAVEDES se encontró directamente en su página web, De igual manera su visión, misión y valores y todos los datos de la organización.

Historia CAVEDATOS

El 26 de Mayo de 1983, un grupo de empresas con visión de futuro y comprometidas con el desarrollo tecnológico del país, se unieron para formar lo que hoy en día es una de las organizaciones más importantes del sector tecnológico nacional, la Cámara Venezolana de Empresas de Tecnologías de la Información (CAVEDATOS), Asociación Civil de carácter privado, autónoma y sin fines de lucro, de interés colectivo y apolítica.

En sus inicios, su denominación como "Cámara Venezolana de Representantes de Sistemas de Procesamientos de Datos", respondía a las necesidades de los productores nacionales ante un mundo que comenzaba a visualizar el concepto de globalización. Posteriormente, en 1986, adaptándose a la dinámica de los avances tecnológicos, la Cámara amplía su alcance, y pasa a llamarse "Cámara Venezolana de Empresas de Tecnologías de la Información", dando cabida a la oferta de nuevos servicios de valor agregado, como las empresas relacionadas con el área de Internet.

Actualmente CAVEDATOS es el representante nacional del sector privado de industria y comercio relacionado con fabricación e integración de software, hardware y redes, incluyendo consultoría en tecnologías de información, internet y otras áreas complementarias de las comunicaciones y la informática.

A continuación los Presidentes de CAVEDATOS desde 1983 a la fecha

Períodos	Presidentes de CAVEDATOS
2011-2013	Gustavo Terrero
2009-2011 2007-2009	Pedro Pablo Ojanguren
2005-2007 2003-2005	Ricardo Holmquist
2001-2003	Eduardo Sosa
1999-2001	Alexis Castro
1997-1999	Eduardo Baquero
1995-1997	Oscar Monteverde
1993-1995	Carlos Barrientos
1991-1993 1989-1991	Hans Klein
1987-1989	Rolando Rodríguez Vio
1985-1987 1983-1985	Francisco Ramírez

Además de los ex presidentes de la Junta Directiva, nuestros directores vitalicios: incluyen a los Srs. Egon Keltai, Jaime Villalta, Rainer Barany y Enrique Gonzalez†.

Misión

Es la asociación que representa, fomenta, desarrolla, defiende y protege al sector privado de las tecnologías de la información.

Visión

Ser reconocida como la organización que más contribuye a la integración y al fortalecimiento del sector de las tecnologías de la información, para mejorar la calidad de vida de la población.

Objetivos

- Fortalecer a las empresas afiliadas, propiciando un ambiente de negocios en la industria de las TIC, a través de una actividad gremial proactiva ante los sectores empresariales y la comunidad en general.
- Fomentar el desarrollo de la industria de las Tecnologías de la Información y Comunicaciones, entre ellas la del Software en Venezuela, por su contribución al desarrollo de la competitividad en el país, y por su potencial de exportación.
- Incentivar la creación de capital nacional, a través de programas de fortalecimiento de las empresas venezolanas.
- Promover la creación y el desarrollo del capital intelectual venezolano, como motor fundamental de un país en la sociedad del conocimiento.

Líneas Estratégicas

CAVEDATOS participa como asesor de organismos gubernamentales e instituciones privadas en la formulación de políticas claras que incentiven el desarrollo de la industria de las TIC como un sector prioritario para el país.

Estas políticas corresponden, primordialmente, a los siguientes aspectos:

- Reconocimiento de las TIC en general y del sector ensamblador y la industria del software y contenidos en particular, como sector productivo del país por su alta capacidad para generar desarrollo y por su potencial de exportación.

- Programa de incentivos fiscales para las empresas de base tecnológica o aquellas que inviertan en procesos de tecnologías.

Masificación del uso de la tecnología. Creación de una sociedad de garantías reciprocas para el sector de las TI.

Estructura Organizativa

Junta Directiva

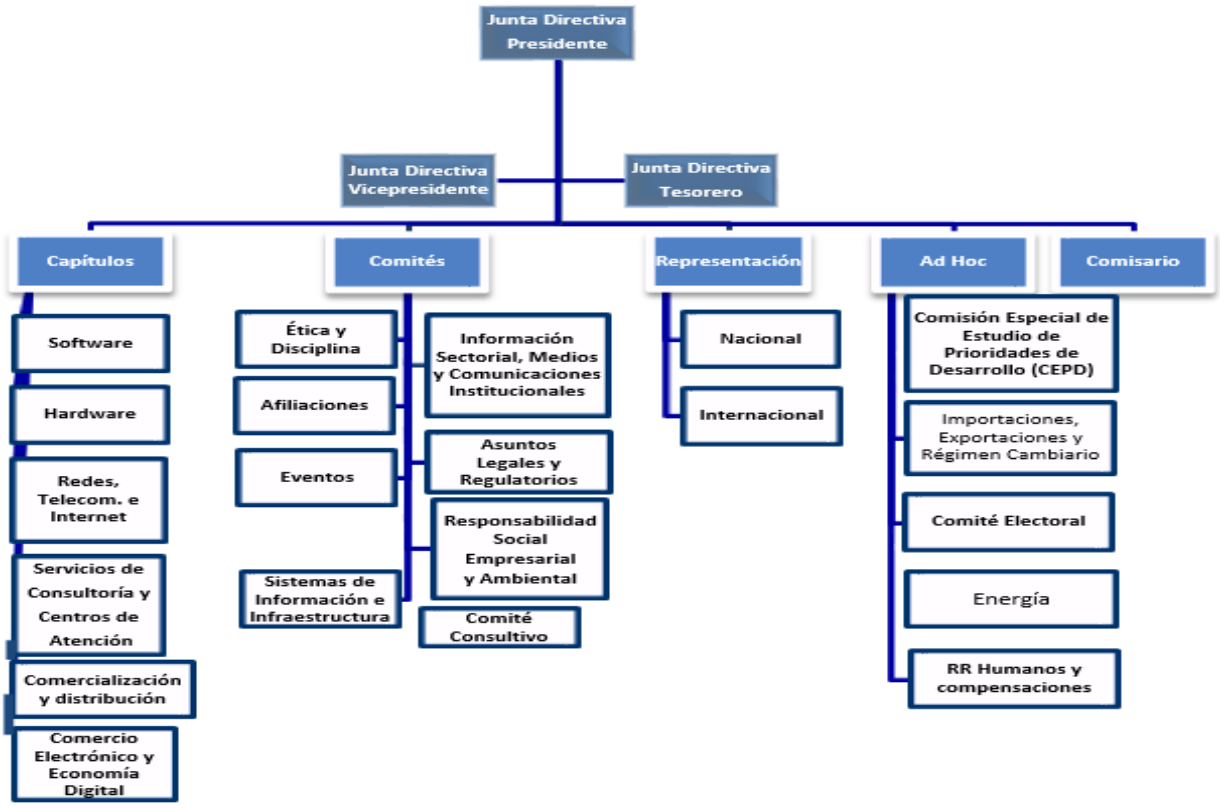


Figura 5. Estructura Organizacional CAVEDATOS
Fuente: CAVEDATOS (2017)

Estructura Operativa

Afiliaciones a otras Organizaciones

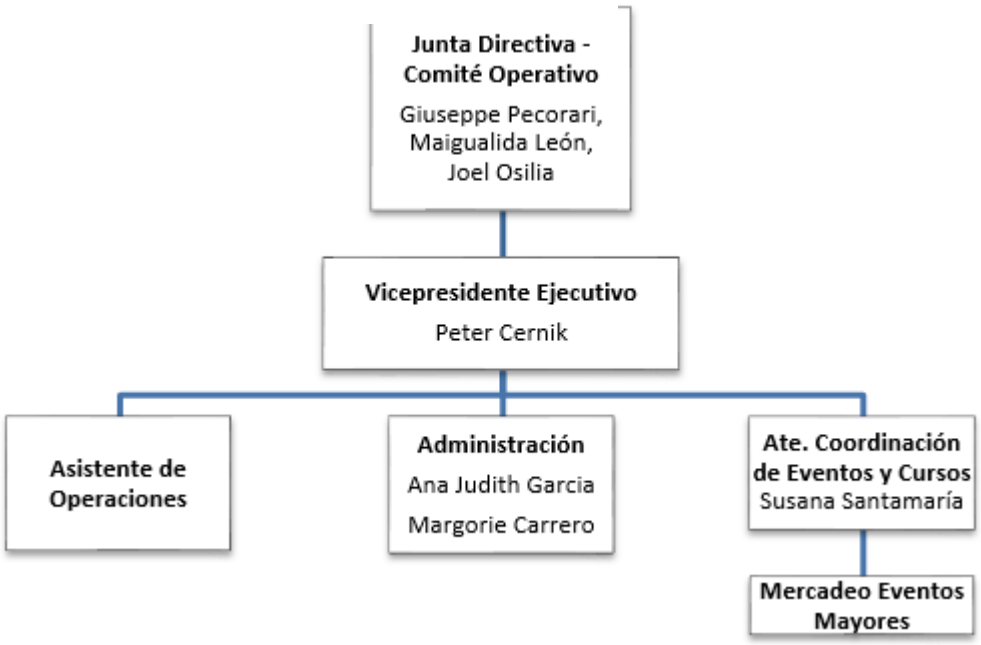


Figura 6. Estructura Operativa CAVEDATOS
Fuente: CAVEDATOS (2017)

Nacionales

Figura 7. Empresas afiliadas a CAVEDATOS
Fuente: CAVEDATOS (2017)

CONINDUSTRIA

La Confederación Venezolana de Industriales -CONINDUSTRIA- es la organización gremial del sector industrial nacional; representa el 90% de la producción manufacturera, la cual incluye grandes, medianas y pequeñas industrias, con servicios empresariales, brindando asistencia técnica a la industria nacional, respaldando su desarrollo, modernización, crecimiento, competitividad. www.conindustria.org

FEDECAMARAS

Es una Asociación Civil sin fines de lucro formada por entidades económicas gremiales privadas integradas por empresarios, personas naturales o jurídicas que conjunta o separadamente, ejerzan la representación de actividades e intereses económicos.

www.fedecamaras.org.ve

Internet Society Venezuela

Es una organización global sin fines de lucro que facilita la realización y promoción de estándares, educación y políticas relacionadas con la Internet, está dedicada a asegurar el desarrollo, evolución y uso de la Internet para el beneficio de todos en todo el mundo.

www.isoc.org

Internacionales

Figura 8. Empresas Internacionales afiliadas a CAVEDATOS
Fuente: CAVEDATOS (2017)

WITSA

La World Information Technology and Services Alliance (WITSA) es un Consorcio de Asociaciones de Tecnologías de la información (TI) alrededor del mundo. Representa a más del 90% del mercado mundial de TI y promueve políticas públicas a escala internacional que afectan la "*infraestructura global de la información*". www.witsa.org

ALETI

Es la Federación que nuclea a la Industria TIC de 19 países. Su misión es integrar a todas las Entidades (Federaciones, Cámaras y Asociaciones) TIC de Latinoamérica, El Caribe, España y Portugal para fomentar el uso, desarrollo, intercambio y comercialización de tecnologías, así como también promover e impulsar la generación de políticas positivas para el desarrollo de la Sociedad de la Información y Conocimiento en la región que permitan acelerar el mejoramiento en la calidad de vida de los pueblos. www.aleti.org

Dirección:

Piso 19, Torre Centro, Parque Boyacá, Av. Sucre, Los Dos Caminos, Caracas, Venezuela.

