Diseño de un sistema integrado de gestión basado en las normas ISO 9001:2015 e ISO 27001:2013 para la empresa La Casa del Ingeniero LCI.

Cohorte N° 34

Autores

Cristian Yohan Cárdenas Herrera

Dayron Yemmery Efrén Higuera Soto

Director Trabajo de Grado

Ing. Lina Patricia Coy Calixto

Escuela Colombiana de Ingeniería Julio Garavito
Programa de Ingeniería Industrial
Especialización Gestión Integrada QHSE
Cohorte 34
Bogotá D.C., Colombia, Mayo 2016.

Publicado en 2016 por la Escuela Colombiana de Ingeniería “Julio Garavito”. Avenida 13 No 205-59 Bogotá. Colombia
TEL: +57 – 1 668 36 00, e-mail: espeqhse@escuelaing.edu.co

Reconocimientos de Cristian Cárdenas Herrera

Agradezco a LA CASA DEL INGENIERO, por abrirnos las puertas de su empresa y aplicar el diseño de este Sistema Integrado de Gestión, igualmente por darnos el acceso a su información y generar los entregables que son el insumo para lograr la implementación de este sistema dentro de la organización.

Igualmente a mi familia, docentes y compañeros con los que compartí y pude aprender algo importante de cada uno de ellos.

Reconocimientos de Dayron Higuera Soto

Agradezco a Dios por darme la oportunidad de escalar un peldaño más en mi formación como profesional, además de poner a mi esposa Leydi, mis padres Alba, Luis y mis maestros de pregrado Leidy Rocío y Egidio por apoyarme y creer siempre que sí se puede, y que cada sueño es posible si se es persistente, sin dejar caer los brazos por mas cansados que parezcan. Gracias a ellos y todas las personas que se presentaron en mi camino para ayudar a culminar una etapa que solo Dios sabe cuánto anhelaba.

Abstract

Title: Integrated Management System Design, based on ISO 9001: 2015 and ISO 27001: 2013 for La Casa del Ingeniero LCI .

Author: Cristian Yohan Cárdenas Herrera
Dayron Yemmery Efrén Higuera Soto

Key Words: Quality, information security, integrated management system, management models..

Content: Nowadays, organizations and their production team are not only responsible for fulfilling requirements or requests from their clients to get a product or service, but also they are responsible for keeping all personal information safe from malicious usages. In some cases, this is also required by law. Taking Into account those needs, quality and information security (InfoSec) are a big priority when it comes to software's, webs apps, mobiles and digital content. Looking at those needs presented by La Casa Del Ingeniero LCI and based on ISO 9001: 2015 and ISO 27001: 2013 we created an integrated management system that can suit all these needs.

Findings: Throughout all the process, there were several pieces of information that were key to develop the project. Some of them were the conservation of documented information to guarantee that all procedures, protocols & client requirements are fully complete and followed. In some cases, there is no enough evidence to support, for example, that important changes were made or that the client allowed any transfer of information.

Results: Design of an integrated management system, based on ISO 9001: 2015 and ISO 27001: 2013

Resumen Ejecutivo

Título:	Diseño de un sistema integrado de gestión basado en las normas ISO 9001:2015 e ISO 27001:2013 para La Casa del Ingeniero LCI.
Autores:	Cristian Yohan Cárdenas Herrera Dayron Yemmery Efrén Higuera Soto
Palabras clave:	Calidad, Seguridad de la Información, Sistema de gestión integrado, modelos de gestión.

Contenido: Por estos días las organizaciones y sus unidades productivas no solo responden a las necesidades de los clientes a través del cumplimiento de sus requisitos o de sus solicitudes para obtener un producto o servicio, los clientes y en muchos casos la ley, exigen un tratamiento especial para salvaguardar la información y protegerla de usos no intencionados. A partir de estas necesidades, se establece que la Calidad y la Seguridad de la Información deben ser un complemento fundamental en el desarrollo de aplicaciones como software, apps web y móviles y contenidos digitales. Con este fundamento se abordó la problemática presentada por La Casa del Ingeniero LCI, en la que formulamos con base en la ISO 9001:2015 e ISO 27001:2013 un modelo integrado de gestión adecuado a sus necesidades.

Consideraciones: Resultó clave durante el desarrollo de las actividades, aspectos tales como la conservación de información documentada durante la operación para garantizar que se cumplen los controles y los requerimientos de seguridad de la información y los requerimientos de los clientes, ya que en algunas ocasiones no se cuenta con evidencia suficiente que respalde por ejemplo que se realizó algún cambio importante o que el cliente autorizó un nuevo envío de información.

Resultado: Diseño del sistema integrado de gestión basado en las normas ISO 9001:2015 e ISO 27001:2013.

Tabla de contenido

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

1 INTRODUCCIÓN

1.1 PROBLEMÁTICA (JUSTIFICACIÓN)

El contexto actual en el que se desenvuelven las organizaciones que diseñan software y/o plataformas web en Colombia se encuentra en auge, gracias a los objetivos del Ministerio de las Tic que actualmente está promoviendo en conjunto con organizaciones privadas, el impulso y acompañamiento a ideas de negocio o negocios ya establecidos de base tecnológica, los objetivos que se promueven son los siguientes:

1. Diseñar, formular, adoptar y promover las políticas, planes, programas y proyectos del sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la ley, con el fin de contribuir al desarrollo económico, social y político de la Nación, y elevar el bienestar de los colombianos. ·
2. Promover el uso y apropiación de las Tecnologías de la Información y de las Comunicaciones entre los ciudadanos, las empresas, el gobierno y demás instancias nacionales como soporte del desarrollo social y económico y político de la Nación.
3. Impulsar el desarrollo y fortalecimiento del sector de la Tecnologías de la Información y las Comunicaciones, promover la investigación e innovación, buscando su competitividad y avance tecnológico conforme al entorno nacional e internacional.

Con base en ello, se están generando emprendimientos de alto impacto e innovación, haciendo crecer el número de empresas que se dedican al desarrollo de software, páginas web y aplicativos móviles entre otros, el acompañamiento y exigencias de las entidades gubernamentales a estos nuevos emprendimientos hacen que se asegure siempre la calidad en los procesos y la seguridad de la información de los productos y servicios prestados a los clientes.

Es por esto que surge la iniciativa de diseñar un sistema de gestión integrado bajo las normas ISO 9001:2015 e ISO 27001:2013 para la empresa *La Casa del Ingeniero LCI*, la cual tenga la capacidad de responder a los requerimientos de los clientes garantizando el cumplimiento de sus solicitudes con procesos adecuados que mantengan protegida y segura la información suministrada para el desarrollo de sus productos y servicios, con el diseño integrado del sistema de gestión, *La Casa del Ingeniero LCI* da un paso para generar mejores oportunidades de ser una organización competitiva y acorde a las necesidades y requerimientos del mercado actual.

1.2 OBJETIVOS Y PREGUNTA DE INVESTIGACIÓN

1.2.1 Objetivo General

Diseñar el sistema de gestión integrado bajo las normas ISO 9001:2015 e ISO 27001:2013 para la empresa *La Casa del Ingeniero LCI.*

1.2.2 Objetivos Específicos

1. Identificar la correlación de los requisitos entre las normas NTC ISO 9001:2015 y NTC ISO 27001:2013
2. Realizar el diagnóstico de la situación actual, que nos permita identificar el estado de cumplimiento de los requisitos de ISO 9001:2015 e ISO 27001:2013.
3. Evaluar el contexto de la organización.
4. Determinar cuáles son las partes interesadas de la organización y los requisitos pertinentes.
5. Definir el alcance del Sistema Integrado de Gestión.
6. Diseñar la Política y objetivos del Sistema Integrado de Gestión.
7. Determinar mapa de procesos y caracterizar los procesos necesarios del Sistema Integrado de Gestión.
8. Analizar los riesgos según ISO 9001:2015 e ISO 27001:2013

1.2.3 Pregunta de investigación

¿Cómo diseñar un sistema de gestión integral para la empresa *La Casa Del Ingeniero* basados en las normas NTC ISO 9001:2015 y NTC ISO 27001:2013?

1.3 ALCANCE Y LIMITACIONES

1.3.1 Alcance

- Diseño del Sistema Integrado de Gestión bajo las normas NTC ISO 9001:2015 y NTC ISO 27001:2013, aplicable a los procesos de la empresa *LA CASA DEL INGENIERO*.
- Diseño de la política integral para la empresa *LA CASA DEL INGENIERO*.
- Definición de los Objetivos, Alcance e indicadores de Gestión Integral de acuerdo con las normas NTC ISO 9001:2015 y NTC ISO 27001:2013
- Caracterización de los procesos necesarios para el sistema integrado de gestión.
- Análisis de riesgos, evaluación y definición de controles para los riesgos identificados.

1.3.2 Limitaciones

No se realizará la implementación del sistema integrado de gestión en la Casa del Ingeniero a nivel de documentación de procedimientos, diseño de registros aplicables

1.4 METODOLOGÍA

1.4.1 Enfoque de la investigación

Mediante la investigación descriptiva se expondrá la situación actual del estado de La casa del Ingeniero respecto a los sistemas de gestión ISO 9001:2015 e ISO 27001:2013.
Investigación descriptiva tiene como finalidad definir, clasificar, catalogar o caracterizar el objeto de estudio. Los métodos descriptivos pueden ser cualitativos o cuantitativos.
La investigación descriptiva se aplicó definiendo la correlación de los numerales de las normas, clasificar y catalogar los datos definidos en las diferentes tablas y matrices expuestas en el trabajo.
Los métodos cualitativos se basan en la utilización del lenguaje verbal y no recurren a la cuantificación. Los principales métodos de la investigación descriptiva son el observacional, el de encuestas y los estudios de caso único[1].

1.4.2 Línea y sublinea de investigación

Debido a que la naturaleza del proyecto es el diseño de un sistema de gestión integrado, se ubica en la línea de investigación de gestión de la calidad: sublinea de procesos para el diseño e implementación de sistemas integrados.

1.4.3 Técnicas de recolección de información

El proyecto se llevará a cabo explorando las fuentes primarias de información como entrevistas y secundaria como archivos, tesis, análisis e información documentada que disponga La Casa del Ingeniero.
La identificación y correlación de los requisitos aplicables a los sistemas de gestión ISO 9001 e ISO 27001 se realizará directamente mediante el uso de las normas NTC ISO disponibles por ICONTEC.
Todos los datos de las tablas contenidos en este documento serán organizados según tipo para posteriormente realizar su análisis de acuerdo a los resultados arrojados.

[1] http://www.uv.es/webgid/Descriptiva/331_mtodos.html

Tabla 1 metodología de trabajo

OBJETIVO	PROCESO	RESULTADOS
Identificar la correlación de los requisitos entre las normas NTC ISO 9001:2015 y NTC ISO 27001:2013	Realizar un análisis comparativo de cada requisito de las normas NTC ISO 9001:2015 y NTC ISO 27001:2013, relacionándolos entre sí, identificando cuales se requieren en ambas normas y cuales en una sola norma	Informe de correlación de las normas NTC ISO 9001:2015 y NTC ISO 27001:2013 Lista de chequeo aplicable a la empresa
Realizar el diagnóstico de la situación actual, que nos permita identificar el estado de cumplimiento de los requisitos de ISO 9001:2015 e ISO 27001:2013.	Aplicar una lista de chequeo que incluye los requisitos de las normas NTC ISO 9001:2015 y NTC ISO 27001:2013	Diagnóstico de la situación actual de la empresa y definición de la norma base a trabajar
Evaluar el contexto de la organización.	Realizar un análisis FODA de factores internos y externos a la organización.	Matriz de análisis FODA con análisis de estrategia FO, DO, FA, DA
Determinar cuáles son las partes interesadas de la organización y los requisitos pertinentes.	Identificación de todas las posibles partes interesadas a través de una matriz relacionando y clasificando según su interés.	Matriz de partes interesadas clasificadas según su interés.
Diseñar la Política y objetivos del Sistema Integrado de Gestión	Aplicación de los requisitos de las normas NTC ISO 9001:2015 y NTC ISO 27001:2013, entrevista al gerente de la organización e identificación de la estrategia.	Política integral y objetivos en base a las normas NTC ISO 9001:2015 y NTC ISO 27001:2013.
Determinar mapa de procesos y caracterizar los procesos necesarios del Sistema Integrado de Gestión	Identificación de las actividades que se realizan en la organización y cómo se relacionan.	Mapa de procesos y procesos caracterizados
Realizar el análisis de riesgos según ISO 9001:2015 e ISO 27001:2013	Aplicación de los conocimientos adquiridos sobre indicadores de gestión.	Objetivos, alcance e indicadores de gestión integral con base en las normas NTC ISO 9001:2015 y NTC ISO 27001:2013
Análisis de riesgos según ISO 9001:2015 e ISO 27001:2013, evaluar los riesgos y definir los controles necesarios	Identificar los riesgos, analizar y evaluar los riesgos, identificar y evaluar las distintas opciones de tratamiento de los riesgos para aplicar controles	Matriz de riesgos priorizados y los controles requeridos definidos

Fuente: los autores

1.5 CRONOGRAMA DEL PROYECTO

Tabla 2 Cronograma de actividades

ACTIVIDAD	MARZO				ABRIL			
Informe de correlación de las normas NTC ISO 9001:2015 y NTC ISO 27001:2013 Lista de chequeo aplicable a la empresa								
Diagnóstico de la situación actual de la empresa y definición de la norma base a trabajar								
Matriz de análisis DOFA con análisis de estrategia FO, DO,FA,DA								
Matriz de partes interesadas clasificadas según su interés y poder								
Política integral y objetivos en base a las normas NTC ISO 9001:2015 y NTC ISO 27001:2013								
Mapa de procesos y procesos caracterizados								
Objetivos, alcance e indicadores de gestión integral en base a las normas NTC ISO 9001:2015 y NTC ISO 27001:2013								
Matriz de riesgos priorizados y los controles requeridos definidos								

2 MARCO REFERENCIAL

2.1 MARCO TEÓRICO

2.1.1 Sistema de gestión de calidad

Un Sistema de Gestión de la Calidad (SGC) no es más que una serie de actividades coordinadas que se llevan a cabo sobre un conjunto de elementos para lograr la calidad de los productos o servicios que se ofrecen al cliente, es decir, es planear, controlar y mejorar aquellos elementos de una organización que influyen en el cumplimiento de los requisitos del cliente y en el logro de la satisfacción del mismo.[2]

2.1.2 Norma NTC 9000:2005

La Norma ISO 9000 describe los fundamentos de los sistemas de gestión de la calidad y especifica la terminología de los sistemas de gestión de la calidad.

2.2 Norma NTC ISO 9001:2015

La norma ISO 9001 es una norma internacional de gestión de la calidad aplicable a cualquier tipo de organización de cualquier sector o actividad. Está basada en los ocho principios de gestión de calidad, fundamentales para una buena gestión empresarial.

- Enfoque al cliente
- Liderazgo
- Compromiso de las personas
- Enfoque a procesos
- Mejora
- Toma de decisiones basada en la evidencia
- Gestión de las relaciones

[2] http://qualitytrends.squalitas.com/articulos/articulos-gestion-de-la-calidad/item/108-sistemas-de-gesti%C3%B3n-de-la-calidad-%E2%80%93-un-camino-hacia-la-satisfacci%C3%B3n-del-cliente-%E2%80%93-parte-i.html

Tabla 3 Correlación entre ISO 9001:2008 e ISO 9001:2015

NORMA UNE EN ISO 9001:2008	NORMA UNE EN ISO 9001:2015
EPÍGRAFES: 1. Objeto y campo de aplicación 2. Normas para consulta 3. Términos y definiciones 4. Sistema de gestión de calidad 5. Responsabilidad de la Dirección 6. Gestión de los Recursos 7. Realización del producto 8. Medición, análisis y mejora	EPÍGRAFES: 1. Objeto y campo de aplicación 2. Referencias normativas 3. Términos y definiciones 4. Contexto de la organización 5. Liderazgo 6. Planificación 7. Soporte 8. Operación 9. Evaluación del desempeño 10. Mejora

Fuente: http://www.larescvalenciana.org/blog/iso-9001-%C2%BFque-diferencias-hay-entre-la-del-2008-y-la-del-2015/2015/06/18/

2.2.1 Sistema de gestión de seguridad de la información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.[3].

[3] http://www.iso27000.es/sgsi.html.

2.2.2 Norma NTC ISO/IEC 27001:2013

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001[4].

2.2.3 NTC ISO 31000:2011 GESTIÓN DEL RIESGO

La Gestión del Riesgo se hace necesaria para controlar y manejar las amenazas que se presentan a nivel organizacional y tecnológico, con los recursos disponibles, a fin de que no se materialicen estos riesgos y afecten los productos y/o servicios que ofrece la empresa.

Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis, luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios del riesgo. A través de este proceso, las organizaciones se comunican y consultan con las partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando con el fin de garantizar que no se requiere tratamiento adicional del riesgo. Esta norma describe este proceso sistemático y lógico en detalle.

Aunque todas las organizaciones gestionan el riesgo en algún grado, esta norma establece un número de principios que es necesario satisfacer para hacer que la gestión del riesgo sea eficaz. Esta norma recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de referencia cuyo propósito sea integrar el proceso para la gestión del riesgo en los procesos

[4] http://advisera.com/27001academy/es/que-es-iso-27001/

globales de gobierno, estrategia y planificación, gestión, procesos de presentación de informes, políticas, valores y cultura de la organización[5].

2.3 MARCO CONTEXTUAL

2.3.1 Generalidades de la empresa

La Casa del Ingeniero es una empresa con 6 años de trayectoria en el mercado, ubicada con una sede central en el Municipio de Facatativá (Cundinamarca) y otra sede en la ciudad de Bogotá Av. 15 No 116-43 Oficina. 505.

La Casa del Ingeniero, presta servicios a empresas y/o particulares que deseen promover el crecimiento de su negocio valiéndose de las Tecnologías de la Información, en este caso la Internet. En auge, este medio se ha convertido en una potente herramienta para el sector del comercio, logrando así que las empresas que incursionan obtengan excelentes resultados. Y si otras empresas lo hicieron, **¿porque la suya no?** En La Casa del Ingeniero estamos dispuestos a ayudarlo, colocando a su empresa en un medio publicitario en el cual podrá ser conocida a nivel mundial, solo con un clic.

[5] NTC ISO 31000:2011 GESTION DEL RIESGO

3 DESARROLLO

3.1 CORRELACIÓN DE NORMAS

3.1.1 Análisis y correlación de las normas ISO 9001:2015 e ISO 27001:2013

La correlación de las Normas muestra la relación de un requisito de la Norma ISO 9001: 2015 con la Normas ISO 27001: 2013, el objetivo es ayudar a entender las variaciones entre cada uno de los capítulos que componen estas normas.

Para lograr este objetivo se diseñó una herramienta para comparar cada uno de los requisitos (ver Anexo A.), se relacionqó numeral por numeral de cada norma, con el objeto de encontrar las diferencias principales o las coincidencias, y con base en ellas, definir la norma base para el diseño del sistema integrado.

Adicionalmente a conocer la similitud de los sistemas, se tomó la correlación de las normas como base para ejecutar la integración de los modelos, es decir, que teniendo como punto de partida los elementos comunes y diferentes de las normas, se definieron cuáles de ellos son integrables al sistema y cuáles no, con base en su complementariedad, es decir que por ejemplo para el caso del numeral 4.1 de las dos normas (ver tabla 4), el contexto de la organización se puede gestionar a través de las herramientas convencionales de calidad como el FODA y complementarlo con las sugerencias que hace la norma como el uso de la ISO 31000. Para ello la norma base de redacción de documentos definida en la correlación es la que se determina como guía, de acuerdo a su complementariedad o especificidad de los requisitos analizados.

Dentro de la (Tabla 5), se hace un resumen general de la correlación de las Normas ISO 9001:2015 y ISO 27001:2013, contemplando cada uno de los capítulos que componen las normas.

Tabla 4 Ejemplo de correlación

ISO 9001:2015		ISO 27001:2013		DIFERENCIAS	NORMA BASE PARA REDACCIÓN
4.1	Comprensión de la organización y de su contexto	**4.1**	Conocimiento de la organización y de su contexto	La ISO 27001 hace una NOTA adicional, no referida en la ISO 9001 que cita “La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la organización, considerado en el numeral 5.3 de la NTC-ISO 31000:2011[5].”	ISO 9001:2015

Fuente: los autores

Tabla 5 Resumen Correlación de Normas

CORRELACIÓN DE NORMAS			
ISO 9001:2015		**ISO 27001:2013**	
0.	Introducción	**0**	Introducción
0.1	Generalidades	**0.1**	Generalidades
0.2	Principios de la gestión de la calidad	**N/A**	N/A
0.3	Enfoque a procesos	**N/A**	N/A
0.4	Relación con otras normas de sistemas de gestión	**0.2**	Compatibilidad con otras normas de sistemas de gestión
1.	Objeto y campo de aplicación	**1.**	Objeto y campo de aplicación
2.	Referencias normativas	**2.**	Referencias normativas
3.	Términos y definiciones	**3.**	Términos y definiciones
4.	Contexto de la organización	**4.**	Contexto de la organización
4.1	Comprensión de la organización y de su contexto	**4.1**	Conocimiento de la organización y de su contexto
4.2	Comprender las necesidades y expectativas de las partes interesadas	**4.2**	Comprensión de las necesidades y expectativas de las partes interesadas
4.3	Determinación del alcance del sistema de gestión de la calidad	**4.3**	Determinación del alcance del sistema de gestión de la seguridad de la información
4.4	Sistema de Gestión de la calidad y sus procesos	**4.4**	Sistema de gestión de la seguridad de la información
5.	Liderazgo	**5.**	Liderazgo
5.1	Liderazgo y compromiso	**5.1**	Liderazgo y compromiso
5.2	Política	**5.2**	Política
5.3	Roles, responsabilidades y autoridades en la organización	**5.3**	Roles, responsabilidades y autoridades en la organización
6.	Planificación	**6.**	Planificación
6.1	Acciones para abordar riesgos y oportunidades	**6.1**	Acciones para tratar riesgos y oportunidades
6.2	Objetivos de la calidad y planificación para lograrlos	**6.2**	Objetivos de seguridad de la información y planes para lograrlos
6.3	Planificación de los cambios	**N/A**	N/A
7.	Apoyo	**7.**	Soporte
7.1	Recursos	**7.1**	Recursos
7.2	Competencia	**7.2**	Competencia
7.3	Toma de Conciencia	**7.3**	Toma de conciencia
7.4	Comunicación	**7.4**	Comunicación
7.5	Información documentada	**7.5**	Información documentada
8.	Operación	**8.**	Operación
8.1	Planificación y control operacional	**8.1**	Planificación y control operacional
8.2	Requisitos para los productos y servicios	**8.2**	Valoración de riesgos de la seguridad de la información
8.3	Diseño y desarrollo de los productos y servicios	**8.3**	Tratamiento de riesgos de la seguridad de la información
8.4	Control de los procesos, productos y servicios suministrados externamente	**N/A**	N/A
8.5	Producción y provisión del servicio	**N/A**	N/A

8.6	Liberación de los productos y servicios	**N/A**	N/A
8.7	De las salidas no conformes	**N/A**	N/A
9.	Evaluación del desempeño	**9.**	Evaluación del desempeño
9.1	Seguimiento, medición, análisis y evaluación	**9.1**	Seguimiento, medición, análisis y evaluación
9.2	Auditoría interna	**9.2**	Auditoría interna
9.3	Revisión por la dirección	**9.3**	Revisión por la dirección
10.	Mejora	**10.**	Mejora
10.1	Generalidades	**N/A**	N/A
10.2	No conformidad y acción correctiva	**10.1**	No conformidad y acción correctiva
10.3	Mejora continua	**10.2**	Mejora continua

Fuente: los autores

3.1.2 Conclusiones de Correlación de la norma

De la correlación de los requisitos de norma de la ISO 9001:2015 y la ISO 27001:2013 presentado en el Anexo A, se pueden concluir los siguientes aspectos:

- Las dos normas presentan una estructura de alto nivel. es decir, que las normas ISO comparten una estructura base en común, capítulos idénticos, numerales, títulos de los numerales, entre otros lo que hace más fácil la integración entre las normas.
- La ISO 9001:2015 relaciona de una manera más amplia los requisitos comunes con ISO 27001:2013, por tal razón la mayoría de los requisitos son redactados tomando como referencia la ISO 9001.
- Los numerales (6.1 y 7.4) de la ISO 27001 requieren desarrollar de manera más profunda el requerimiento enfocados en la Seguridad de la Información.
- El capítulo 8 de ambas normas no se relaciona (ver tabla 6) por lo que es necesario que se gestionen de manera independiente, ya que en ISO 9001 se despliegan 7 numerales y en 27001 solamente 3 de los que el 8.1 es el único que comparte contenido con 9001.

Tabla 6 Comparación capítulo 8 de las normas ISO 9001 e ISO 27001

	ISO 9001:2015		ISO 27001:2013
8.1	Planificación y control operacional	**8.1**	Planificación y control operacional
8.2	Requisitos para los productos y servicios	**8.2**	Valoración de riesgos de la seguridad de la información
8.3	Diseño y desarrollo de los productos y servicios	**8.3**	Tratamiento de riesgos de la seguridad de la información
8.4	Control de los procesos, productos y servicios suministrados externamente	**N/A**	N/A
8.5	Producción y provisión del servicio	**N/A**	N/A
8.6	Liberación de los productos y servicios	**N/A**	N/A
8.7	De las salidas no conformes	**N/A**	N/A

Fuente: los autores

3.2 DIAGNÓSTICO DE CUMPLIMIENTO DE REQUISITOS ISO 9001 E ISO 27001

3.2.1 Lista de chequeo de las normas ISO 9001:2015 e ISO 27001:2013.

Las listas de chequeo permiten realizar un primer inventario o verificación de las características de la empresa, pueden aplicarse también a conglomerados empresariales y pueden acondicionarse de acuerdo con la estructura objeto de chequeo. Este instrumento permite identificar puntos débiles así como oportunidades de mejora a través de la verificación de un listado de aspectos presentes o no en el área a revisar[6].