Teléfonos:

(+58-212) 285-6520 / 283-5511

www.cavedatos.net
www.cavedatos.org.ve
Twitter: twitter.com/Cavedatos
Facebook: facebook.com/Cavedatos
eMail: cavedatos@gmail.com

Figura 9. Dirección de empresa CAVEDATOS
Fuente: CAVEDATOS (2017)

CAPITULO V. DESARROLLO DE LOS OBJETIVOS DE LA INVESTIGACIÓN

El presente capítulo presenta los resultados de la investigación, detallando las actividades realizadas para alcanzar cada uno de los objetivos planteados, usando las herramientas de recolección de datos descritas en el Marco Metodológico de este Trabajo Especial de Grado.

Objetivo 1. Determinar los requisitos que exige la norma ISO/IEC 27001:2013 para la implementación de proyectos en certificación de empresas desarrolladoras de software

ISO/IEC 27001:2013 se divide en 14 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

- **Sección 0** – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
- **Sección 1** – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.
- **Sección 2** – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
- **Sección 3** – Términos y definiciones – de nuevo, hacen referencia a la norma ISO/IEC 27000.

- **Sección 4** – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
- **Sección 5** – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
- **Sección 6** – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
- **Sección 7** – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
- **Sección 8** – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
- **Sección 9** – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
- **Sección 10** – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).7

MARCO LEGAL

Una herramienta de la gestión estratégica para la protección de la información es la norma ISO/IEC 27001:2013, que se usa para lograr la certificación de una empresa u organización o ya sea para implementar las buenas prácticas de la seguridad de la información tanto en los aspectos internos como externos de la misma Cuando se implementa esta norma, consagra un conjunto de dominios con la finalidad de robustecer la seguridad sin que todos estos tengan un impacto jurídico Por la escasa legislación que existe se toma el enfoque a normas internacionales y nacionales.

La norma ISO/IEC 27001:2013 comprende 14 dominios a saber:

- A.5 Políticas de la seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad de los recursos humanos
- A.8 Gestión de activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con los proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de la seguridad de la información de la gestión de continuidad del negocio

- A.18 Cumplimiento

El propósito del presente objetivo es determinar los requisitos que permitan implementar un Sistema de Gestión de Seguridad de la Información aplicable a cualquier tipo de entidad, incluyendo el proceso de certificación del **ISO/IEC 27001:2013.**

Requisitos: Requisitos necesarios para la implementación de proyectos aplicando la Norma ISO/IEC 27001:2013 en certificación de Empresas Consultoras De Software.

Tabla N° 2. Requisitos para certificación de proyectos aplicando la norma ISO/IEC 27001:20013

ID	Método	Aplicabilidad
01	Formalización del Proyecto	Exponer ante la directiva beneficios, tiempos, recursos y áreas involucradas en esta implementación.
02	Análisis de Brecha (GAP)	Se usa un modelo de madurez con el propósito de ayudar a evaluar la seguridad de la información, a determinar en qué nivel o grado se encuentra y así tomar decisiones que permitan identificar las falencias que se tienen en un determinado nivel.
03	Determinación del alcance del SGSI	El alcance determinara, ubicaciones físicas y ciudades del Sistema de Gestión de Seguridad de la Información
04	Elaboración de la Política de Seguridad de la Información	-. Enfocado en el propósito de la organización; -. Incluye objetivos de seguridad de la información (o proporciona el marco de referencia para fijar los objetivos de seguridad de la información; -. Incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información;

ID	Método	Aplicabilidad
		-. Incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información.
05	Análisis y Gestión de Riesgos.	Esta actividad cuyo resultado nos va a dar información de dónde residen los problemas actuales o potenciales que tenemos que solucionar para alcanzar el nivel de seguridad deseado.
06	Información Documentada	Debe incluir: -. Información documentada requerida por el ISO/IEC 27001:2013; -. Información documentada determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.
07	Formación y Concientización	Indica que las personas que trabajan bajo el control de la organización deben ser conscientes de: -. La política de seguridad de información; -. Su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información.
08	Auditoria Interna	La organización debe conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información está en conformidad con los requisitos de la propia organización para su sistema de gestión de seguridad de la

ID	Método	Aplicabilidad
		información; y los requisitos del ISO/IEC 27001: 2013
09	Revisión por la alta Dirección	La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.
10	Proceso de Certificación	Se deberá seleccionar una entidad certificadora acreditada para realizar esta actividad, dicha entidad, deberá dimensionar la cantidad de auditores y horas/auditor sobre la base del alcance, cantidad del personal involucrado en la organización y sedes que abarca el SGSI.

Se identifica que:

-. La alta dirección tiene un rol protagónico y principal en el proceso de Seguridad de la Información, este rol permite la asignación de recursos, liderazgo del proyecto y adecuada implementación del SGSI.

-. Aún después de una adecuada implantación, se debe revisar el SGSI en intervalos planificados para detectar de una manera oportuna, alguna desviación del SGSI y mejorarlo en el tiempo.

-. No existe una receta mágica que permita asegurar en su totalidad los activos críticos de una organización, ni componentes tecnológicos ni normas que nos garanticen que todo irá bien, se debe considerar una serie de factores como la importancia que le damos a la seguridad en la organización, el apoyo y compromiso de la alta dirección, los recursos asignados, la propia experiencia y el lugar que tiene en nuestra agenda los temas relacionados a la Seguridad de la Información.

-. El factor humano es importante en la seguridad de la información, sensibilizarlos y entrenarlos en estos temas garantiza el apoyo y conocimiento en el proceso de aseguramiento de la información.

Para determinar si la empresa cumple con los requisitos exigidos para realizar la certificación de la norma ISO/IEC 27001: 2013 se decidió realizar un documento en donde pasando por cada uno de los dominios de control se verificara si la empresa cumple o no con lo solicitado por la norma. (Ver página siguiente).

Proceso a Revisar	Anexo A Dominio de Control 5	Fecha de Auditoria	26/04/2018 a 27/04/2018

Nombres de los Auditados
Gerente de Desarrollo de Software

Nombre de los Auditores
Pedro Perez

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Dominio	Objetivo de Control	Clausula	Descripción del control	Calificación	Obtenido	Esperado	Observaciones
5. Politicas de Seguridad	Directrices de la direccipon de seguridad de la información						
	5.1	5.1.1	Conjunto de politicas para la seguridad de la información	**Cumple**	5	5	La organización cuenta con un documento de politica de seguridad que es conocido por todos los procesos de la organización
	5.1	5.1.2	Revisión de las politicas para la seguridad de la información	**Cumple**	5	5	Las politicas de seguridad de la información son revisadas y actualizadas por lo menos dos veces en cada periodo anual.
				% Cumplimiento	100%	100%	

RESUMEN AUDITORIA	
Criterios	Total
Número de Preguntas	2
Número de Observaciones No Conformidades Menores	0
Número de No Conformidades Mayores	0
Número de Oportunidades de Mejora	0
Calificación Final	100%

Para la interpretación de la misma se detalla:

Interpretación: Para los 4 criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estará en la columna de “Obtenido” y será distribuido de la siguiente manera:

Cumple: Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera =1/ Número de Preguntas en el dominio, lo anterior también aplica para el criterio de “**Oportunidad de Mejora**”

No conformidad menor: Sera la mitad del valor esperado.

No conformidad mayor: En este caso el valor de la pregunta se registra con cero (0)

En la columna “Esperado” se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora.

Objetivo 2. Elaborar plan de auditoria para aplicar la norma ISO/IEC 27001:2013 en empresas consultoras de software.

Para la puesta en práctica del Sistema de Gestión de Seguridad de la Información, se debe definir un informe de auditoría interna del SGSI, para determinar el nivel de avance en la implementación de proyectos, controles y planes de acción al corto plazo, en la gestión del SGSI.

Para evaluar el nivel de cumplimiento de los controles implementados en los planes de tratamiento de riesgos, iniciativas de seguridad de la información, hasta la fecha actual del proceso de implementación y validar le evolución de la madurez de la organización.

Para garantizar el correcto funcionamiento y mantenimiento de un SGSI basado en la norma ISO/IEC 27001:2013, se hace necesario llevar a cabo auditorías internas cada cierto tiempo para poder comprobar que el sistema se encuentra en un estado idóneo.

Existen dos grandes tipos de auditorías internas:

- Gestión. Donde se supervisa el liderazgo, el contexto, etc.
- Controles. En este caso se auditan los 114 controles, normalmente se realiza por personal más experto y puede realizarse en años distintos.

La norma ISO 27001: Aspectos claves de su diseño e implantación

Básicamente, el principal motivo de que se realicen las auditorías internas periódicamente es poder determinar si los procedimientos del SGSI se encuentran conforme a: los requisitos de la norma, la legislación vigente en cada país o sector y los objetivos marcados por la Dirección para el propio sistema de gestión.

El plan de auditoría interna

En la planificación de la auditoría se debe contar con el nivel de importancia de los procesos y de las áreas que van a ser auditadas y, además, hay que tener en cuenta los resultados obtenidos de auditorías previas. También es necesario

definir los criterios utilizados durante la auditoría, el alcance, la frecuencia y los métodos utilizados.

Si se detectan problemas o desviaciones entre los objetivos de seguridad planteados y los resultados obtenidos, el equipo auditor comprueba si se están aplicando las medidas necesarias, proponiendo nuevas medidas en caso necesario.