Con base en este análisis comparativo de la correlación de las normas presentado en el capítulo anterior, se diseñó el formulario (ver Anexo B.) Con base en los requisitos solicitados en cada norma y en las diferencias encontradas en la correlación de las mismas. Allí se diseñaron y plasmaron las preguntas correspondientes que abarcaran de manera integral los requisitos solicitados de ambas normas en una sola herramienta, lo cual permite simplificar la tarea de verificar el cumplimiento de los requisitos, extractando de esta forma la situación actual de la organización con respecto a la gestión realizada para su sistema de gestión de calidad y de seguridad de la información.

[6] http://datateca.unad.edu.co/contenidos/358049/Modulo_en_linea/leccin_22_lista_de_chequeo.html

3.2.2 Análisis de la lista de chequeo integrada

La lista de chequeo se aplicó a la empresa La Casa del Ingeniero y permitió visualizar de una manera global la situación actual de la organización con respecto al cumplimiento de los requisitos de las normas ISO 9001:2015 e ISO 27001:2013. Teniendo en cuenta que la estructura de la lista de chequeo se presenta por los capítulos integrados de las normas y con el fin de identificar el estado de la empresa respecto a los requisitos de las normas integradas, se estableció un mecanismo de valoración del cumplimento de los requisitos dando una ponderación que se califica con la siguiente nomenclatura: (1) para el cumplimiento o incumplimiento de cada uno de los requisitos, los cuales al final de cada capítulo serán totalizados con el fin de establecer cuál es el nivel de cumplimiento de cada uno de los requisitos establecidos en la lista de chequeo.

Una vez aplicada la lista de chequeo a la empresa La Casa del Ingeniero, mediante entrevista y revisión documental de la empresa, se concluye que la organización tiene las mayores debilidades en los capítulos de **Planificación (6), Evaluación de desempeño (9) y Mejora (10)** ya que, según los resultados de la tabla 5, el cumplimiento de estos numerales se encuentra en el (0%) cada uno, debido principalmente a que, a pesar que en algunos procesos se realizan correctamente las actividades, no existe evidencia que respalde que se están cumpliendo de la manera en que detalla la norma en cada uno de sus requerimientos. Adicionalmente y según los resultados presentados por la lista de chequeo, no solo se debe concentrar esfuerzos en los anteriores 3 capítulos, sino en todos en general, a partir de que ninguno cumple con el 100% de los requerimientos de norma.

Tabla 7 Resultados lista de chequeo

N°	Capitulo	Cumple	No cumple	Cumplimiento
4	Contexto de la organización	10	6	62.5%
5	Liderazgo	6	13	31.5%
6	Planificación	0	22	0%
7	Apoyo - Soporte	5	23	17.8%
8	Operación	34	47	41.9%
9	Evaluación de Desempeño	0	25	0%
10	Mejora	0	5	0%
	TOTAL	**196**		

Fuente: los autores

A continuación se detalla de manera específica aquellos capítulos que al ser evaluados en la empresa se detecta que no se cuenta con ningún aspecto de cumplimiento:

Capítulo 6 Planificación: dado que la organización no posee una planificación estratégica, no conoce su contexto, ni posee información documentada de acerca de la valoración y el tratamiento de los riegos de calidad y seguridad de la información.
En relación a los objetivos, estos no se encuentran definidos ni documentados, la organización no posee una estructura que mida y haga seguimiento a sus procesos principales.

Capítulo 9 Evaluación de Desempeño: la organización hace algunos seguimientos a los procesos sobre los cuales requiere hacer pruebas, como por ejemplo la búsqueda y carga de datos en sistemas de información, pero estos no se documentan ni se mantiene alguna evidencia de que se ejecutó un seguimiento y medición del desarrollo del sistema, es decir, que no hay evidencia de un versionamiento que pueda hacer traza de los controles realizados.

Capítulo 10 Mejora: al momento de revisar como La Casa del Ingeniero gestionaba las no conformidades y respondía a ellas mediante correcciones o acciones correctivas, encontramos que ante estas situaciones la organización respondía a estos requerimientos de tal forma que en la medida en que se presentan no documentan ninguna actividad y dejan sin evidencia de que realmente se trató la no conformidad con base en su causa real.

3.3 PLANIFICACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN

3.3.1 Desarrollo de la estrategia organizacional

Los mapas estratégicos desarrollados por Robert Kaplan y David Norton son una excelente herramienta para desarrollar la estrategia organizacional ya que se basa en 4 pilares, Aprendizaje y crecimiento, procesos internos, grupos de interés y financiera, lo cual provee a las compañías de 4 perspectivas diferentes para plasmar su estrategia y definir de esta manera las métricas correspondientes para evaluar el desempeño organizacional que pueden ser plasmadas a través de indicadores o un cuadro de mando integral que mida la estrategia definida.

La Casa del Ingeniero durante el desarrollo de las actividades y en el momento de realizar la verificación con la lista de chequeo en el numeral 4.1 contexto de la

organización, se evidencia que no posee la definición estratégica del negocio, no existe una proyección formal y al realizar las entrevistas no se evidencia que el personal la conozca; por esta razón, se estructuró un taller con el gerente de la organización a fin de identificar cuáles serán los posibles escenarios estratégicos en los que se se espera se desenvuelva la empresa. Esto permite orientar a la organización a corto y mediano y plazo; se extractaron algunas preguntas clave para definir el contexto y el mapa estratégico sobre el cual la organización debería guiarse, para mantener el curso de su gestión y su eficacia organizacional a través del tiempo.

Para ello, se tomó como referencia as preguntas que permitan responder a los planteamientos de las cuatro perspectivas del mapa estratégico definido por Kaplan y Norton que son: Aprendizaje y crecimiento, procesos internos, grupos de interés y financiera, con base en ellas se diseñaron las preguntas para definir el futuro estratégico de la organización. A continuación se presenta los resultados de estas preguntas:

a) ¿Cuál es el futuro deseable de la organización?

El futuro deseable de la organización es abrir su brecha de mercado a nivel internacional, ofreciendo productos con calidad y que brinden la efectiva ejecución de procesos en las diferentes organizaciones.

b) ¿Cuál es el futuro posible de la organización?

El futuro posible para LA CASA DEL INGENIERO, es ampliar su portafolio de clientes, implementación de nuevos lenguajes de desarrollo, para el diseño de aplicativos web.

c) ¿Cómo se encuentra actualmente la organización?

Actualmente la organización LA CASA DEL INGENIERO, se encuentra en el proceso de implementación de la ISO 9001:2105, con el fin de mejorar los procesos, y certificar sus productos y/o servicios bajo una norma de calidad.

d) ¿Cuál es la cultura que la organización debe desarrollar para alcanzar el futuro posible? (Principales características).

Cultura Corporativa:

El trabajo en la organización se basa en el trabajo en equipo, delegar responsabilidades y que se trabaje con autonomía, teniendo como base el liderazgo y la toma de decisiones para el desarrollo de los productos.

e) ¿Cuáles son las características más relevantes de la cultura actual de la organización?

Las Características más relevantes de la cultura organizacional son: el trabajo en equipo y el valor de formarse como un líder.

f) ¿Qué estrategias deberá emplear la organización para cerrar las brechas identificadas?

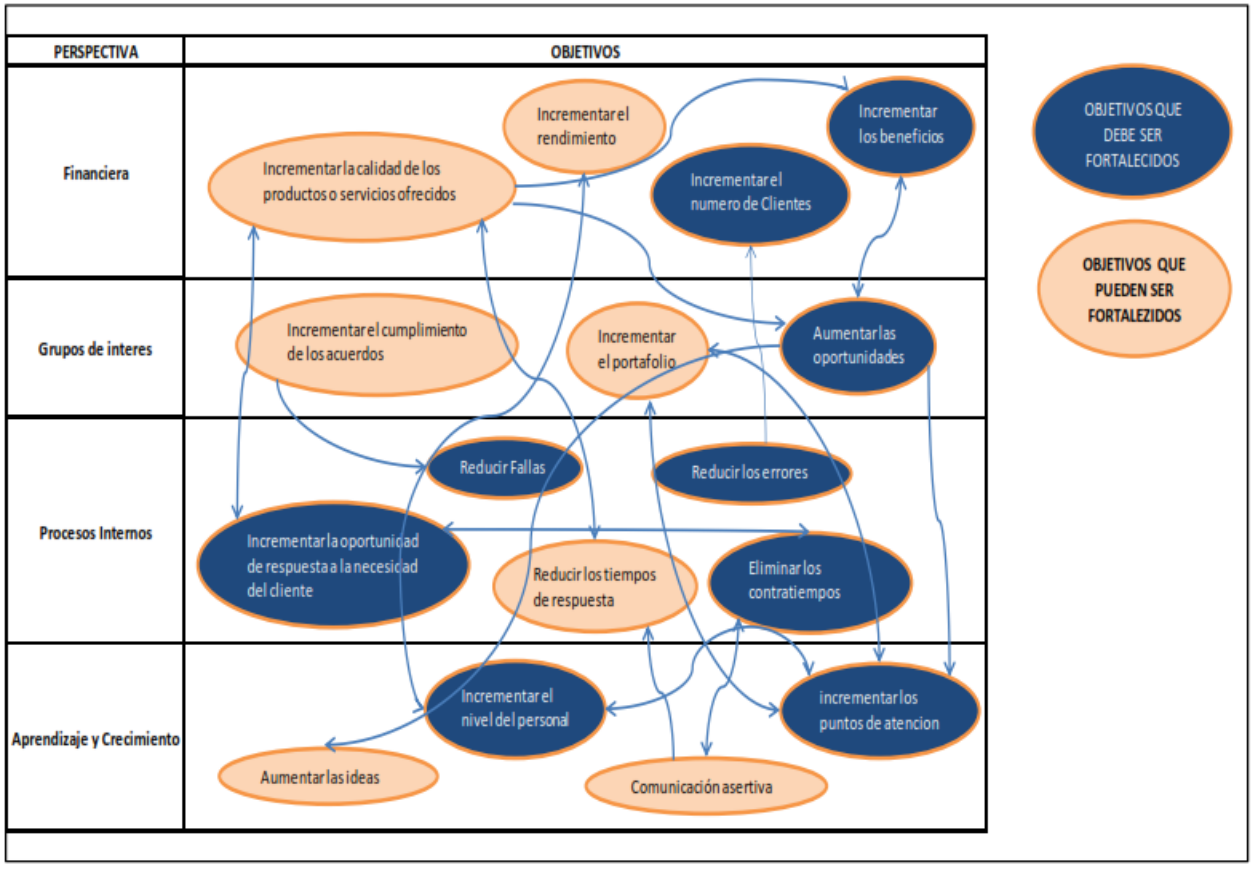
Los tipos de estrategia que utilizara LA CASA DEL INGENIERO, son los siguientes: Diagrama de causa – efecto (Identificar características y elementos fundamentales para la organización; y Mapa conceptual (Decidir cuáles son nuestras prioridades. Decidir cuáles de nuestros objetivos debemos hacer y en qué orden es esencial para gestionar estratégicamente la producción de nuestro trabajo.)

3.3.2 Definición del mapa estratégico

El mapa estratégico hace referencia a la estrategia de LA CASA DEL INGENIERO, mediante una serie de relaciones de causa y efecto, teniendo en cuenta 4 perspectivas:

- Financiera
- Grupos de interés
- Procesos Internos
- Aprendizaje y Crecimiento

A partir de estas perspectivas se define como la organización implementará la estrategia.



3.3.3 Análisis FODA

La sigla FODA, es un acróstico de Fortalezas (factores críticos positivos con los que se cuenta), Oportunidades, (aspectos positivos que podemos aprovechar utilizando nuestras fortalezas), Debilidades, (factores críticos negativos que se deben eliminar o reducir) y Amenazas, (aspectos negativos externos que podrían obstaculizar el logro de nuestros objetivos)[7].

Según las características de este análisis, se usa para determinar los factores internos y externos de la organización, con el objetivo de analizar las variables más representativas y determinar de esta manera el mejor camino para engranar la estrategia de la organización con el diseño del sistema.

[7] http://www.matrizfoda.com/home.html

Si bien la herramienta estratégica ideal para plasmar la misión, la visión, las metas, los objetivos y las estrategias de una empresa es el Plan de Negocios, realizando correctamente el análisis FODA se pueden establecer las estrategias[8].

MATRIZ DOFA LA CASA DEL INGENIERO	FORTALEZAS	DEBILIDADES
	1. Apoyo de la Alta Dirección para la adaptación a nuevas tecnologías de la información, en LA CASA DEL INGENIERO S.A. 2. Conocimientos en el Desarrollo de Software de Software a la medida (lenguaje PHP-JAVA). 3. Trabajo en equipo para la realización de proyectos en la creación de software a la medida.	1. No se cuenta con políticas documentadas para el manejo de activos de información. 2. No existe fortalecimiento al Recurso Humano en las nuevas tecnologías de la información. 3. No hay un método estándar establecido en LA CASA DEL INGENIERO, para la creación de un proyecto de software requerido por un cliente. 4. Deficiencia en el seguimiento de quejas y reclamos de los clientes. 5. Falta de Automatización de algunos procesos en busca de la mejor calidad en la entrega de productos. 6. Desconocimiento del personal en algunos temas de Mantenimiento de Equipos.
	AMENAZAS	OPORTUNIDADES
	1. Vulnerabilidad de la información 2. Incremento en el costo de desarrollo de proyectos de software a la medida. 3. Ineficientes mediciones en el avance del proyecto. 4. Incremento en la demanda de los requerimientos exigidos por el cliente. 5. Impactos en el producto a consecuencia de quejas y reclamos.	1. Conferencias, Tutoriales, Guías. Para tecnologías y aplicativos Web. 2. Plataformas de Desarrollo de Software Libre. 3. Convenios con terceros para el alquiler de equipos de cómputo. 4. Permiso a personal para Acceso a Control Remoto. 5. Trabajo para personal de desarrollo desde su casa.