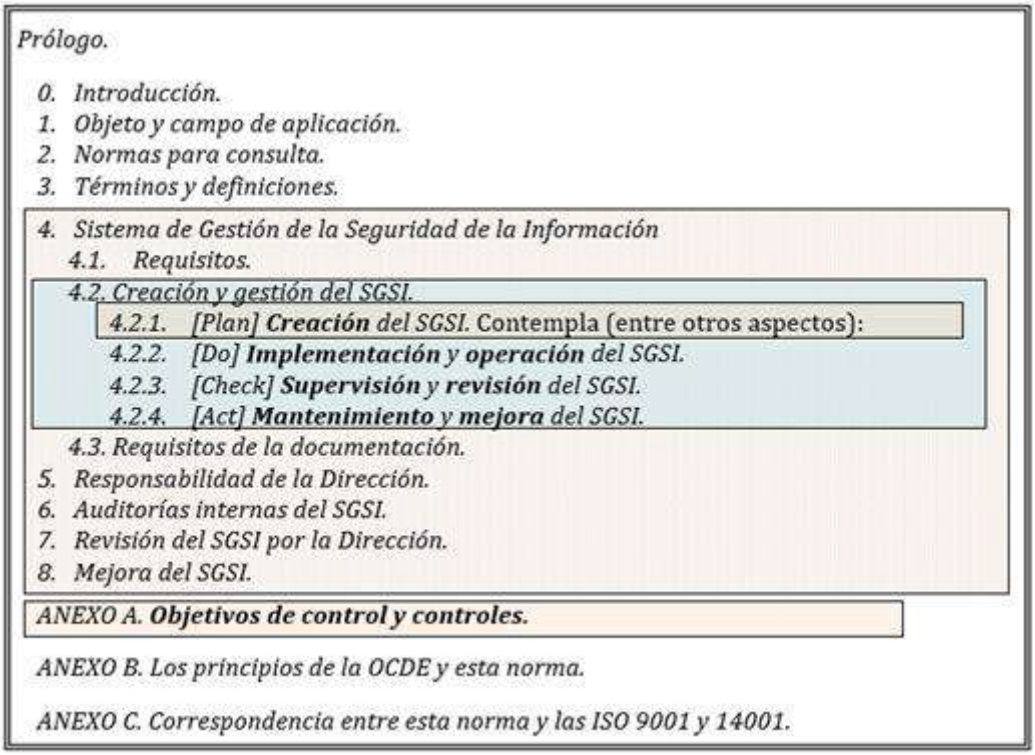


Figura 10. Estructura de la norma ISO/IEC 27001

ISO/ IEC 27001:2013 exige que el SGSI contemple los siguientes puntos:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.

- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses, se puede pasar a la fase de auditoría y certificación, que se muestra en la figura 5 y se desarrolla de la siguiente forma:

- Solicitud de la auditoría por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.
- Respuesta en forma de oferta por parte de la entidad certificadora.
- Compromiso.
- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.
- Pre-auditoría: opcionalmente, puede realizarse una auditoría previa que aporte información sobre la situación actual y oriente mejor sobre las posibilidades de superar la auditoría real.
- Fase 1 de la auditoría: no necesariamente tiene que ser in situ, puesto que se trata del análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en

la Fase 2. Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.

- Fase 2 de la auditoría: es la fase de detalle de la auditoría, en la que se revisan in situ las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. Finaliza con una reunión de cierre en la que se presenta el informe de auditoría.
- Certificación: en el caso de que se descubran durante la auditoría no conformidades graves, la organización deberá implantar acciones correctivas; una vez verificada dicha implantación o, directamente, en el caso de no haberse presentado no conformidades, el auditor podrá emitir un informe favorable y el SGSI de organización será certificado según ISO/ IEC 27001.
- Auditoría de seguimiento: semestral o, al menos, anualmente, debe realizarse una auditoría de mantenimiento; esta auditoría se centra, generalmente, en partes del sistema, dada su menor duración, y tiene como objetivo comprobar el uso del SGSI y fomentar y verificar la mejora continua.
- Auditoría de re-certificación: cada tres años, es necesario superar una auditoría de certificación formal completa como la descrita.

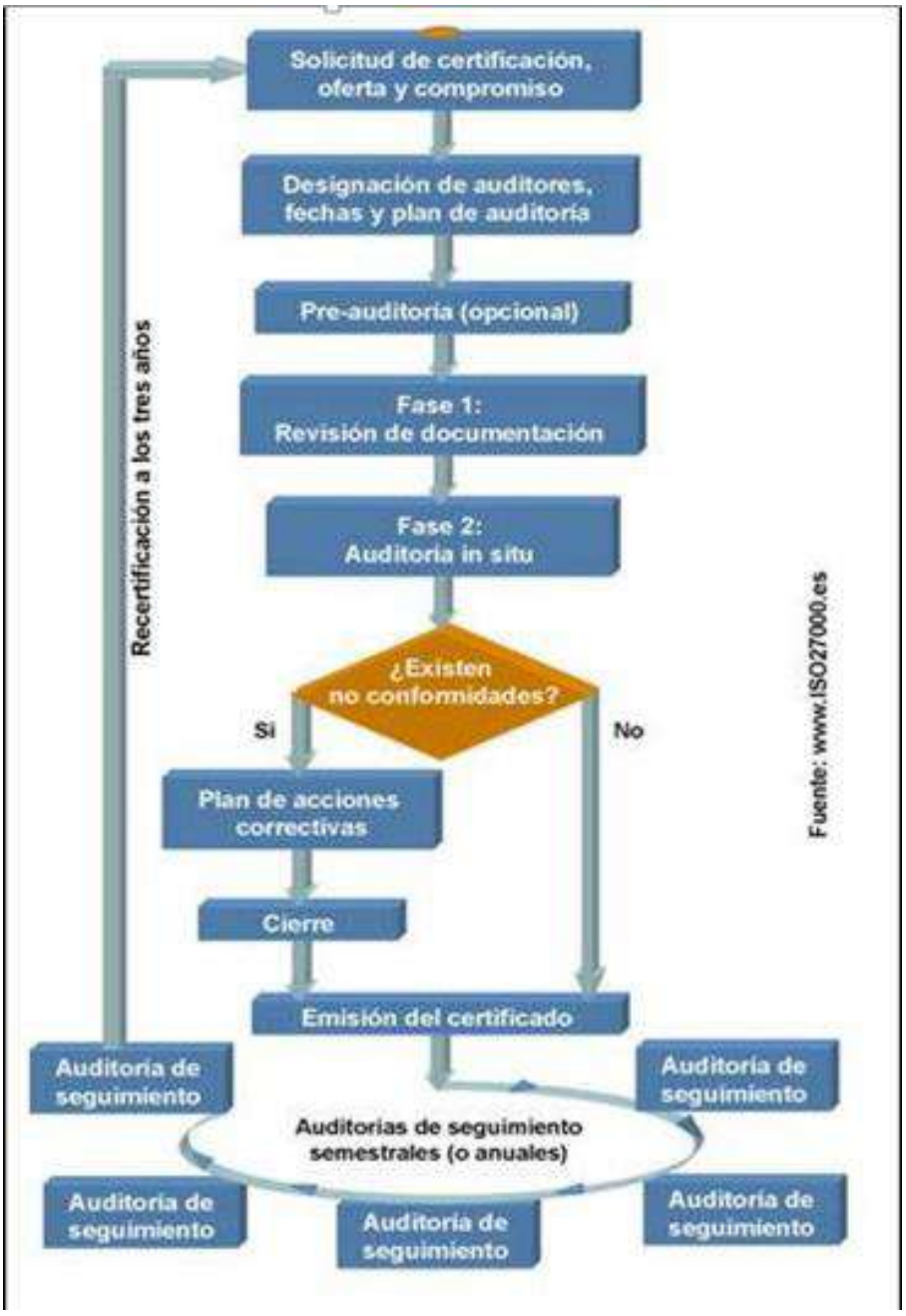


Figura 11. Proceso de auditoría de un SGSI.

Fuente: www.ISO27000.es

Para realizar la auditoria y determinar si la empresa cumple con los requisitos exigidos para realizar la certificación de la norma ISO/IEC 27001: 2013 se decidió realizar un documento en donde pasando por cada uno de los

dominios de control se verificara si la empresa cumple o no con lo solicitado por la norma. (Documento ubicado en el Anexo B).

Para la interpretación de la misma se detalla:

Interpretación: Para los 4 criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estará en la columna de"Obtenido" y será distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera =1/ Número de Preguntas en el dominio, lo anterior también aplica para el criterio de "**Oportunidad de Mejora**"
2. **No conformidad menor:** Sera la mitad del valor esperado.
3. **No conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna "Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora.

Objetivo 3. Elaborar el plan maestro para la implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en empresas desarrolladoras de software. En el desarrollo de este objetivo fue utilizado como referencia el modelo Plan Maestro de la Universidad de Bristol. A Continuación se presentan los apartados que contiene el Plan Maestro de Proyecto desarrollado:

I. Identificación del proyecto
II. Introducción
III. Objetivo del proyecto
IV. Inclusiones del alcance
V. Exclusiones del alcance
VI. Restricciones
VII. Plan de gestión de requisitos y cronogramas
VIII. Estructura desagregada de trabajo

IX. Unidades involucradas de la organización
X. Interesados
XI. Beneficios del proyecto
XII. Gobierno del proyecto
XIII. Plan de gestión de la calidad y mejoras del proceso
XIV. Plan de gestión de recursos humanos
XV. Plan de comunicaciones
XVI. Plan de gestión de Riesgos
XVII. Plan de adquisiciones
XVIII. Plan de gestión de interesados
XIX. Declaración final

El Plan de Migración desarrollado es genérico, por lo tanto presenta espacios en blanco que deben ser completados en caso de ser aplicado en alguna organización (ver Anexo C), así mismo lo referente a Interesados, Riesgo, Entorno y Unidades Internas involucradas deben ser evaluadas en cada organización.

CAPITULO VI. ANALISIS DE LOS RESULTADOS

En el presente capítulo se analizan los resultados obtenidos en los tres capítulos anteriores. En el capítulo V se construyó el desarrollo de los objetivos del trabajo especial de grado para realizar el Plan Maestro para implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en certificación de empresas consultoras de software en el que se pudo identificar lo siguiente:

1) Los anexos de la ISO 27001 incluyen información relevante sobre lo que no debe olvidarse para gestionar la seguridad de la información. Si bien esta gestión no está necesariamente ligada a la certificación de una norma particular, el hecho de conocer y entender las mejores prácticas existentes en el mercado da una visión completa del camino que debería seguirse.
2) Es importante que las empresas que utilicen este estándar como guía cumplan con los controle de dominio especificados en el Anexo A.