3.3.4 Estrategias del análisis FODA

Estrategias F-O: Estas son las mejores estrategias para sacar el máximo provecho de las oportunidades que se presentan. No podemos aprovecharlas si no tenemos desarrolladas las fortalezas que necesitamos.

Estrategias D-A: Estas estrategias son muy importantes para prevenir que las amenazas nos debiliten a través de la vulnerabilidad que las debilidades nos generan.

Estrategias F-A: Estas estrategias se desarrollan para identificar las vías que necesitamos para reducir los efectos negativos de las amenazas que se presentan en el entorno.

[8] http://www.matrizfoda.com/home.html

Estrategias D-O: Estas estrategias se generan para reducir o eliminar las debilidades de tal manera que no inhiban el aprovechamiento de las oportunidades que tenemos.

Estas estrategias se priorizan teniendo en cuenta el desarrollo de un plan de trabajo con el fin de definir actividades, responsables y tiempos de desarrollo y realizando un seguimiento periódico[9].

3.3.4.1 Potencialidades (estrategias FO)

Aquí se señalan las líneas de acción que la empresa debería asumir para mejorar su gestión.

- Generar programas de capacitación, mediante la utilización de herramientas de trabajo en LA CASA DEL INGENIERO S.A.
- Desarrollar la automatización de procesos que generan actividades manuales y generar valor en la entrega final del producto.
- Generar una metodología de proyecto de Software, a partir de una herramienta que facilite el control por etapas y el avance del producto/servicio que se ofrece en LA CASA DEL INGENIERO S.A.

3.3.4.2 Limitaciones (estrategias DA)

Aquí se señalan las principales advertencias que debe conocer la organización

- Realizar auditorías periódicas a fin de detectar las fallas dentro del Sistema.
- Contratar personal competente para cubrir la demanda de requerimientos.
- Realizar buck up de manera frecuente, evitando la perdida de información y generando riesgos potenciales para el desarrollo de los productos y/o servicios.

3.3.4.3 Riesgos (estrategias FA)

- Apoyarse en la alta dirección para implementar el sistema de gestión de seguridad de la información.

---

9 http://axeleratum.com/2012/analisis-foda-5-pasos-para-desarrollar-el-analisis-segunda-parte/#sthash.Ot2p3GGQ.dpuf

- Aprovechar los altos conocimientos en lenguajes de programación para optimizar los tiempos de desarrollo de productos y disminuir costos.
- Usar el trabajo en equipo como estrategia para cubrir la demanda de requerimientos de los clientes.

3.3.4.4 Desafíos (estrategias DO)

- Capacitar al personal para el manejo de los activos de la organización y en tecnologías de la información y mantenimiento de equipos.
- Adoptar una metodología para desarrollo de proyectos.
- Diseñar una herramienta que optimice y automatice los procesos para mejorar la calidad de los productos.

3.3.5 Matriz de partes interesadas (stakeholders)

Los *stakeholders*, un término muy difícil de traducir literalmente al español, son las personas y organizaciones como clientes, patrocinadores, organización ejecutante y el público, involucrados activamente en el proyecto, o cuyos intereses pueden verse afectados de manera positiva o negativa por la ejecución o conclusión del proyecto. También se les conoce como interesados, involucrados o actores del proyecto[10]. Es por esto, que para continuar la alineación de la estrategia organizacional con los requerimientos del Sistema Integrado de Gestión, se evaluó el Numeral 4.2 de la ISO 9001:2015 y de la ISO 27001:2013 para aclarar las necesidades y expectativas de las partes interesadas, y de esta forma aumentar la efectividad para garantizar la capacidad de la organización en cumplir con sus requerimientos.

Tabla 8 partes interesadas

PARTE INTERESADA	DENOMINACIÓN	NOMBRE	OBJETIVO	PODE	NIVEL DE INTERÉ	REQUERIMIENTO PRINCIPAL	ESTRATEGI

[10] ESPECIALIZACION GESTION INTEGRADA QHSE, GERENCIA DE PROYECTOS, Matriz_de_Stakeholders_-_Guia.docx- cohorte N° 34 - ESCUELA COLOMBIANA DE INGENIERIA

CLIENTES	Pequeñas y medianas empresas de cualquier sector productivo que estén en capacidad económica y que deseen automatizar la gestión de sus procesos haciendo uso de las TIC.	**Empresa:** CODECUM	Que sea Oportuno	ALTO	ALTO	PRODUCTO - Equipo de cómputo o Software	PI Estratégica
		Empresa: DON PASTELER	Confiable – Habeas Data	ALTO	ALTO		
		Empresa: Gestión Integral	Eficaz	ALTO	ALTO		
		Empresa: Merizalde Abogados	Integro (que la información no se pierda, no se	ALTO	ALTO		PI Estratégica
			Que se actualicen o mejoren las funcionalidades	ALTO	ALTO		PI Estratégica
			Pertinentes para			SERVICIO – Capacitación de software	
			La metodología				
			El material de apoyo debe ser				
			El tiempo es				
EMPLEADOS	Director y Contratistas	Desarrollador Operario Técnico Operario Servicios Generales	Cumplimiento de las	BAJO	BAJO	RESULTADO – Buen clima organizacional	No requiere
			Ambiente (Físico) de trabajo apropiado para				
			Estabilidad laboral				
			Reglas claras: Que se espera de				
			Bienestar				
SOCIOS	Integrantes de la sociedad de La Casa del Ingeniero	Merizalde Abogados	Rentabilidad	ALTO	ALTO	RESULTADO – Utilidad Operativa	PI Estratégica
			Buen nombre /	ALTO	ALTO		
			Proyección	ALTO	ALTO		
			Equidad y	ALTO	ALTO		
PROVEEDORES	Hosting Dominios Redes Dispositivos	**Empresa:** Hostgator	Cumplimiento en el pago	BAJO	ALTO	RESULTADO – Calidad, oportunidad y confianza	Mantener Informado
		Empresa: Hostdime	Claridad y cumplimiento en				
		Empresa: Compucenter ltda	Claridad en las condiciones de Evaluación del				
		Empresa: Godaddy	Retroalimentación Oportuna.				

3.3.6 Política y Objetivos del sistema de gestión integrada

Política Integral

LCI “LA CASA DEL INGENIERO” es una compañía dedicada a proveer a las empresas y/o trabajadores individuales a potencializar su crecimiento comercial y empresarial con soluciones informáticas de acuerdo a las diferentes necesidades que se presentan hoy en día en el mundo comercial, y mediante su política integral pretende:

1. Dar cumplimiento a los requisitos legales asociados y aplicables en materia de calidad y seguridad de la información.
2. Garantizar la efectividad del mejoramiento continuo de los procesos y la satisfacción de las necesidades del Cliente y de las demás partes interesadas.
3. Mantener y Mejorar los objetivos organizacionales y verificar el cumplimiento de la legislación aplicable vigente.

Objetivos organizacionales

Con base en el mapa estratégico se definieron los objetivos organizacionales en la siguiente matriz:

PERSPECTIVA	OBJETIVO	INDICADOR	FRECUENCIA	RESPONSABLE
Financiera	Incrementar la calidad de los productos y servicios ofrecidos.	$\frac{clientes\ satisfechos\ x\ periodo\ de\ tiempo}{total\ clientes\ atendidos\ x\ periodo\ de\ tiempo}$	Mensual	Coordinador comercial
	Incrementar el rendimiento	$\frac{Recursos\ utilizados}{Recursos\ Presupuestados}$	Mensual	Coordinador de contabilidad
	Incrementar el número de clientes	$\frac{Clientes\ nuevos\ x\ periodo\ de\ tiempo}{Total\ de\ clientes\ x\ periodo\ de\ tiempo}$	Mensual	Coordinador comercial
	Incrementar los beneficios	$ingresos - costos$	Mensual	Coordinador de contabilidad
Grupos de Interés	Incrementar el cumplimiento de los acuerdos.	$\frac{Requisitos\ cumplidos}{Total\ de\ requisitos\ solicitados}$	Mensual	Coordinador de desarrollo de software
	Incrementar el portafolio	$\frac{Productos\ o\ servicios\ nuevos}{Total\ de\ productosy\ servicios}$	Mensual	Coordinador comercial
	Aumentar las oportunidades	$\frac{\%\ de\ mercado\ nuevo}{\%\ total\ de\ mercado}$	Mensual	Coordinador comercial
Procesos internos	Incrementar la oportunidad de respuesta al cliente.	$\frac{\#\ de\ horas\ de\ respuesta\ real}{\#\ de\ horas\ establecidas}$	Mensual	Coordinador de tecnologías de la información
	Reducir las fallas de software	$cantidad\ de\ fallas\ reportadas\ por\ el\ cliente$	Mensual	Coordinador de tecnologías de la información
	Los errores operativos	$cantidad\ de\ fallas\ encontradas\ en\ la\ operacion$	Mensual	Coordinador de desarrollo de software
	Eliminar los contratiempos	$cantidad\ de\ horas\ improductivas\ al\ dia$	Mensual	Coordinador de talento humano

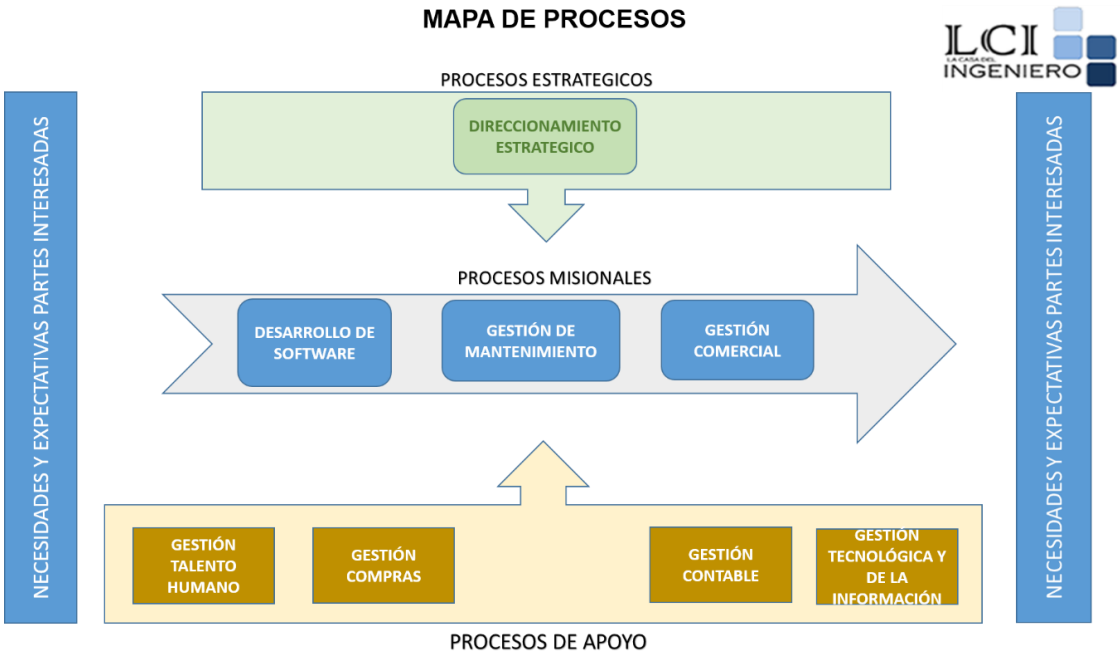
Aprendizaje y crecimiento	Aumentar las ideas	$cantidad\ de\ ideas\ recibidas\ nuevas$	Mensual	Coordinador de talento humano
	Incrementar el nivel del personal	$\frac{personal\ nuevo}{personal\ actual}$	Mensual	Coordinador de talento humano
	Comunicación asertiva	$cantidad\ de\ resolucion\ de\ problemas\ de\ comunicacion$	Mensual	Coordinador de talento humano
	Incrementar los puntos de atención.	$\frac{puntos\ de\ atencion\ nuevos}{punstos\ de\ atencion\ actuales}$	Mensual	Coordinador comercial

3.3.7 Alcance del sistema integrado de gestión.

El alcance del sistema integrado de gestión abarca los procesos de direccionamiento estratégico, gestión de software, gestión de mantenimiento, gestión comercial, gestión de talento humano, gestión de compras, gestión contable y gestión tecnológica y de la información que se ubican en la sede central de sus oficinas en la Calle 147 # 7C-51 Bogotá, Colombia.

3.3.8 Mapa de procesos

Diseño del mapa de procesos.



3.3.9 Caracterización de los procesos

Luego de diseñar el mapa de procesos de la organización, fue necesario establecer la caracterización de los procesos estratégicos, misionales y de apoyo (ver tabla 8), permitiendo identificar sus entradas, actividades, salidas, indicadores, documentos etc. véase (Anexo C).

Tabla 9 Diseño de caracterización de proceso

<table>
<tr><th colspan="5">CARACTERIZACIÓN DEL PROCESO</th></tr>
<tr><td colspan="3">1. OBJETIVO: (Describe la finalidad del proceso, lo que se quiere lograr, basado en las directrices de la organización)</td><td colspan="2">2. ALCANCE: (Describe la amplitud de la aplicación del proceso, desde donde inicia y hasta donde termina, de acuerdo al objetivo definido)</td></tr>
<tr><td colspan="3">3. RESPONSABLE: (Se define el cargo responsable por el funcionamiento del proceso)</td><td colspan="2">4. PARTICIPANTES (Se definen los cargos responsables por la ejecución de las actividades del proceso)</td></tr>
<tr><td colspan="5">REQUISITOS</td></tr>
<tr><td colspan="2">ISO 9001:2015</td><td colspan="3">ISO 27001:2013</td></tr>
<tr><td>5. PROVEEDOR</td><td>6. ENTRADAS</td><td>7. ACTIVIDADES</td><td>8. SALIDAS</td><td>9. CLIENTE</td></tr>
<tr><td>Hace referencia a los clientes externos o a los procesos (proveedores internos) que suministran las entradas a este proceso).</td><td>(Constituidas por las salidas (productos) que deben entregar los proveedores para llevar a cabo las actividades de este proceso, relacionadas con información y documentos.)</td><td>A. Establecer los métodos de seguimiento apropiados para demostrar la capacidad del proceso para alcanzar el objetivo.
B. Establecer los métodos de seguimiento a las características de los productos o salidas para verificar que cumplen con los requisitos de los mismos.</td><td>(Constituidas por el resultado (producto) obtenido durante la ejecución del proceso (documentos, reportes, listados, planillas, entre otros). Hacen parte de las entradas a los procesos clientes)</td><td>(Hace referencia a los clientes externos o a los procesos (clientes internos) que reciben las salidas de este proceso)</td></tr>
<tr><td colspan="3">10. DOCUMENTOS: (Relacionar los documentos (planes, procesos, procedimientos, instructivos y formatos), requeridos para la ejecución de las actividades del proceso, incluye los documentos de origen externo)</td><td colspan="2">11. RECURSOS: (Determinar las necesidades de recursos (Humano, Infraestructura y Ambiente de trabajo) para implantar y mantener el proceso)</td></tr>
<tr><td colspan="3">12. REGISTROS: (Relacionar los documentos que presentan los resultados obtenidos o proporcionan evidencia de la ejecución de las actividades del proceso).</td><td colspan="2">13. INDICADORES: (Establecer los indicadores del proceso que permiten medir la eficacia frente al logro del objetivo)</td></tr>
</table>

Fuente: Adaptado de: ESPECIALIZACIÓN GESTIÓN INTEGRADA QHSE, SOPORTE OPERATIVO PARA QHSE, modelo de presentación de procesos – caracterización de procesos – cohorte N° 34, ESCUELA COLOMBIANA DE INGENIERÍA

4 ANÁLISIS DE RIESGOS

4.1 Metodología para la gestión del riesgo de La Casa del Ingeniero

En este capítulo se describe la metodología propuesta para la gestión de riesgos de La Casa del Ingeniero, la cual es adaptada de la metodología propuesta por ISO 31000:2011, descrita en la ilustración 2.

Ilustración 1 Metodología para la gestión de riesgos.
Fuente: Los autores

4.1.1 Establecimiento del contexto

El fin de establecer el contexto es alinear la gestión del riesgo de La Casa del Ingeniero a las situaciones externas e internas que se puedan presentar con base en los siguientes aspectos:

4.1.1.1 **Contexto externo** (ambiente externo en el cual la organización busca alcanzar sus objetivos)

Entender el contexto externo es importante con el fin de garantizar que los objetivos y las preocupaciones de las partes involucradas externas se toman en consideración al desarrollar los criterios del riesgo. Esto se basa en el contexto a todo lo ancho de la organización, las percepciones de las partes involucradas y otros aspectos de los riesgos específicos para el alcance del proceso para gestionar el riesgo[11], como se despliega a continuación:

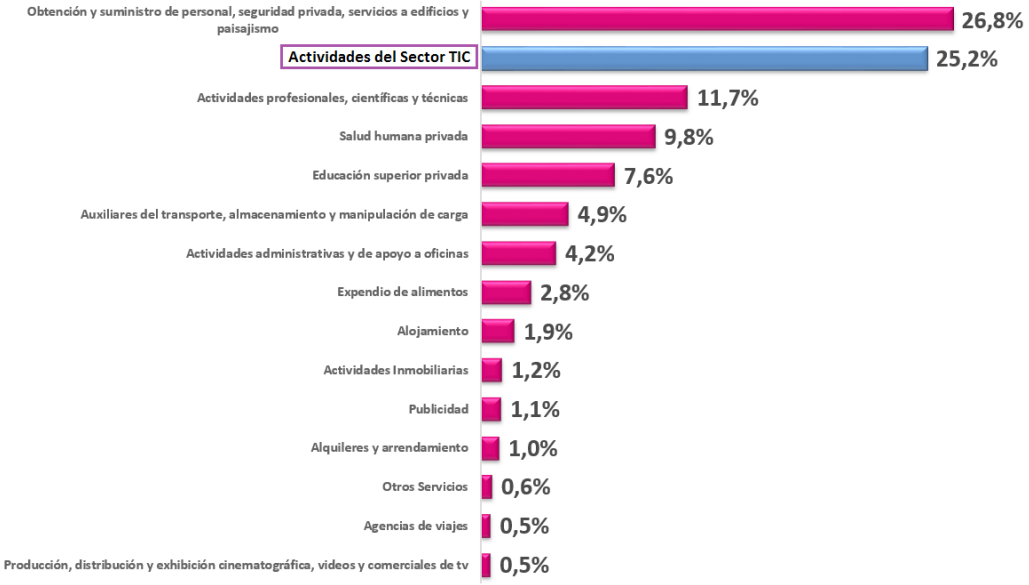
4.1.1.1.1 Sector TIC en Colombia

En el 2013, según cifras preliminares del DANE en la Encuesta Anual de Servicios, el sector TIC tuvo una participación del 25% del total del valor agregado de la economía colombiana. Esto significa que el sector TIC está posicionado

[11] NTC ISO 31000:2011

como uno de los sectores que genera mayor valor agregado, siendo el más dinámico del país y ocupando el segundo lugar del ranking.

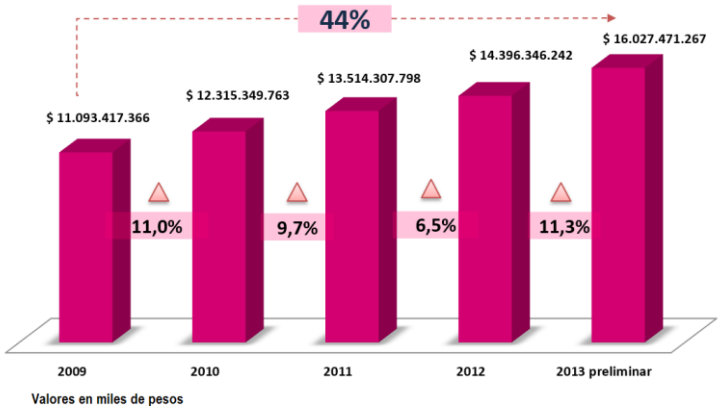
Distribución del Valor Agregado total de las empresas investigadas, según actividades de servicio.



Fuente: DANE (2014), cálculos propios. Encuesta Anual de Servicios (Resultados Corrientes) Recuperado de: http://www.dane.gov.co/index.php/servicios/encuesta-anual-de-servicios-eas

En cuanto al consumo de bienes intermedios, aprovechando la producción de los demás sectores, el sector TIC creció entre el 2009 y 2013 un 44%.

De acuerdo con las cifras preliminares del DANE en la Encuesta Anual de Servicios, el mayor crecimiento del consumo intermedio en el sector TIC fue entre 2012 y 2013, con un incremento del 11,3%. El crecimiento presentado desde el 2009 del consumo intermedio del sector TIC, comprueba que cada año el sector TIC se comporta como un sector transversal en la economía colombiana, por lo que tiene influencia en el crecimiento de los demás sectores.



Fuente: DANE (2014), cálculos propios. Encuesta Anual de Servicios (Resultados Corrientes) Recuperado de: http://www.dane.gov.co/index.php/servicios/encuesta-anual-de-servicios-eas

4.1.1.1.2 Competencia

El 25% de las empresas del sector TI a novel nacional ofrecen “manejo de centros de datos (data center)”, el segundo producto más ofrecido es “desarrollo de software” (23% de las empresas lo incluyen en su catálogo). “mesas de ayuda” con el 14% y “Testing” con el 10% ocupan el tercero y cuarto lugar respectivamente en productos/servicios ofrecidos por las empresas de la industria.

Productos y Servicio	Cantidad	Participación
Manejo de centros de datos (data center)	851	25%
Desarrollo / fábrica de software	772	23%
Mesas de ayuda (Otras)	477	14%
Testing de software	330	10%
Infraestructura como servicio	300	9%
Consultoría e implementación	143	4%
Mantenimiento o soporte de aplicaciones	143	4%
Software como servicio	116	3%
Otro	115	3%
Plataformas tecnológicas como servicio	90	3%
Cloud computing	27	1%
Gerencia	6	0%
Total General	**3370**	

Fuente: censo MinTic 2015

4.1.1.2 **Contexto interno** (ambiente interno en el cual la organización busca alcanzar a sus objetivos)

El contexto interno es todo aquello dentro de la organización que pueda tener influencia en la forma en que se gestionará el riesgo, a continuación se describe este ambiente en el cual se desenvuelve La Casa del Ingeniero.

4.1.1.2.1 Misión

La Casa del Ingeniero tiene como misión potencializar el crecimiento comercial de empresas y/o trabajadores independientes, implementando las Tecnologías de la Información en su plan de desarrollo empresarial, dando así soluciones informáticas a las diferentes necesidades que exige hoy en día el sector del comercio.

4.1.1.2.2 Visión

Nos proyectamos como una empresa líder en el campo de las soluciones informáticas, valiéndonos de las Tecnologías de la Información. Así, queremos llegar a que cualquier ente desde la comodidad de su casa u oficina pueda encontrar en su computadora el producto o servicio que necesita, donde y como conseguirlo. Esta persona o cliente llegara a conocer las empresas, sus productos y/o servicios y a requerir de ellos, logrando así fortalecer el mundo del comercio y su economía.

4.1.1.2.3 Organigrama

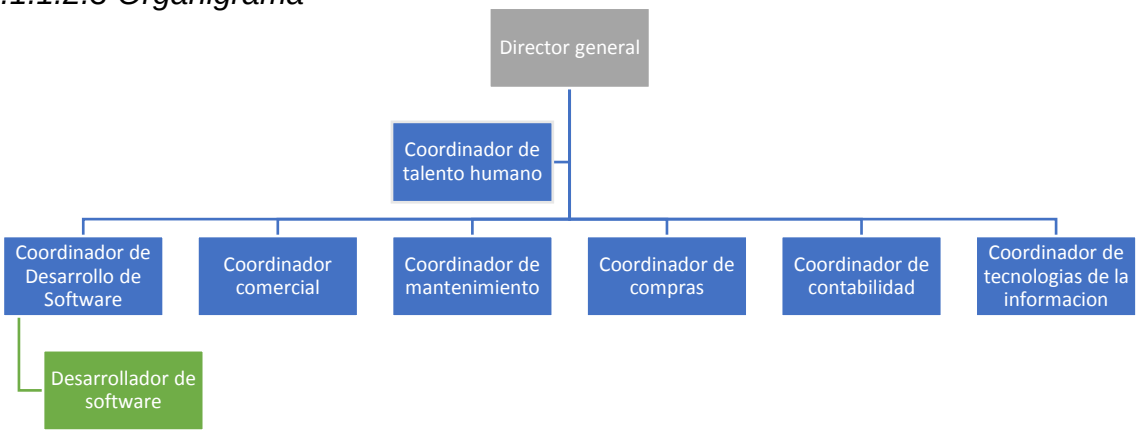


Ilustración 2 Organigrama

4.1.1.2.4 PRODUCTOS

Gestión Jurídica (Software para la administración del departamento jurídico)

Gestión Jurídica versión 1.0 es un sistema web para administrar y controlar el departamento legal, los clientes y las entidades donde se gestionan cada uno de los negocios de cualquier organización pública y privada. Para tal fin, el sistema permite la creación de actuaciones jurídicas, la trazabilidad en todos los casos legales a cargo, asignación de tareas, alarmas y visualización de los documentos que forman parte de los expedientes digitalizados en la nube, que pueden ser consultados y descargados desde cualquier dispositivo.

Encuesta.me (Software para la aplicación de encuestas)

encuesta.me es un software para la aplicación de encuestas en línea, escrita en PHP. Las encuestas incluyen ramificación a partir de condiciones y diseño personalizado usando un sistema de plantillas web, provee utilidades de análisis estadístico para el tratamiento de los resultados obtenidos. Las encuestas pueden tener tanto un acceso público como un acceso controlado estrictamente por las claves que pueden ser utilizadas una sola vez (tokens) asignadas a cada persona que participa en la encuesta. Además los resultados pueden ser anónimos, eparando los datos de los participantes de los datos que proporcionan, inclusive en encuestas controladas.