Posteriormente en el capítulo VI se desarrollaron los tres Objetivos Específicos, de estos se infiere lo siguiente:

1) ISO/IEC 27001:2013 se divide en 14 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma.
2) Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.
3) La norma ISO/IEC 27001:2013 comprende 14 dominios a saber:

- A.5 Políticas de la seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad de los recursos humanos
- A.8 Gestión de activos

- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con los proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de la seguridad de la información de la gestión de continuidad del negocio
- A.18 Cumplimiento

4) Para determinar si la empresa cumple con los requisitos exigidos para realizar la certificación de la norma ISO/IEC 27001: 2013 se realizó un documento en donde pasando por cada uno de los dominios de control se verificara si la empresa cumple o no con lo solicitado por la norma, ubicado en el anexo B.
5) Para garantizar el correcto funcionamiento y mantenimiento del SGSI basado en la norma ISO/IEC 27001:2013, se realizó un plan de auditorías interno para ser aplicado a las empresas que optan por la certificación de la norma, la cual debe ser realizada cada cierto tiempo para poder comprobar que el sistema se encuentra en un estado idóneo.
6) Se realizó un documento para la verificación correcta de la auditoria, ubicado en el anexo B.
7) El Plan Maestro aborda la planificación de las áreas del conocimiento de la gerencia de proyectos, sentando las bases para la ejecución del mismo.

El lienzo modelo de negocio permite representar de manera gráfica la propuesta para la empresa consultora, por medio de diferentes perspectivas, creando una visión estructurada de la empresa, disminuyendo incertidumbres y relacionando de manera rápida a los lectores con la idea de negocio que se maneja.

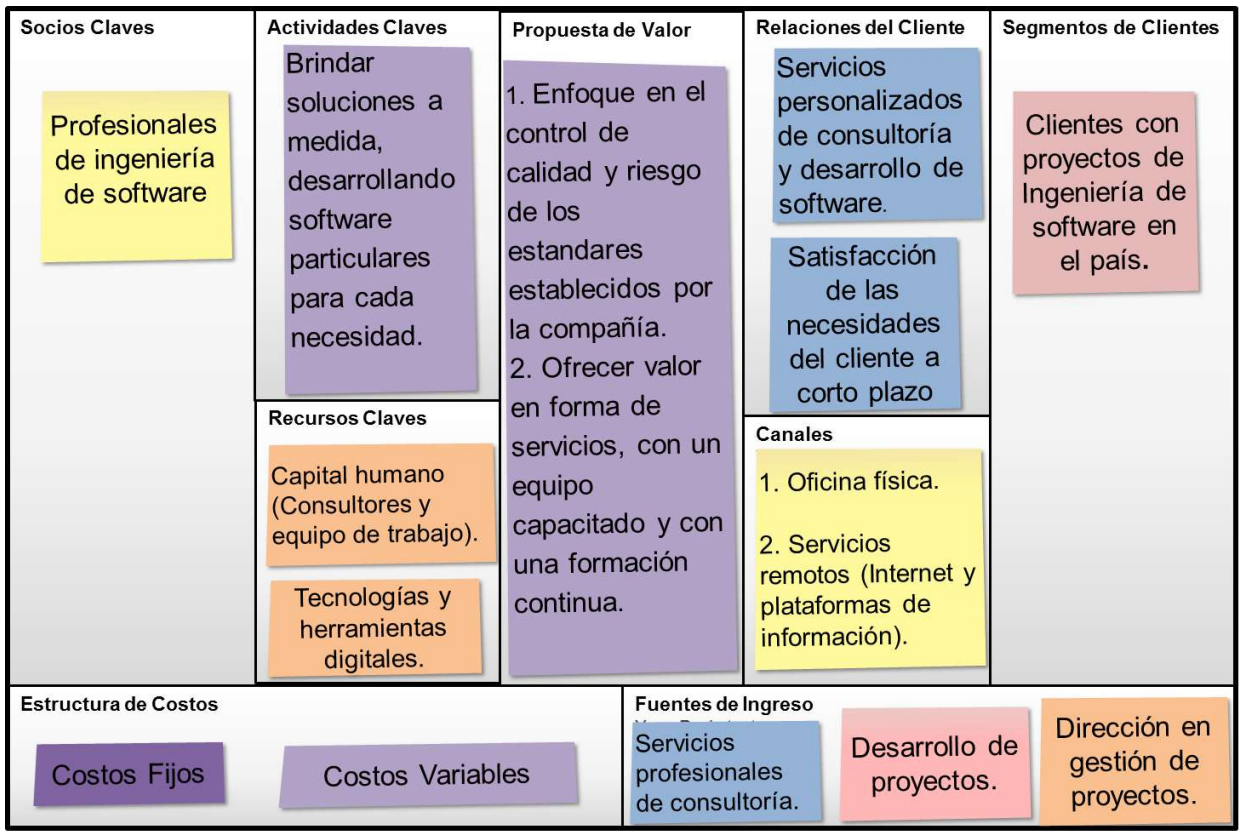


Figura 12. Lienzo modelo de negocios de la empresa consultora de software
Fuente: Osterwalder & Pigneur (2006)

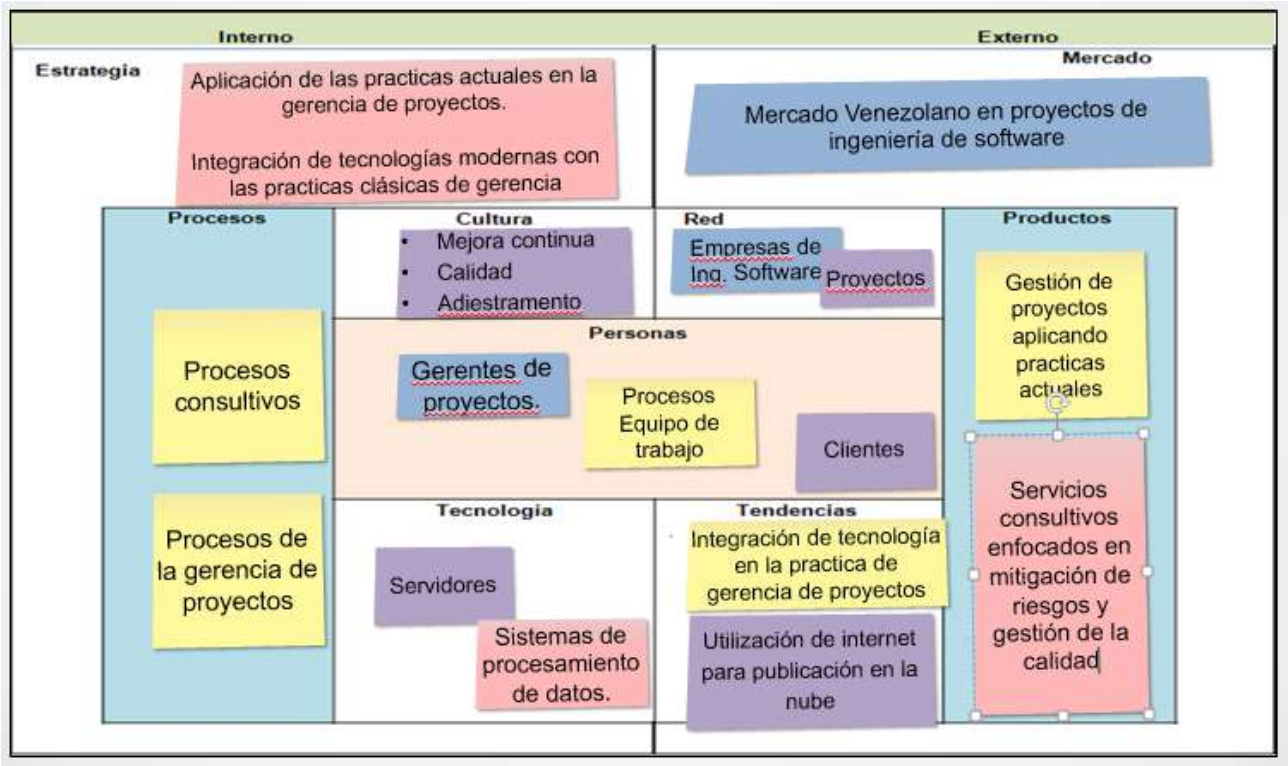


Figura 13. Lienzo de innovación del proyecto de la empresa consultora de software.
Fuente: Osterwalder & Pigneur (2006)

CAPITULO VII. LECCIONES APRENDIDAS

En este capítulo se presentan las lecciones aprendidas y oportunidades de mejora generada por la investigación, la documentación de las Lecciones Aprendidas es parte de la mejora continua y ayuda a futuros investigadores a conocer la causa raíz de problemas de futuros trabajos de investigación (University of Calgary, 2013).

- Definir el alcance del proyecto es la tarea más importante al realizar un Plan Maestro, ya que se delimitan claramente los entregables del proyecto y aún más importante se realizan las exclusiones de lo que no debe ser el en proyecto.
- El no planificar los tiempos de entrega puede ser un error costosísimo para la culminación de la certificación de empresas desarrolladoras de software aplicando la norma ISO/IEC 27001:2013.
- Las organizaciones que emprendan el proceso de certificación deben contar con personal suficiente y calificado para realizar las tareas asignadas. De lo contrario deberán contar con asesores externos que guíen el proceso.
- La correcta y acertada distribución de la información es esencial ya que será muchas las áreas o unidades internas de las organizaciones las que forman parte del proyecto.
- Mitigar los riesgos que puedan afectar la culminación exitosa del proyecto es fundamental, para ello la organización debe trabajar seriamente en los planes de contingencia.

CAPITULO VIII. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

La Norma ISO/IEC 27001:2013 es de gran importancia para diseñar un buen Sistema de Gestión Seguridad de la información SGSI para cualquier empresa ayudando a mitigar riesgos.

1. En el primer objetivo específico de la investigación, se concluye con que es indispensable determinar los requisitos exigidos por la norma ISO/IEC 27001:2013 para poder aplicar la certificación en empresas desarrolladoras de software, esto permitirá minimizar el margen de error al momento de iniciar una certificación, permitiendo que las empresas cuente con el documento para el inicio de su proyecto.

   Se debe destacar que las políticas de seguridad que se implementen en cualquier empresa se deben ajustar al estándar ISO/IEC 27001:2013.

   Es importante que para la implementación del SGSI se involucre al personal de la empresa dándoles las respectivas capacitaciones.