Aula Hub (Software de servicios educativos)

Aula HUB es una plataforma de aprendizaje virtual su arquitectura y herramientas son apropiadas para realizar actividades en línea. Tiene una interfaz de navegación de tecnología sencilla, ligera, y compatible, permite presentar los contenidos por curso, crear enlaces con otros materiales, colaborar, hacer cuestionarios, enviar tareas, y realizar comentarios sobre el material o el desarrollo del curso.

Id Print (Software para control de identidades y carnetización)

Id Print es un software que permite gestionar el diseño y la impresión de sus tarjetas de identificación. Con Id Print, puede elegir, desde las funcionalidades básicas como la impresión de nombres en monocromo hasta la avanzada impresión de diseños a todo color y a doble cara.

Gestión CRM (Software para gestión de marketing y ventas)

Gestión CRM (Customer Relationship Manager) te permite aumentar tus beneficios, impulsar la productividad de tu equipo de fuerza de ventas y sacar partido de las redes sociales.

- Dirigido a cualquier sector de actividad.
- Mejora tu rendimiento Comercial.
- Marketing orientado y medible.
- Atención al Cliente excepcional.

Solution CRM (Software que es más que un CRM)

La comercialización eficaz asegura clientes potenciales y un flujo de ventas consistente. Desafortunadamente, muchos sistemas de venta sólo incluyen capacidades básicas de marketing y las empresas deben comprar e integrar una solución de software separada, esto genera mayores costos y es innecesariamente complejo. Solution CRM es diferente: tenemos en cuenta la comercialización de un componente esencial de un sistema de ventas y Solution CRM cuenta con capacidades integradas de marketing, altamente utilizables que se pueden implementar con eficacia y utilizados por cualquier persona en su organización. Solution CRM permite la automatización de tareas, esto aumenta la productividad de los empleados y le permite ampliar el alcance de su organización, sin la contratación y formación de nuevos empleados. Estas son tan solo algunas de las miles características con las que cuenta esta poderosa herramienta. Solution CRM es mas que un CRM.

Gestión ERP (Conecte su empresa en un solo lugar)

Gestión ERP es un sistema completo integrando un sistema de contabilidad y gestión empresarial que sólo requiere un navegador web y lector de pdf para su uso. Cuenta con una amplia gama de características adecuadas para muchas empresas especialmente empresas de distribución, empresas de venta al por mayor y empresas de manufactura. También combina una tercera parte interactiva de sistema de punto de venta, logrando formar el núcleo de un sistema de gestión de venta multi-rama dispersa. Posee integración de una tienda virtual. Gestión ERP es la herramienta de gestión empresarial más completa y robusta en el mercado.

4.1.2 Identificación del riesgo

A través de este paso, lo que se busca establecer es los eventos que pueden afectar negativamente a la empresa, igualmente los elementos principales para identificación de riesgos, análisis, evaluación y tratamiento.

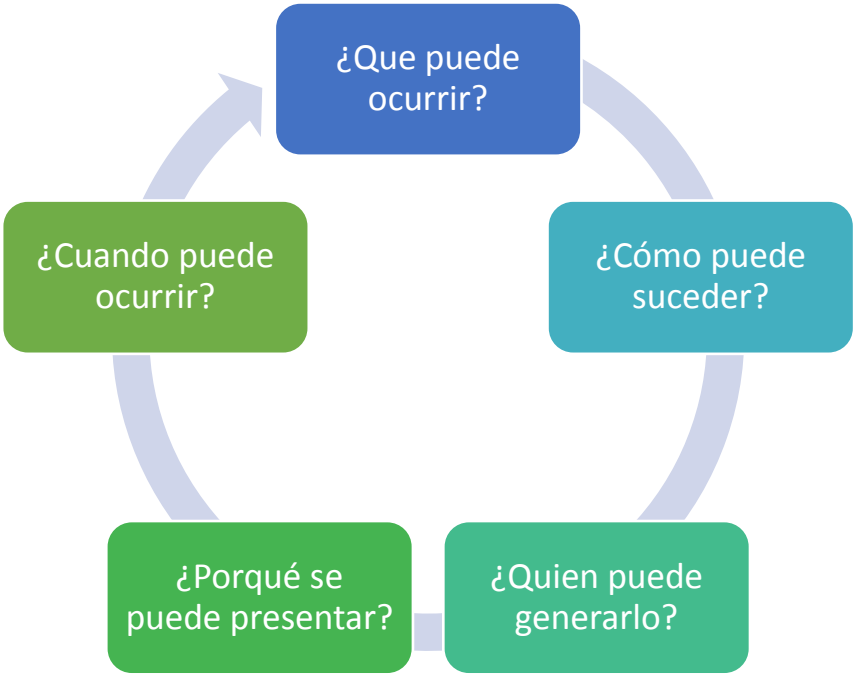


Ilustración 3 Preguntas para la identificación de riesgos
Fuente: Mejía Quijano, Rubi Consuelo. (2006). Administración de riesgos. Un enfoque empresarial. Medellín. Fondo Editorial Universidad EAFIT.

Una vez definidos e identificados cada uno de los riesgos es necesario precisar los siguientes elementos:

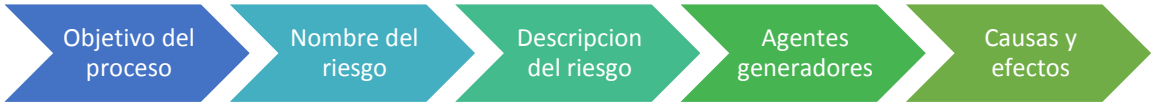


Ilustración 4 Elementos a definir para la identificación de riesgos
Fuente: Mejía Quijano, Rubi Consuelo. (2006). Administración de riesgos. Un enfoque empresarial. Medellín. Fondo Editorial Universidad EAFIT.

4.1.2.1 Clasificación del riesgo

Para La Casa del Ingeniero, y aquellas personas que participan directa o indirectamente de sus actividades, se definieron los riesgos asociados con la misión de la organización de la siguiente manera:

- **Riesgos Económicos:** son aquellos riesgos que provienen directamente del entorno económico del sector y de los consumidores.
- **Riesgos Tecnológicos:** se relacionan con los posibles nuevos desarrollos en tecnología, telecomunicaciones y TIC´s en general, que también pueden afectar por interrupciones en la prestación del servicio.
- **Riesgo de Recursos humanos:** Está relacionado con la capacidad de las personas para cumplir y hacer cumplir lo estipulado dentro de la organización, como procesos, procedimientos, normas, reglamentaciones etc.
- **Riesgo de Operativo:** Este comprende los riesgos derivados del funcionamiento y operación de los sistemas de información de la organización.
- **Riesgo de Tecnología:** Relaciona la capacidad tecnológica de la organización para satisfacer las necesidades y expectativas de los clientes.

4.1.2.2 Tipificación del riesgo

4.1.2.2.1 Factores De Riesgo Externos

Estos se relacionan con los cambios a los que la organización está expuesta.

- **Riesgos Económicos:**
  - Disponibilidad de capital
  - Liquidez
  - Competencia
  - Desempleo
- **Riesgos tecnológicos:**
  - Interrupciones de servicio
  - Tecnologías emergentes

4.1.2.2.2 Factores De Riesgo Internos

Estos hacen referencia al funcionamiento de los procesos y las actividades organizacionales

- **Riesgos de recursos humanos:**
  - Baja motivación.
  - Insatisfacción laboral.
  - Poca habilidad en el manejo de equipos o lenguajes de programación.
  - Impedimentos físicos.
  - Monotonía
  - Altos ritmos de trabajo
  - Utilización indebida de información confidencial
- **Riesgos operativos:**
  - Fallas en la escritura del código de programación.
  - Falta de oportunidad en la respuesta.
  - Perdidas de información.
  - Daños a los sistemas informáticos
- **Riesgos de tecnología:**
  - Fallas del software.
  - Fallas del hardware (equipos de cómputo o almacenamiento).
  - Fallas en los sistemas de telecomunicaciones.
  - Intrusión a los sistemas informáticos.

Tabla 10 Identificación de riesgos

Proceso	Riesgo	Descripción del riesgo	Agente generador	Causa	Efecto
Desarrollo de software	Fallas en la escritura del lenguaje de programación	Posible incumplimiento de requisitos de calidad de software.	Desarrollador de software	Bajo conocimiento o experiencia	Pérdida económica
	Perdidas de información	Posible daño a la propiedad del cliente.	Desarrollador de software	Descuido en el manejo o almacenamiento de la información	Sanción legal o económica
	Falta de oportunidad en la respuesta	Posibles demoras en gestionar los requerimientos del cliente.	Desarrollador de software	Falta de información	Quejas y reclamos
	Fallas en el software	Posibles errores en el diseño o desarrollo de software.	Desarrollador de software	Uso inadecuado	Pérdida económica
	Robo de información	Posible Utilización indebida de información confidencial	Desarrollador de software	Controles deficientes Descuido en el manejo o almacenamiento de la información	Sanción legal o económica
Gestión comercial	Error en la descripción de requisitos	Posibles diseño y desarrollo de software inadecuado	Coordinador comercial	Bajo conocimiento o experiencia	Pérdida económica
	Cálculos equivocados	Posibles Costos incorrectos de diseño y desarrollo para el cliente	Coordinador comercial	Falta de información	Pérdida económica Quejas y reclamos
	Pérdida de clientes	Posible migración de clientes hacia la competencia	Coordinador comercial	Bajo conocimiento o experiencia Mala atención	Pérdida económica
Gestión de mantenimiento	Perdida de información	Posibles daños o perdidas de datos irrecuperables	Coordinador de mantenimiento	Bajo conocimiento o experiencia Método de backup inadecuado	Pérdida económica Sanción legal o económica
	Daño en el software	Posibles daños o perdidas de datos irrecuperables	Coordinador de mantenimiento	Bajo conocimiento o experiencia Método de mantenimiento inadecuado	Pérdida económica Sanción legal o económica

	Daño en el hardware	Posibles daños o pérdidas de datos irrecuperables.	Coordinador de mantenimiento	Bajo conocimiento o experiencia Método de mantenimiento inadecuado	Pérdida económica Sanción legal o económica
	Interrupciones del servicio	Posible Caída en el servicio de telecomunicaciones.	Coordinador de mantenimiento	Método de mantenimiento inadecuado	Pérdida económica Sanción legal o económica
Gestión de talento humano	Accidentes de trabajo	Posible Exposición a peligros en el lugar del trabajo.	Coordinador de talento humano	Falta de conciencia del riesgo, equipos de protección inadecuados, actos inseguros.	Pérdida económica Sanción legal o económica
	Monotonía	Posibles Trabajos rutinarios	Coordinador de talento humano	Baja rotación de puestos de trabajo	Baja productividad
	Insatisfacción laboral	Posible ambiente laboral inapropiado Posible ocupación de cargo incorrecta por parte del personal.	Coordinador de talento humano	Ambiente laboral afectado, presiones, insatisfacción salarial, estrés.	Baja productividad
	Robo de información	Posible Utilización indebida de información confidencial.	Coordinador de talento humano	Controles deficientes Descuido en el manejo o almacenamiento de la información	Pérdida económica Sanción legal o económica
	Errores de nómina o liquidación de prestaciones sociales	Posible incumplimiento de las obligaciones contractuales con los empleados.	Coordinador de talento humano	Bajo conocimiento o experiencia	Quejas y reclamos
Gestión de compras	Error de especificación	Posible Compra de productos o servicios inadecuados	Coordinador de compras	Error de comunicación	Perdida económica
	Error en cantidad	Posible compra de productos o servicios en cantidades inadecuadas	Coordinador de compras	Error de comunicación	Quejas y reclamos
	Demoras o retrasos	Posibles retrasos en la llegada o prestación del producto o servicio	Coordinador de compras	Falta de seguimiento	Quejas y reclamos

Gestión contable	Generación incorrecta de informes	Posible generación de datos irreales de la organización	Coordinador de contabilidad	Incorrecta contabilización de comprobantes	Pérdida económica Sanción legal o económica
	Error en la declaración de impuestos	Posible generación de Informes irreales	Coordinador de contabilidad	Bajo conocimiento o experiencia	Pérdida económica Sanción legal o económica
	Generación incorrecta de comprobantes	Posible facturación incorrecta de ítems	Coordinador de contabilidad	Bajo conocimiento o experiencia	Pérdida económica Sanción legal o económica
	Liquidez	Posible falta de liquidez para pago de nómina y prestaciones sociales	Coordinador de contabilidad	Cartera retrasada o mora de usuarios	Quejas y reclamos
Gestión tecnológica y de la información	Cambios en la normatividad relacionada con los requerimientos	Posible incumplimiento de requisitos	Coordinador de tecnologías de la información	Descuido o bajo conocimiento	Sanción legal o económica
	Asignación de recursos insuficientes	Posible establecimiento de necesidades insuficientes para satisfacer los requerimientos de la plataforma tecnológica.	Coordinador de tecnologías de la información	Estimación incorrecta por falta de información	Pérdida económica
	Acceso no autorizado a sistemas de información	Posible Utilización indebida de información confidencial.	Coordinador de tecnologías de la información	Controles deficientes	Pérdida económica Sanción legal o económica

Fuente: Los autores

4.1.3 Análisis y evaluación del riesgo

Una vez identificados todos los riesgos de la organización, lo que se busca es calificar cada uno de ellos otorgándoles una ponderación para determinar su gravedad, definiendo la frecuencia si es alta o baja, si su impacto es leve o grave etc. allí se plasmaran los criterios de calificación con que la empresa contara para establecer los riesgos que están dispuestos a asumir y cuáles no.