2. El segundo objetivo específico permite concluir, que es necesario la elaboración de un plan de auditoria debido a que a través de esto se podrá evidenciar de manera integral que el cumplimiento de los numerales sean aceptables para dar una mejor certificación a la norma.

   El desarrollo y mantenimiento de una política de gestión integrada permitirá enfocar y dar cumplimiento a todo el desarrollo de los procesos organizacionales.

   De igual manera el plan de auditoria ayuda a establecer el norte y el desarrollo de cada proceso de manera individual, mostrando cada una de sus actividades y las maneras de controlar y hacer seguimiento a ellas.

3. En el tercer objetivo se concluye, que la creación de un plan maestro es de suma importancia debido a que esta refleja cual será la estrategia a seguir por las empresas en el mediano plazo.

   La implementación de este plan maestro nos permitirá la planificación de los pasos fundamentales para la administración de la organización, debido a que este nos estructura el camino a seguir para el logro de los objetivos y su sustentabilidad en el tiempo.

   De igual forma se destaca que definir el alcance del proyecto se podría determinar como una de las tareas más importante al realizar en un Plan Maestro, ya que a través de ella se definen claramente los entregables del proyecto y aún más importante se realizan las exclusiones de lo que no debe ser.

RECOMENDACIONES

- Aplicar una metodología para la identificación de riesgos de Seguridad de la Información, apropiada para cada empresa.
- Establecer el enfoque por procesos que permita el correcto cometido y el control de cada uno de ellos manteniendo o mejorando la identificación de los elementos esenciales.
- Identificar los requisitos legales y reglamentarios y verificar su continuo cumplimiento, ya que a través de esto, pueden ser adaptadas nuevas metodologías para el control de la organización.
- Implementar las actividades y documentos diseñados en este proyecto para la certificación correcta del SGSI, que en cualquier momento que la organización decida, este material contribuirá para la acreditación o certificación del modelo implantado.

REFERENCIAS BIBLIOGRAFICAS

- Balestrini, M. (2006). Como se Elabora el Proyecto de Investigación (7ma ed.). Caracas (Venezuela): BL Consultores Asociados.
- Código de ética y conducta profesional del PMI. Project Management Institute. (2.010).
- Colegio de Ingenieros de Venezuela. (2014). Código de Ética Profesional. Obtenido de: http://www.civ.net.ve/uploaded_pdf/cep.pdf
- Constitución Bolivariana de Venezuela promulgada en Gaceta Oficial Nº 5.908 de fecha 19 de febrero de 2.009, Caracas Venezuela.
- Dennis, C. y Goldman, D (2013). "Journal of Internet Law. Data Security Laws and The Cybersecurity Debate". Volumen 17. Number 2. Editado por DLA PIPER Hernández, R., Fernández, C. y Baptista, M. (2010). Metodología de la Investigación (5ta ed.). México, D.F. (México): McGraw-Hill.
- Integrity IT (2011). Servicios de Consultoría y Auditoría TIC de Abstract System. Auditoría de Seguridad basada en las Normas ISO27001 e ISO27002.
- ISO/IEC 27000:2014 – Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Organización Internacional de Estándares (ISO).
- ISO 21500:2012- Guía de dirección de proyectos. Organización Internacional de Estándares (ISO).
- Ley Especial Contra Delitos Informáticos promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2.001 por la Asamblea Nacional, Caracas Venezuela.
- Ley Orgánica de Telecomunicaciones, promulgada 28 de febrero de 2001 y publicada en Gaceta Oficial No.37.148. Caracas Venezuela.
- Ley Orgánica de Ciencia, Tecnología e Innovación, Promulgada en Gaceta Oficial N° 38.242 de fecha 03 de Agosto de 2005. Caracas Venezuela.

- Ley Sobre Mensajes de Datos y Firmas Electrónicas promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2.001, por Decreto N° 1.024 – 10 de febrero de 2001, Caracas Venezuela.
- Project Management Institute, Inc. (2013). Guía de los Fundamentos de la Dirección de Proyectos (Guía del PMBOK®) (5ta ed.). Pennsylvania (EEUU): PMI.
- Tamayo y Tamayo, M. (2009). El Proceso de la Investigación Científica. México, D.F. (México): Editorial Limusa. 3ª Ed.
- Osterwalder, A. y Pigneur, Y. (2014). Diseño de propuesta de valor. Hoboken, New Jersy. (USA). Editorial: John Wiley & Sons.
- Disterer, Journal of Information Security (2013**).** "ISO / IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información"
- Gernot (2013) 13th IEEE International Symposium "Fortificación de la seguridad de la información por mapeo ontológico de ISO / IEC 27001Standard"
- Arroyo (2017). "Formulación de estrategias para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (pci-dss) de Bancaribe banco universal" (Trabajo Especial de Grado, para optar al Título de Especialista en Planificación, Desarrollo y Gestión de Proyectos, Universidad Monteávila, Caracas, Venezuela).
- León (2017). "Plan maestro del proyecto "migración de la norma iso 9001:2008 a la 9001:2015 caso: empresas de servicio en Venezuela" (Trabajo Especial de Grado, para optar al Título de Especialista en Gerencia de Proyectos, Universidad Católica Andrés Bello, Caracas, Venezuela).
- Kliem (1999) "Usando la Gerencia de Proyectos para Certificarse ISO 9000".
- Nieto (2013) "Plan de implementación de la ISO/IEC 27001:2013" (Trabajo de especialización en Gerencia y Desarrollo Organizacional, Universidad Simón Bolívar, Caracas, Venezuela).

- Salcedo, (2014) “Plan de implementación del SGSI basado en la norma ISO/IEC 27001:2013”. (Trabajo de especialización en Proyectos, Universidad de Cataluña, España).

ANEXO A

LISTA DE DOMINIOS CON SUS RESPECTIVOS CONTROLES DE LA NORAMA ISO/IEC 27001:2013.

A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información
A.5.1. 1 Políticas para la seguridad de la información
A.5.1. 2 Revisión de las Políticas para la seguridad información
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
A.6.1 Organización interna
A.6.1.1.Roles y responsabilidades para la seguridad de la información
A.6.1.2 Separación de deberes
A.6.1.3 Contacto con las autoridades
A.6.1.4 Contacto con grupo de interés social
A.6.1.5 Seguridad de la información en la gestión de proyectos
A.6.2 Dispositivos móviles y teletrabajo
A.6.2.1 Política para dispositivos móviles
A.6.2.2 Teletrabajo
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS
A.7.1 Antes de asumir el empleo
A.7.1.1 Selección
A.7.1.2 Términos y condiciones del empleo
A.7.2 Durante la ejecución del empleo
A.7.2.1 Responsabilidades de la dirección
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la

información
A.7.2.3 Proceso disciplinario
A.7.3Terminación y cambio de empleo
A.7.3.1Terminacion o cambio de responsabilidades de empleo
A.8 GESTION DE ACTIVOS
A.8.1 Responsabilidad por los activos
A.8.1.1 Inventario de Activos
A.8.1.2 Propiedad de los activos
A.8.1.3 Uso aceptable de los activos
A.8.1.4 Devolución de activos
A.8.2 Clasificación de la información
A.8.2.1 Clasificación de la información
A.8.2.2 Etiquetado de la información
A.8.2.3 Manejo de activos
A.8.3 Manejo de medios
A.8.3.1 Gestión de medios removibles
A.8.3.2 Disposición de los medios
A.8.3.3Transferencia de medio físicos
A.9 CONTROL DE ACCESO
A.9.1 Requisitos del negocio para el control de acceso
A.9.1.1 Política de control de acceso
A.9.1.2 Acceso a redes y a servicios de red

A.9.2 Gestión de acceso a usuarios
A.9.2.1 Registro y cancelación del registro de usuarios
A.9.2.2 Suministro de acceso de usuarios
A.9.2.3 Gestión de derechos de acceso privilegiado
A.9.2.4 Gestión de información de autenticación secreta de usuarios
A.9.2.5 Revisión de los derechos de acceso de usuarios
A.9.2.6 Retiro o ajuste de los derechos de acceso
A.9.3 Responsabilidades de los usuarios
A.9.3.1 Uso de la información de la autenticación secreta
A.9.4 Control de acceso a sistemas y aplicaciones
A.9.4.1 Restricción de acceso a la información
A.9.4.2 Procedimiento de ingreso seguro
A.9.4.3 Sistema de gestión de contraseñas
A.9.4.4 Uso de programas utilitarios privilegiados
A.9.4.5 Control de acceso a código fuente de programas
A.10 CRIPTOGRAFIA
A.10.1 Controles criptográficos
A.10.1.1 Políticas sobre uso de controles criptográficos
A.10.1.2 Gestión de llaves
A.11 SEGURIDAD FISICA Y DEL ENTORNO
A.11.1 Áreas seguras
A.11.1.1 Perímetro de seguridad Física
A.11.1.2 Controles de acceso físico

A.11.1.3 Seguridad de oficinas, recintos e instalaciones
A.11.1.4 Protección contra amenazas externas y ambientales
A.11.1.5 Trabajo en áreas seguras
A.11.1.6 áreas de despacho y carga
A.11.2 Equipos
A.11.2.1 Ubicación y protección de equipos
A.11.2.2 Servicios de suministros
A.11.2.3 Seguridad del Cableado
A.11.2.4 Mantenimiento de equipos
A.11.2.5 Retiro de activos
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
A.11.2.7 Disposición segura o reposición de equipos
A.11.2.8 Equipos de usuarios desatendidos
A.11.2.9 Política de escritorio limpio y pantalla limpia
A.12 SEGURIDAD DE LAS OPERACIONES
A.12.1Procedimientos operacionales y responsabilidades
A.12.1.1 Procedimientos de operación documentados
A.12.1.2 Gestión de cambios
A.12.1.3 Gestión de capacidad
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
A.12.2 Protección contra código malicioso
A.12.2.1 Controles contra códigos
A.12.3 Copias de respaldo

A.12.3.1 Respaldo de la información
A.12.4 Registros y seguimientos
A.12.4.1 Registro de eventos
A.12.4.2 Protección de la información de registro
A.12.4.3 Registros del operador y del administrador
A.12.4.4 Sincronización de relojes
A.12.5 Control de software operacional
A.12.5.1 Instalación de software en sistemas operativos
A.12.6 Gestión de la vulnerabilidad técnica
A.12.6.1 Gestión de las vulnerabilidades técnicas
A.12.6.2 Restricciones sobre las instalaciones de software
A.12.7 Consideraciones sobre las auditorias de sistemas de información
A.12.7.1 Controles de auditorías de sistemas de información
A.13 SEGURIDAD DE LAS COMUNICACIONES
A.13.1 Gestión de la seguridad de las redes
A.13.1.1 Controles de redes
A.13.1.2 Seguridad de los servicios de red
A.13.1.3 Separación en las redes
A.13.2 Transferencia de información
A.13.2.1 Políticas y procedimientos de transferencia de información
A.13.2.2 Acuerdo sobre la transferencia de información
A.13.2.3 Mensajería electrónica
A.13.2.4 Acuerdos de confidencialidad o de no divulgación

A.14 ADQUISION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
A.14.1 Requisitos de seguridad de los sistemas de información
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas
A.14.1.3 Protección de las transacciones de los servicios de las aplicaciones A.14.2 Seguridad en los procesos de desarrollo y soporte
A.14.2.1 Políticas de desarrollo seguro
A.14.2.2 Procedimientos de control de cambios en sistemas
A.14.2.3 Revisión técnica de las aplicaciones después de cambio en la plataforma de operación
A.14.2.4 Restricciones en los cambios a los paquetes de software
A.14.2.5 Principios de la construcción de sistemas seguros
A.14.2.6 Ambiente de desarrollo seguro
A.14.2.7 Desarrollo contratado externamente
A.14.2.8 Pruebas de seguridad de sistemas
A.14.2.9 Pruebas de aceptación de sistemas
A.14.3 Datos de prueba
A.14.3.1 Protección de datos de prueba
A.15 RELACIONES CON LOS PROVEEDORES
A.15.1 Seguridad de la información en las relaciones con los proveedores
A.15.1.1 Políticas de seguridad de la información para las operaciones con los proveedores
A.15.1.2 tratamiento de la seguridad dentro de los acuerdos con los proveedores A.15.1.3 Cadena de suministro de tecnología de información y comunicación

A.15.2 Gestión de la prestación de servicios de proveedores
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores
A.15.2.2 Gestión de cambios en los servicios de los proveedores
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información
A.16.1.1.Responsabilidades y procedimientos
A.16.1.2 Reporte de eventos de seguridad de la información
A.16.1.3 Reporte de debilidades de seguridad de la información
A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
A.16.1.5 Respuesta a incidentes de la seguridad de la información
A.16.1.6 Aprendizaje obtenido de los incidentes de la seguridad de la información A.16.1.7 Recolección de evidencias
A.17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO
A.17.1 Continuidad de seguridad de la información
A.17.1.1 Planificación de la continuidad de la seguridad de la información
A.17.1.2 implementación de la continuidad de la seguridad de la información
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A.17.2 Redundancias
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información

A.18 CUMPLIMIENTO
A.18.1 Cumplimiento de requisitos legales y contractuales
A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales A.18.1.2 Derechos de propiedad intelectual
A.18.1.3 Protección de registros
A.18.1.4 Privacidad y protección de información de datos personales
A.18.1.5 Reglamentación de controles criptográficos
A.18.2 Revisiones de seguridad de la información
A.18.2.1 Revisión independiente de la seguridad de la información
A.18.2.2 Cumplimiento con las políticas y normas de seguridad
A.18.2.3 Revisión del cumplimiento técnico

ANEXO B

Interpretación: Para los 4 criterios de Auditoria (Cumple, No Conformidad Menor, No Conformidad Mayor y Oportunidad de Mejora), el resultado de la calificación estará en la columna de"Obtenido" donde 5 expresa el valor máximo y 0 el valor mínimo y será distribuido de la siguiente manera:

1. **Cumple:** Sera el peso porcentual de cada pregunta y el valor esperado, se calculara de la siguiente manera =1/ Número de Preguntas en el dominio, lo anterior también aplica para el criterio de "**Oportunidad de Mejora**"
2. **No conformidad menor:** Sera la mitad del valor esperado.
3. **No conformidad mayor:** En este caso el valor de la pregunta se registra con cero (0)

En la columna "Esperado" se estiman las preguntas que son tenidas en cuenta para la evaluación y su sumatoria significa que es la máxima puntuación que se puede obtener si todos los criterios cumplen y/o son oportunidades de mejora.

Proceso a Auditar	Dominio 5	Fecha de Auditoria	26/04/2018 a 27/04/2018

Criterios de Auditoria
Cumple
No Conformidad Menor
No Conformidad Mayor
Oportunidad de Mejora

Nombres de los Auditados
Gerente de Desarrollo de Software

Nombre de los Auditores
Pedro Perez

Dominio	Objetivo de Control	Clausula	Descripción del control	Calificación	Obtenido	Esperado	Observaciones
5. Politicas de Seguridad	Directrices de la direccipon de seguridad de la información						
	5.1	5.1.1	Conjunto de politicas para la seguridad de la información	**Cumple**	5	5	La organización cuenta con un documento de politica de seguridad que es conocido por todos los procesos de la organización
	5.1	5.1.2	Revisión de las politicas para la seguridad de la información	**Cumple**	5	5	Las politicas de seguridad de la información son revisadas y actuakizadas por lo menos dos veces en cada periodo annual.
				% Cumplimiento	100%	100%	

RESUMEN AUDITORIA	
Criterios	Total
Número de Preguntas	2
Número de Observaciones No Conformidades Menores	0
Número de No Conformidades Mayores	0
Número de Oportunidades de Mejora	0
Calificación Final	100%

ANEXO C

PLAN MAESTRO DEL PROYECTO

Histórico de Revisión

Descripción de la Revisión	Revisión	Fecha	Responsable

Lista de Distribución

Copia Controlada	Revisión	Fecha	Nº Área a la que pertenece

Contenido

IDENTIFICACIÓN DEL PROYECTO

Plan Maestro para implementación de proyectos aplicando la norma ISO/IEC 27001:2013 en certificación de la empresa consultora de software

_____

INTRODUCCIÓN

Todas las normas ISO son revisadas cada 5 años, para establecer si es necesaria una actualización. La norma ISO 27001 fue publicada por primera vez en 2005 y luego fue revisada en 2013; por lo tanto, la versión válida actual es la ISO/IEC 27001:2013.Los cambios más importantes de la revisión 2013 están relacionados con la estructura de la parte principal de la norma, las partes interesadas, los objetivos, el monitoreo y la medición. Todos estos cambios en realidad no modificaron mucho la norma en su conjunto, su filosofía principal sigue centrándose en la evaluación y tratamiento de riesgos y se mantienen las mismas fases del ciclo de Planificación, Implementación, Revisión y Mantenimiento (PDCA, por sus siglas en inglés).

Esta nueva revisión de la norma es más fácil de leer y comprender y es mucho más sencilla de integrar con otras normas de gestión como ISO 9001, ISO 22301, etc. El proyecto tiene como propósito certificar empresas consultoras de software a través de la aplicación de la norma ISO/IEC 27001:2013 dicha norma ayuda a gestionar la seguridad de la información en una empresa y proteger la confidencialidad, integridad y disponibilidad de la información. ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento

El presente documento constituye el compromiso del equipo del proyecto y de la dirección, cualquier cambio significativo en el material contenido en el Plan

maestro del proyecto deberá ser sometido a aprobación del gerente y patrocinador del proyecto.

1. OBJETIVO DEL PROYECTO

Obtener Certificación de la norma ISO/IEC 27001:2013 para la empresa consultora de software _____

2. INCLUSIONES DEL ALCANCE

El proyecto incluye la capacitación del personal en las nuevas versiones de la Norma ISO/IEC 27001:2013, implementación de acciones para cerrar la brecha existente entre el cumplimiento de los requisitos de la norma, auditoría de primera parte del Sistema de Gestión de Seguridad de la Información, tratamiento de no conformidades derivadas de auditoría de primera parte y solicitud de auditoría de certificación al ente certificador.

3. EXCLUSIONES DEL ALCANCE

El proyecto no incluye análisis de brecha en el cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013, (previo a la iniciación del proyecto) .

4. RESTRICCIONES

4.1 La implementación del Sistema de Gestión de Seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013 en certificación de empresas consultoras de software debe cumplir con las 11 secciones y el anexo A de la norma, las secciones de la 4 a l 10 deben ser aplicadas de manera obligatoria lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma.

4.2 El costo del proyecto no deberá superar el 50% de lo establecido en el presupuesto de gastos de la organización.

4.3 El Sistema de Gestión de Seguridad de la información (SGSI) de _____ cumplirá con los requisitos de la Norma ISO/IEC 27001:2013.

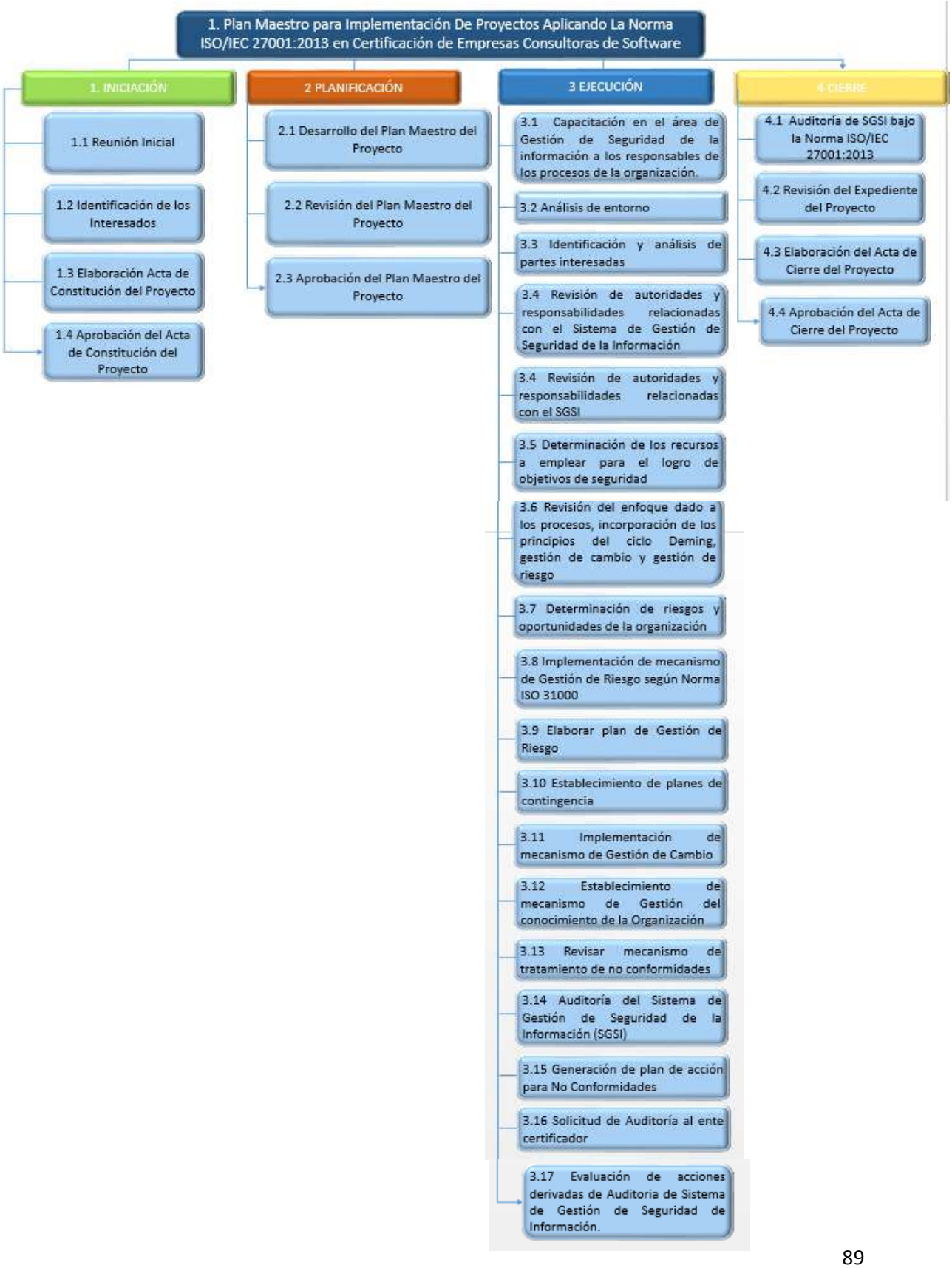
5. PLAN DE GESTIÓN DE REQUISITOS Y CRONOGRAMAS