Tabla 11 Tabla de calificación de frecuencia

CALIFICACIÓN DE FRECUENCIA		
VALOR	**FRECUENCIA**	**DESCRIPCIÓN**
1	**BAJA**	1 evento en un año o menos
2	**MEDIA**	Entre 2 y 5 eventos en un año
3	**ALTA**	Entre 6 y 10 eventos en un año
4	**MUY ALTA**	Más de 10 eventos en un año

Fuente: adaptada de: ACOSTA, Cruz. Cristian Adolfo. Implementación del método Risicar para la administración de riesgos en una empresa pequeña de la ciudad de Bogotá.

Tabla 12 Tabla de calificación del impacto

CALIFICACIÓN DEL IMPACTO					
VALOR	**IMPACTO**	**OPERATIVO**	**ECONÓMICO**	**HUMANO**	**TECNOLÓGICO**
25	**LEVE**	Interrupción de la operación hasta por 2 horas	Perdidas hasta por 1 millón de pesos	Sin lesiones	Sin pérdida de datos o daño de la plataforma tecnológica
50	**MODERADO**	Interrupción de la operación de 2 a 6 horas	Perdidas entre 1 y 3 millones de pesos	Lesiones con incapacidad	Datos recuperables y/o Daños moderados sobre la plataforma tecnológica
75	**SEVERO**	Interrupción de la operación de 6 a 12 horas	Perdidas entre 3 y 7 millones de pesos	Victimas graves	Pérdida parcial de datos y/o daños severos sobre la plataforma tecnológica
100	**CATASTRÓFICO**	Interrupción de la operación de más de 12 oras	Pérdidas de más de 7 millones de pesos	Muertes	Pérdida total de datos y/o daños catastróficos sobre la plataforma tecnológica

Fuente: adaptada de: ACOSTA, Cruz. Cristian Adolfo. Implementación del método Risicar para la administración de riesgos en una empresa pequeña de la ciudad de Bogotá.

Con base en la ubicación que posea cada riesgo, se definirá la gravedad y las medidas de tratamiento correspondientes, es decir, se determinara la clasificación de los riesgos según su aceptabilidad y se catalogaran en aceptables, tolerables, graves e inaceptables y con base en ellos se establecerán las medidas correspondientes.

Tabla 13 Matriz de evaluación de riesgos

FRECUENCIA	**MUY ALTA**	**Tolerable 100**	**Grave 200**	**Inaceptable 300**	**Inaceptable 400**
	ALTA	**Tolerable 75**	**Grave 150**	**Grave 225**	**Inaceptable 300**
	MEDIA	**Tolerable 50**	**Tolerable 100**	**Grave 150**	**Inaceptable 200**
	BAJA	**Aceptable 25**	**Tolerable 50**	**Tolerable 75**	**Grave 100**
		LEVE	**MODERADO**	**SEVERO**	**CATASTRÓFICO**
		IMPACTO			

Fuente: adaptada de: ACOSTA, Cruz. Cristian Adolfo. Implementación del método Risicar para la administración de riesgos en una empresa pequeña de la ciudad de Bogotá.

Tabla 14 Interpretación de la severidad del riesgo

INTERPRETACIÓN	COLOR	CONTROLES
Riesgo Inaceptable		Eliminar la actividad, prevenir el riesgo, proteger la empresa o transferir el riesgo.
Riesgo Grave		Prevenir el riesgo, proteger la empresa o transferir el riesgo.
Riesgo Tolerable		Retener las perdidas, proteger la empresa o prevenir el riesgo.
Riesgo Aceptable		Aceptar el riesgo.

Fuente: Los autores

Tabla 15 Matriz de análisis y evaluación de riesgos

Proceso	Riesgo	Frecuencia	Impacto	Calificación	Evaluación	Tratamiento/Controles
Desarrollo de software	Fallas en la escritura del lenguaje de programación	2	25	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Daño de información	1	75	**75**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Falta de oportunidad en la respuesta	3	25	**75**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Fallas en el software	3	25	**75**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Robo de información	1	100	**100**	Grave	Prevenir el riesgo, proteger la empresa o transferir el riesgo.
Gestión comercial	Error en la descripción de requisitos	2	50	**100**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Cálculos equivocados	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Pérdida de clientes	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
Gestión de mantenimiento	Perdida de información	1	100	**100**	Grave	Prevenir el riesgo, proteger la empresa o transferir el riesgo.
	Daño en el software	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Daño en el hardware	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Interrupciones del servicio	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
Gestión de talento humano	Accidentes de trabajo	2	50	**100**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Monotonía	1	25	**25**	Aceptable	Aceptar el riesgo.
	Insatisfacción laboral	1	25	**25**	Aceptable	Aceptar el riesgo.
	Robo de información	1	100	**100**	Grave	Prevenir el riesgo, proteger la empresa o

						transferir el riesgo.
	Errores de nómina o liquidación de prestaciones sociales	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
Gestión de compras	Error de especificación	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Error en cantidad	1	25	**25**	Aceptable	Aceptar el riesgo.
	Demoras o retrasos	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
Gestión contable	Generación incorrecta de informes	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Error en la declaración de impuestos	1	75	**75**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Generación incorrecta de comprobantes	1	75	**75**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Liquidez	1	75	**75**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
Gestión tecnológica y de la información	Cambios en la normatividad relacionada con los requerimientos	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Asignación de recursos insuficientes	1	50	**50**	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo
	Acceso no autorizado a sistemas de información	1	100	**100**	Grave	Prevenir el riesgo, proteger la empresa o transferir el riesgo.

Fuente: Los autores

4.1.4 Tratamiento del riesgo

- Para los riesgos inaceptables es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la Probabilidad del riesgo, de Protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

- Las medidas dependen de la celda en la cual se ubica el riesgo, así: los Riesgos de Impacto leve y Frecuencia alta se previenen; los Riesgos con Impacto moderado y Frecuencia leve, se reduce o se comparte el riesgo, si es posible; también es viable combinar estas medidas con evitar el riesgo cuando éste presente una Frecuencia alta y media, y el Impacto sea moderado o catastrófico. Cuando la Frecuencia del riesgo sea media y su Impacto leve, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre reducir el riesgo, asumirlo o compartirlo. Cuando el riesgo tenga una Frecuencia baja e Impacto catastrófico se debe tratar de compartir el riesgo y evitar la entidad en caso de que éste se presente[12].

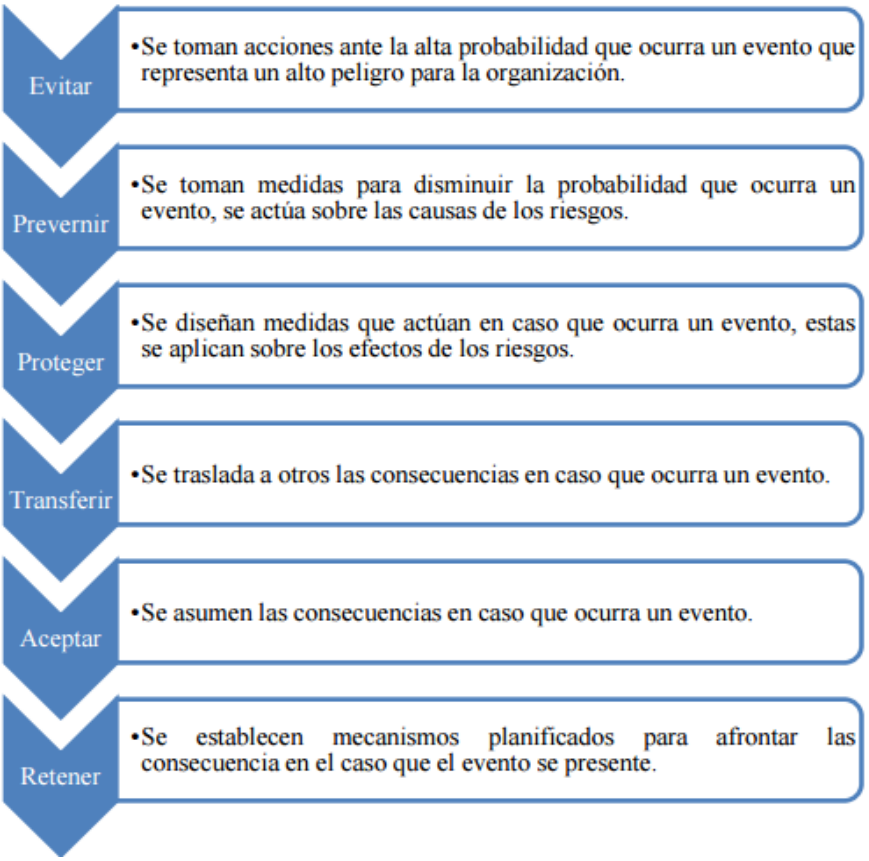


Ilustración 5 Medidas de tratamiento de riesgo
Fuente: adaptada de: ACOSTA, Cruz. Cristian Adolfo. Implementación del método Risicar para la administración de riesgos en una empresa pequeña de la ciudad de Bogotá.

[12] GUIA DE ADMINISTRACIÓN DEL RIESGO, departamento administrativo de la función pública, 2006.pdf

Tabla 16 Tabla de control de riesgos

Proceso	Riesgo	Evaluación	Controles
Desarrollo de software	Fallas en la escritura del lenguaje de programación	Tolerable	Prevenir el riesgo implementando el control y aseguramiento de calidad
	Daño de información	Tolerable	Prevenir el riesgo creando un plan de contingencias y respaldo de información.
	Falta de oportunidad en la respuesta	Tolerable	Prevenir el riesgo midiendo y analizando las causas principales para determinar su solución.
	Fallas en el software	Tolerable	Prevenir el riesgo implementando el control y aseguramiento de calidad
	Robo de información	Grave	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma tecnológica. Transferir el riesgo a través de una póliza de seguro.
Gestión comercial	Error en la descripción de requisitos	Tolerable	Prevenir el riesgo Validando y verificando la información con el cliente antes de enviarla a diseño y desarrollo.
	Cálculos equivocados	Tolerable	Prevenir el riesgo diseñando una metodología para evaluar la viabilidad de los requerimientos del cliente.
	Pérdida de clientes	Tolerable	Prevenir el riesgo haciendo seguimiento a los objetivos estratégicos de la compañía.
Gestión de mantenimiento	Perdida de información	Grave	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma tecnológica. Transferir el riesgo a través de una póliza de seguro.
	Daño en el software	Tolerable	Prevenir el riesgo creando un plan de contingencias y respaldo de información.
	Daño en el hardware	Tolerable	Prevenir el riesgo creando un plan de contingencias y respaldo de información.
	Interrupciones del servicio	Tolerable	Prevenir el riesgo creando un plan de contingencias y respaldo de información.
Gestión de talento humano	Accidentes de trabajo	Tolerable	Proteger a los trabajadores definiendo la matriz de Identificación de Peligros, Valoración de Riesgos y Determinación de Controles en seguridad y salud ocupacional.
	Monotonía	Aceptable	Proteger la organización realizando actividades como pausas activas o rotación de puestos de trabajo.
	Insatisfacción laboral	Aceptable	Proteger la organización diseñando un plan de incentivos a los trabajadores.
	Robo de información	Grave	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma

			tecnológica. Transferir el riesgo a través de una póliza de seguro.
	Errores de nómina o liquidación de prestaciones sociales	Tolerable	Prevenir el riesgo enviando la información a un nivel superior en donde pueda ser revisada y autorizada mensualmente.
Gestión de compras	Error de especificación	Tolerable	Prevenir el riesgo validando y verificando la información con desarrollo de software
	Error en cantidad	Aceptable	Prevenir el riesgo validando y verificando la información con desarrollo de software
	Demoras o retrasos	Tolerable	Prevenir el riesgo haciendo seguimiento a las solicitudes o requerimientos con el proveedor.
Gestión contable	Generación incorrecta de informes	Tolerable	Prevenir el riesgo manteniendo y controlando un procedimiento específico para generación de informes.
	Error en la declaración de impuestos	Tolerable	Prevenir el riesgo manteniendo y controlando un procedimiento específico para la declaración de impuestos.
	Generación incorrecta de comprobantes	Tolerable	Prevenir el riesgo manteniendo y controlando un procedimiento específico para generación de comprobantes
	Liquidez	Tolerable	Prevenir el riesgo definiendo un nivel mínimo de liquidez para responder con las obligaciones contractuales de los trabajadores.
Gestión tecnológica y de la información	Cambios en la normatividad relacionada con los requerimientos	Tolerable	Prevenir el riesgo a través de la inscripción en newsletters de normatividad legal.
	Asignación de recursos insuficientes	Tolerable	Prevenir el riesgo validando y consultando con los demás procesos las necesidades de requerimientos para el normal funcionamiento de la plataforma tecnológica.
	Acceso no autorizado a sistemas de información	Grave	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma tecnológica.