Requisitos	Entregable	Fecha tope	Responsables	Aprobado
- Realización de talleres de actualización de la Norma ISO/IEC 27001:2013. - Capacitación en el área de Gestión de Seguridad de la información a los responsables de los procesos de la organización. - Actualización de vocabulario de acuerdo con la Norma ISO/IEC 27001:2013.	- Programa de desarrollo de competencias en el área de seguridad de la información.	30/04/2018	Gerente de Talento Humano	Gerente de Proyecto
- Identificación de partes interesadas - Establecimiento de contribución, legitimidad, compromiso, influencia y necesidad de participación de cada parte interesada. - Análisis de los aspectos tecnológicos, normativo, económico- financiero, social, de mercado y político del entorno de la organización.	- Análisis de partes interesadas	01/05/2018	Gerente de Administración	Gerente de Proyecto
- Revisión del enfoque dado a los procesos - Incorporación de los principios del Ciclo de Deming - Incorporación de los principios del Ciclo de Deming	Mapa de procesos	08/05/2018	Gerente de Operaciones	Gerente de Proyecto
- Implementación de mecanismo de Gestión de Riesgos según	- Plan de acciones para	02/05/2018	Gerente de Administración	Gerente de Proyecto

Norma ISO 31000 - Determinación de riesgos y oportunidades de la organización - Elaborar plan de gestión de riesgos - Elaborar plan de acciones para abordar oportunidades y riesgos (sustitución de acciones preventivas) - Incorporar gestión de riesgos a procesos relacionados con la satisfacción del cliente - Incorporar las partes interesadas como insumo en la gestión de riesgos	abordar oportunidades y riesgos			
- Implementación de mecanismo de Gestión de Cambios	- Procedimiento para la gestión de cambios	18/05/2018	Gerente de Calidad	Gerente de Proyectos
- Determinación de los recursos a emplear para el logro de objetivos de la calidad, fechas tope, responsables y mecanismos de evaluación de resultados - Revisión de autoridades y responsabilidades relacionadas con el Sistema de Gestión de la Calidad - Establecimiento de mecanismo de Gestión del conocimiento de la organización	- Matriz de recursos para el logro de objetivos de la calidad - Matriz de responsabilidades y autoridades - Procedimiento para gestión de conocimientos	19/05/2018	Gerente de Talento Humano	Gerente de Proyecto
- Inclusión de factores sociales y psicológicos en la gestión de medio ambiente para la operación de los procesos				

- Establecimiento de planes de contingencia cuando no sea posible cumplir con los requisitos del cliente	- Revisión de procedimientos relacionados con cumplimiento de requisitos de los clientes	25/05/2018	Gerente de la Calidad	Gerente de Proyectos
- Revisión de mecanismo de tratamiento de no conformidades e inclusión de modificaciones en la planificación, riesgos y oportunidades cuando se requiera - Inclusión de la evaluación de la eficacia de acciones para abordar riesgos y oportunidades en mecanismo de revisión de resultados del Sistema de Gestión de Seguridad de la información	Revisión de mecanismos de Sistemas de Gestión de Seguridad de la información	11/06/2018	Gerente de Seguridad de datos	Gerente de Proyectos
- Auditoría de primera parte -Tratamiento de no conformidades - Solicitud de Auditoría al ente certificador	-Informe de Auditoría - Plan de acción de no conformidades (incluidos resultados)	12/09/2018	Gerente de la Calidad	Gerente de Proyectos.
Auditoría de certificación	Certificación ISO/IEC 27001:2013	15/10/2018	Gerente de la Calidad	Gerente de Proyectos.
Elaborado por: Argelys Marquina		Cargo: Gerente de Proyecto		
Versión 1		Fecha: 18/04/2018		

6. ESTRUCTURA DESAGREGADA DE TRABAJO



7. UNIDADES INVOLUCRADAS DE LA ORGANIZACIÓN

7.1 Capital Humano

7.2 Investigación

7.3 Tecnología

7.4 Administración

7.5 Calidad

7.6 Operaciones

7.7 Atención al cliente

8. INTERESADOS

8.1 Propietarios: accionistas

8.2 Clientes: usuarios directos e indirectos del servicio

8.3 Empleados: colaboradores, exempleados, candidatos a cargos, directivos

8.4 Industria: Empresas de Tecnologías de la Información, asociaciones gremiales, proveedores.

8.5 Comunidad: asociaciones de vecinos

8.6 Medio ambiente: Recursos naturales, ecologistas, organismos no gubernamentales

8.7 Organismos gubernamentales: ministerios, alcaldía, gobernaciones

8.8 Sociedad civil organizada: colegios de profesionales

9. BENEFICIOS DEL PROYECTO

9.1 Ventaja competitiva

9.2 Reconocimiento nacional e internacional

9.3 Reducción de costos

9.4 Capacidad de reaccionar de manera adecuada ante situaciones adversas

9.5 Mayor capacidad para abordar oportunidades

9.6 Mayor capacidad para la evaluación de riesgos

10. GOBIERNO DEL PROYECTO

El equipo de proyecto conformado por: Gerente de Talento Humano, Gerente de Administración, Gerente de operaciones, Gerente de la Calidad, Gerente de Tecnología y Gerente de Proyectos se reunirá mensualmente para informar sobre el progreso, revisar las acciones y los riesgos del proyecto. El equipo del proyecto por excepción se reunirá en otros momentos en que se necesiten decisiones clave para progresar.

El Gerente del Proyecto producirá reportes mensuales destacados y los pondrá a disposición de las partes interesadas.

11. PLAN DE GESTIÓN DE LA CALIDAD Y MEJORAS DEL PROCESO

Atributo de la Calidad	Objetivo de la Calidad	Métrica a utilizar	Frecuencia, momento de medición y fecha de reporte	Acciones de contingencia
- Calidad de planes de formación	- El 100% del personal evaluado debe aprobar - Mínimo aceptable: 90% (primera evaluación) 100% en segunda evaluación	- Evaluación de 50 preguntas con un valor de 1 punto cada una - La evaluación se aprobará con 40 puntos	Frecuencia: Única Medición: 03/04/2018 05/04/2018	- Reinducción en puntos débiles de la evaluación - Reevaluación
- Eficacia del Plan de gestión de requisitos	- Eficacia 1 en la gestión de requisitos y cronogramas - Mínimo aceptable 0,8	- N° de requisitos cumplidos/N° de requisitos planteados - N° de requisitos cumplidos en el tiempo planificado/N° de requisitos planteados	- Frecuencia: bimestral - Medición: 10/04/2018 10/05/2018 10/06/2018 10/07/2018	Análisis de causa raíz, implementación de acciones correctivas
Eficiencia del Plan	- Eficiencia 100% en	-(N° requisitos	- Frecuencia:	- Análisis de

de Gestión de Costos	plan de gestión de cronogramas y costos - Mínimo aceptable 0,8	cumplidos (Costos ejecutados / tiempo de ejecución))/ N° requisitos planteados/(Costos planteados * tiempo planteado)	bimestral - Medición: 10/04/2018 10/05/2018 10/06/2018 10/07/2018	causa raíz, implementación de acciones correctivas
Eficacia en el cumplimiento de los requisitos de la Norma ISO 9001:2015.			- Frecuencia: única - Medición: 10/06/2018	- Análisis de causa raíz, plan de acciones y elaboración de nuevo cronograma con requisitos no cumplidos
Elaborado por: Argelys Marquina		Cargo: Gerente de Proyecto		
Versión 1		Fecha: 27/04/2018		

12. PLAN DE GESTIÓN DE RECURSOS HUMANOS

Nombre del cargo: Gerente de proyecto
Rol dentro del proyecto: Definir, controlar y gestionar el proyecto
Responsabilidades: - Solicitar aprobación de presupuesto al patrocinador del proyecto cuando los costos excedan más del 50% de lo presupuestado - Resolver conflictos presentados durante la ejecución del proyecto - Monitorear el proyecto - Gestionar los cambios del proyecto
Autoridades: - Asignar y/o desincorporar personal al proyecto - Autorizar excesos de gastos planificados hasta un 50% sobre lo presupuestado
Funciones: - Elaborar Acta de constitución del proyecto

- Iniciar el proyecto - Aprobar el plan del proyecto - Cerrar el proyecto - Planificar los cambios del proyecto
Reporta a: Patrocinador del proyecto
Revisa a: Todo el equipo del proyecto

Nombre del cargo: Gerente de Talento Humano
Rol dentro del proyecto: Gestionar el recurso humano del proyecto
Responsabilidades: Gestionar la capacitación de colaboradores del proyecto
Autoridades: Asignar y reasignar actividades sobre la base de la planificación del proyecto
Funciones: Elaborar y monitorear el plan de capacitación del proyecto - Determinar el recurso humano a emplear para el logro de objetivos de la calidad - Implementar acciones para la capitalización del conocimiento derivado de la ejecución del proyecto - Revisar autoridades y responsabilidades relacionadas con el SGSI - Establecer mecanismo de gestión del conocimiento de la organización - Gestionar factores sociales y psicológico del medio ambiente de la organización
Reporta a: Patrocinador del proyecto
Revisa a: Todo el equipo del proyecto

Nombre del cargo: Gerente de Operaciones
Rol dentro del proyecto: Definir, gestionar y controlar los procesos de la organización relacionados con el proyecto
Responsabilidades: Gestionar los procesos involucrados en la ejecución del proyecto
Autoridades: - Diseñar y rediseñar procesos sobre la base de la planificación del proyecto
Funciones: - Revisar el enfoque dado a los proyectos - Incorporar los principios del ciclo de Deming a los procesos de la organización
Reporta a: Gerente de proyecto
Revisa a: Colaboradores adscritos al departamento de Operaciones

Nombre del cargo: Gerente de Administración
Rol dentro del proyecto: Administrar de manera efectiva los recursos del proyecto
Responsabilidades: Analizar el entorno y partes interesadas de la organización
Autoridades: - Asignar y reasignar actividades sobre la base de la planificación del proyecto
Funciones: Implementar mecanismo de gestión de riesgos • Determinar riesgos y oportunidades de la organización • Elaborar plan de gestión de riesgos • Elaborar plan de acciones para abordar oportunidades y riesgos • Incorporar gestión de riesgos a procesos relacionados con satisfacción de

clientes • Gestionar factores sociales y psicológico del medio ambiente de la organización
Reporta a: Gerente de proyecto
Revisa a: Colaboradores adscritos al departamento de Administración

Nombre del cargo: Colaboradores
Rol dentro del proyecto: Ejecutar actividades asignadas por los gerente involucrados en el proyectos
Responsabilidades: Cumplir los requisitos establecidos en el plan maestro de proyecto
Funciones: - Reportar periódicamente resultados de actividades del proyecto a los gerentes involucrados - Documentar información del proyecto
Reporta a: Gerentes involucrados en el proyecto
Revisa a: Colaboradores adscritos al cargo

Nombre del cargo: Gerente de la Calidad
Rol dentro del proyecto: Lograr el cumplimiento de los objetivos de la calidad del proyecto
Responsabilidades: - Monitorear el Plan de gestión de la calidad y mejoras del proyecto - Llevar a cabo planes de contingencia detallados en el Plan de gestión de la calidad y mejoras del proyecto
Autoridades:

- Emprender análisis e investigaciones correspondientes ante desviaciones de los procesos involucrados en el proyecto - Rechazar las salidas de las actividades involucradas en el proyecto cuando estas no cumplan con los requisitos de la calidad
Funciones: - Establecer planes de contingencia para casos en que no sea posible cumplir con los requisitos del cliente - Revisar mecanismos para el tratamiento de no conformidades e incluir modificaciones en la planificación , riesgos y oportunidades cuando sea requerido - Incluir la evaluación de la eficacia de acciones para abordar riesgos y oportunidades en mecanismos de revisión de resultados del SGC - Planificar la auditoría de primera parte - Gestionar plan de acción para tratamiento de no conformidades - Solicitar auditoría al ente certificador
Reporta a: Gerentes involucrados en el proyecto
Revisa a: Colaboradores involucrados en el proyecto

13. PLAN DE GESTIÓN DE LAS COMUNICACIONES

13.1 Idioma de las comunicaciones: ESPAÑOL

13.2 Distribución de la comunicación

Qué comunicar	**Motivo de la distribución**	**Frecuencia de distribución**	**Responsable de comunicar**	**A quien comunicar**	**Medios empleados para la comunicación**
1. Plan maestro del proyecto	1. Líneas de base del proyecto	1. Una vez sean emitidos	Gerente de proyecto	Equipo del proyecto	Reunión
2. Acta de constitución del proyecto	2.Descripción de alto nivel del proyecto	2. Una vez sean emitidos	Gerente de proyecto	Patrocinador del proyecto y equipo del proyecto	Reunión

3.Informes de avances de proyecto	3. Status del proyecto	3. Bimensual	Gerente de proyecto	Patrocinador del proyecto y equipo del proyecto	Correo electrónico
4. Información documentada relacionada con el proyecto	4.Documentación controlada del proyecto	4. Una vez sean emitidos	Gerente de la Calidad	Equipo del proyecto	Reunión y/o correo electrónico
5. Planes de acción	5. Detalles acerca de las responsabilidades en cada acción	5. Una vez sean emitidos	Gerente de proyecto	Colaboradores involucrados en el proyecto	Reunión
6. Revisiones de documentos del proyecto	6. Actualizaciones sobre la base de los resultados de la ejecución del proyecto	6. Una vez sean emitidos	Gerente de proyecto	Equipo del proyecto	Reunión
Elaborado por: Argelys Marquina			Cargo: Gerente de proyecto		
Versión: 1			Fecha: 17/05/2017		

13.3 Plan de comunicación por interesados

Interesados	Qué comunicar	Medios empleados para la comunicación	Responsable de Comunicar	Motivos para comunicarles
1. Accionistas	1. Acta de constitución, Plan maestro, Informes de avances, Certificación	1. Reuniones, correos electrónicos	Gerente de proyecto	Proporcionar las bases del proyecto e informar el status durante toda la ejecución del proyecto
2. Usuarios y contratantes del servicio	2. Certificaciones de calidad que la empresa posee y está próxima a tener	2. Carteleras, redes sociales, correos electrónicos	Gerente de la Calidad	Hacer del conocimiento del cliente que la organización está en capacidad de cumplir sus requisitos
3.Colaboradores	3. Planes de acción donde estén involucrados, requisitos del proyecto, plazos de tiempo,	3. Reuniones Correos electrónicos	Gerente de proyecto y Gerentes de su	Toma de conciencia de sus responsabilidades y autoridades en el

	responsabilidades y autoridades		área	proyecto
4. Industria	4. Objetivo del proyecto	4. Correos electrónicos	Gerente de Proyecto	Liderazgo en la industria
Elaborado por: Argelys Marquina			Cargo: Gerente de Proyectos	
Versión: 1			Fecha: 19/04/2018	

14. PLAN DE GESTIÓN DE LOS RIESGOS

14.1 Metodología

La metodología a utilizar es MAGERIT para el análisis de riesgo del proyecto.

El análisis de riesgos propuesto por MAGERIT es una aproximación metódica que permite determinar el riesgo siguiendo los siguientes pasos:

- Determinar los activos relevantes para la empresa.
- Determinar las amenazas a la que están expuestos aquellos activos.
- Estimar el impacto, definido como el daño sobre el activo, si se llega a concretar la amenaza.
- Valorar dichos activos en función del coste que supondría para la empresa recuperarse ante un problema de disponibilidad, integridad o confidencialidad de información.
- Valorar las amenazas potenciales.
- Estimar el riesgo

La misma presenta los siguientes objetivos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

RIESGO	POSIBLE CAUSA	EFECTO				
Que los costos de migración superen el presupuesto destinado	Inflación, necesidad de emplear recursos del exterior (auditores, capacitaciones), presupuesto limitado, aumentos en beneficios salariales vía decretos ejecutivos, regulación de precios. Falla en el cálculo de los recurso	Imposibilidad de cumplir la planificación efectuada para la migración a la nueva Norma				
Personal poco motivado	Frustración del recurso humano por el entorno (variables socioeconómicas), mala selección del personal asignado al proyecto	Demoras en la ejecución de las actividades planificadas, impacto negativo en la calidad del trabajo realizado				
Incumplimiento del SGC con el estándar ISO/IEC 27001:2013	Recurso humano sin las competencias necesarias, alta rotación del personal, poca oferta local de recurso humano especializado , nuevos conceptos, poca experticia con el nuevo estándar	Desconocimiento del nuevo estándar por parte del recurso humano seleccionado para el proyecto				

15. PLAN DE GESTIÓN DE ADQUISICIONES

Producto o servicio a adquirir	Tipo de contratación	Procedimiento de contratación	Responsable de contratación	Proveedores preseleccionados
Capacitaciones en el área de Calidad	Por módulos (3)	Procedimiento de compras de la organización	Gerente de la Calidad	- MLA Consultores - Fondonorma - Bureau Veritas
Auditoría de primera parte	Por contrato	Procedimiento de compras de la organización	Gerente de la Calidad	- MLA Consultores -Oyaga consultores - TBR consult

Auditoría de certificación	Por contrato	Procedimiento de compras de la organización	Gerente de la Calidad	- Fondonorma - Bureau Veritas

16. PLAN DE GESTIÓN DE INTERESADOS

	Contribución Tienen la información, experticia, recursos o experiencia que puede ser de utilidad para la empresa	**Legitimidad** Tienen un correcto proceder con respecto a lo establecido	**Disposición al Compromiso** Están dispuestos a comprometerse con la Organización	**Influencia** Contribuyen con el desarrollo de la Organización	**Necesidad de Participación** Si no se tomaran en cuenta en el proceso, podrían deslegitimizarlo
Propietarios Accionistas	Alta	Alta	Alta	Alta	Alta
Clientes Usuarios del servicio, contratantes del servicio	Media	Media	Baja	Alta	Alta
Colaboradores Colaboradores, exempleados, candidatos a cargos, departamento de apoyo, directivos	Alta	Alta	Alta	Alta	Alta
Industria Proveedores, Ente Certificador, Competidores, Líderes de	Media	Media	Baja	Media	Media

opinión					
Comunidad Comunidad, asociación de vecinos	Baja	Baja	Baja	Baja	Baja
Medio Ambiente Recursos naturales, ecologistas, ONGs	Baja	Alta	Media	Alta	Alta
Entes Gubernamentales Alcaldía, Gobernación, Ministerios	Baja	Alta	Baja	Alta	Alta
Sociedad Civil Organizada Colegio de Profesionales	Media	Alta	Media	Alta	Alta

17. DECLARACIÓN FINAL

Los abajo firmantes hemos leído el presente plan y estamos de acuerdo con los términos y condiciones en el descrito, y asumimos una posición de compromiso y apoyo al proyecto y al equipo de trabajo para lograr el objetivo planteado

Nombre	Cargo	Fecha