5 Conclusiones y recomendaciones

5.1 CONCLUSIONES

El sistema integrado de gestión para la casa del ingeniero a través de sus diferentes análisis logró:

- La elaboración de la correlación nos permitió identificar claramente los requisitos comunes y específicos para cada norma, y nos demostró que para este diseño la norma que primó fue la ISO 9001:2015, por especificar de mejor manera los requisitos comunes para las la integración del sistema.
- Por medio del diagnóstico realizado a través de la lista de chequeo pudimos evidenciar de manera integral que el cumplimiento de los numerales no eran aceptables, lo que nos permitió de cierta forma orientar la propuesta hacia la documentación de algunas actividades para dar un mejor cumplimiento a la norma.
- Por medio de la entrevista al gerente de la organización y el desarrollo del FODA, evidenciamos el contexto interno y externo y diseñamos la estrategia de la organización, de la misma manera que engranamos los sistemas de gestión a ella a través de los objetivos que se desplegaron de la estrategia.
- Con la matriz de partes interesadas identificamos los requisitos pertinentes a cada una de ellas, dando una visión a La Casa del Ingeniero más amplia de a quienes posiblemente pueden afectar a través de la ejecución de las actividades.
- El desarrollo y mantenimiento de una política de gestión integrada permite enfocar y dar cumplimiento a todo el desarrollo de los procesos organizacionales.
- El diseño del mapa de procesos permite orientar a la organización y sus partes interesadas en un escenario que les permite visualizar la interacción entre cada uno de los procesos.
- La caracterización de los procesos 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.
- La herramienta diseñada para el control integral del sistema, permite a la organización mantener de forma centralizada y organizada la información pertinente al sistema integrado de gestión.

5.2 RECOMENDACIONES

- Aplicar una metodología para la identificación de riesgos de Seguridad de la Información, apropiada al tamaño de la 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 plasmados en el mapa de procesos.

- 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 implantación correcta del sistema integrado de gestión, que en cualquier momento que la organización decida, este material contribuirá para la acreditación o certificación del modelo implantado.

Bibliografía

1. http://www.uv.es/webgid/Descriptiva/331_mtodos.html
2. http://qualitytrends.squalitas.com/articulos/articulos-gestion-de-la-calidad/item/108-sistemas-de-gesti%C3%B3n-de-la-calidad-%E2%80%93-un-camino-hacia-la-satisfacci%C3%B3n-del-cliente-%E2%80%93-parte-i.html
3. http://www.bureauveritas.es/services+sheet/certificacion+iso+9001
4. http://www.iso27000.es/sgsi.html.
5. http://advisera.com/27001academy/es/que-es-iso-27001/
6. http://datateca.unad.edu.co/contenidos/358049/Modulo_en_linea/leccin_22_lista_de_chequeo.html
7. http://www.matrizfoda.com/home.html
8. ESPECIALIZACION GESTION INTEGRADA QHSE, GERENCIA DE PROYECTOS, Matriz_de_Stakeholders_-_Guia.docx- cohorte N° 34 - ESCUELA COLOMBIANA DE INGENIERIA

ANEXOS

ANEXO A.

CORRELACIÓN DE LAS NORMAS ISO 9001 e ISO 27001					
ISO 9001:2015		**ISO 27001:2013**		**DIFERENCIAS**	**NORMA BASE PARA REDACCIÓN**
0.	Introducción	**0**	Introducción	N/A	N/A
0.1	Generalidades	**0.1**	Generalidades	N/A	N/A
0.2	Principios de la gestión de la calidad			N/A	N/A
0.3	Enfoque a procesos			N/A	
0.4	Relación con otras normas de sistemas de gestión	**0.2**	Compatibilidad con otras normas de sistemas de gestión	N/A	
1.	Objeto y campo de aplicación	**1.**	Objeto y campo de aplicación	N/A	N/A
2.	Referencias normativas	**2.**	Referencias normativas	N/A	N/A
3.	Términos y definiciones	**3.**	Términos y definiciones	N/A	N/A

4.	Contexto de la organización	**4.**	Contexto de la organización	Titulo	
4.1	Comprensión de la organización y de su contexto	**4.1**	Conocimiento de la organización y de su contexto	La ISO 27001 hace una NOTA adicional, no referida en la ISO 9001 que cita "La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la organización, considerado en el numeral 5.3 de la NTC-ISO 31000:2011[5]."	ISO 9001:2015
4.2	Comprender las necesidades y expectativas de las partes interesadas	**4.2**	Comprensión de las necesidades y expectativas de las partes interesadas	No hay diferencias.	ISO 9001:2015
4.3	Determinación del alcance del sistema de gestión de la calidad	**4.3**	Determinación del alcance del sistema de gestión de la seguridad de la información	La ISO 27001 en su numeral c) establece "las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones."	ISO 9001:2015

				La ISO 9001 agrega 3 párrafos, en los que establece la aplicabilidad de los requisitos y la conformidad de los mismos para no afectar la capacidad o responsabilidad de la organización.	
4.4	Sistema de Gestión de la calidad y sus procesos	**4.4**	Sistema de gestión de la seguridad de la información	La ISO 9001 determina 10 numerales de requisitos, mientras que la ISO 27001 detalla en un párrafo lo siguiente "La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma."	ISO 9001:2015
5.	Liderazgo	**5.**	Liderazgo	Titulo	
5.1	Liderazgo y	**5.1**	Liderazgo y	La ISO 9001 enuncia dos literales adicionales que	ISO 9001:2015

	compromiso		compromiso	no aparecen en la ISO 27001, los cuales son literal a) y el literal d) del numeral 5.1.1. La ISO 27001 no hace mención al enfoque al cliente de la cual la ISO 9001 lo menciona en su numeral 5.1.2.	
5.2	Política	**5.2**	Política	La ISO 9001 hace mención en el literal a) del numeral 5.2.1 “sea apropiada al propósito y contexto de la organización y apoye su dirección estratégica”, lo que en ISO 27001 únicamente especifica que sea “adecuada al propósito de la organización”.	ISO 9001:2015
5.3	Roles, responsabilidades y autoridades en la organización	**5.3**	Roles, responsabilidades y autoridades en la organización	La ISO 9001 especifica de manera más detallada, incluyendo en su primer párrafo que “se entiendan en toda la organización”. Adicionalmente incluye	ISO 9001:2015

				los numerales b), d) y e), no mencionados en la ISO 27001.	
6.	Planificación	**6.**	Planificación	Titulo	
6.1	Acciones para abordar riesgos y oportunidades	**6.1**	Acciones para tratar riesgos y oportunidades	La ISO 9001 incluye el numeral b) que menciona “aumentar los efectos deseables” e incluye dos NOTAS al final del numeral 6.1.2 aclarando las opciones para abordar riesgos y oportunidades. En este caso en especial la ISO 27001 detalla de manera específica en dos numerales adicionales a los de ISO 9001, la valoración de los riesgos y el tratamiento de los mismos en los numerales 6.1.2 y 6.1.3 especificando de manera más amplia el requisito, por lo tanto prima en este	ISO 27001:2013

				caso la ISO 27001 para la redacción.	
6.2	Objetivos de la calidad y planificación para lograrlos	**6.2**	Objetivos de seguridad de la información y planes para lograrlos	La ISO 9001 adiciona con respecto a la 27001 en este numeral en su primer párrafo "y los procesos necesarios para el sistema de gestión de calidad" lo que en 27001 está reflejado únicamente para "funciones y niveles pertinentes". En numeral d) de esta misma norma se contempla adicionalmente que los objetivos deben ser "pertinentes para la conformidad de los productos y servicios y para el aumento de la satisfacción del cliente". La ISO 27001 contempla adicionalmente en el literal c) los resultados de la valoración y el	ISO 9001:2015 e ISO 27001:2013

				tratamiento de los riesgos.	
6.3	Planificación de los cambios			No existe numeral, por lo tanto prima la ISO 9001 para la redacción de los requisitos.	ISO 9001:2015
7.	Apoyo	**7.**	Soporte	Titulo	
7.1	Recursos	**7.1**	Recursos	La ISO 27001 detalla de manera muy sencilla los requisitos para los recursos del sistema de gestión en un solo párrafo; mientras que la ISO 9001 detalla en 4 subnumerales con sus respectivos literales los detalles para considerar a las personas, infraestructura, ambiente, recursos de seguimiento y medición y conocimientos de la organización.	ISO 9001:2015

7.2	Competencia	**7.2**	Competencia	Mismos requisitos	ISO 9001:2015
7.3	Toma de Conciencia	**7.3**	Toma de conciencia	La ISO 9001 incluye un literal adicional que menciona "los objetivos de calidad pertinentes"	ISO 9001:2015
7.4	Comunicación	**7.4**	Comunicación	La ISO 27001 especifica una estructura similar de comunicación a la de ISO 9001, pero esta primera es mucho más concreta respecto a la forma de comunicar interna y externamente los temas pertinentes al sistema de gestión, ya que determina que se incluya el contenido y los procesos para llevar a cabo la comunicación.	ISO 27001:2013
7.5	Información documentada	**7.5**	Información documentada	La ISO 9001 especifica en su último párrafo que "la información documentada conservada como evidencia de la conformidad debe protegerse contra modificaciones no	ISO 9001:2015

				intencionadas".	
8.	Operación	**8.**	Operación	Titulo	
8.1	Planificación y control operacional	**8.1**	Planificación y control operacional	La ISO 9001 detalla de manera más específica los requisitos para este numeral	ISO 9001:2015
8.2	Requisitos para los productos y servicios	**8.2**	Valoración de riesgos de la seguridad de la información	Requisitos diferentes	ISO 9001:2015 e ISO 27001:2013
8.3	Diseño y desarrollo de los productos y servicios	**8.3**	Tratamiento de riesgos de la seguridad de la información	Requisitos diferentes	ISO 9001:2015 e ISO 27001:2013
8.4	Control de los procesos, productos y servicios suministrados externamente			No existe numeral en la ISO 27001, por lo tanto prima la ISO 9001 para la redacción de los requisitos.	ISO 9001:2015
8.5	Producción y provisión del servicio			No existe numeral en la ISO 27001, por lo tanto prima la ISO 9001 para la redacción de los requisitos.	ISO 9001:2015

8.6	Liberación de los productos y servicios			No existe numeral en la ISO 27001, por lo tanto prima la ISO 9001 para la redacción de los requisitos.	ISO 9001:2015
8.7	De las salidas no conformes			No existe numeral en la ISO 27001, por lo tanto prima la ISO 9001 para la redacción de los requisitos.	ISO 9001:2015
9.	Evaluación del desempeño	**9.**	Evaluación del desempeño	Titulo	
9.1	Seguimiento, medición, análisis y evaluación	**9.1**	Seguimiento, medición, análisis y evaluación	La ISO 27001 es más específica en este numeral respecto a la ISO 9001, ya que incluye en su literal a) “los procesos y los controles de la seguridad de la información” e incluye dos literales adicionales sobre los cuales hace mención de cuándo y quienes deben realizar el seguimiento, la medición, el análisis y la evaluación.	ISO 9001:2015 e ISO 27001:2013

				La ISO 9001 en dos subnumerales especifica los requisitos para la satisfacción del cliente, y el análisis y evaluación.	
9.2	Auditoría interna	**9.2**	Auditoría interna	La ISO 9001 agrega un literal en este numeral añadiendo “realizar las correcciones y tomar las acciones correctivas adecuadas sin demora injustificada”.	ISO 9001:2015
9.3	Revisión por la dirección	**9.3**	Revisión por la dirección		ISO 9001:2015 e ISO 27001:2013
10.	Mejora	**10.**	Mejora	Titulo	
10.1	Generalidades			La ISO 27001 no especifica este numeral	ISO 9001:2015
10.2	No conformidad y acción correctiva	**10.1**	No conformidad y acción correctiva	La ISO 9001 determina en el inicio de su párrafo un adicional de ”incluida cualquiera originada por quejas”, no especificada	ISO 9001:2015

				en la ISO 27001, adicionalmente la 9001 especifica en el literal b) numeral 1) el "análisis de la no conformidad" y en el numeral e) que tampoco está incluido en la 27001 que define "si fuera necesario, actualizar los riesgos y oportunidades, determinados durante la planificación.	
10.3	Mejora continua	**10.2**	Mejora continua	La ISO 9001 considera adicionalmente "los resultados del análisis y la evaluación, y las salidas de la revisión por la dirección, para determinar si hay necesidades u oportunidades que deben considerarse como parte de la mejora continua.	ISO 9001:2015

ANEXO B.

LISTA DE CHEQUEO INTEGRADA					
Nral	**ISO 9001:2015**	**ISO 27001:2013**	**CUMPLE**		**OBSERVACIONES**
			SI	**NO**	
4	**Contexto de la organización**				
4.1	**Comprensión de la organización y su contexto**	**Conocimiento de la organización y de su contexto**			
	¿La organización ha realizado análisis de contexto?			1	
	¿La organización hace seguimiento y revisión a los resultados de este análisis?			1	
4.2	**Comprensión de las necesidades y expectativas de las partes interesadas**	**Comprender las necesidades y e1pectativas de las partes interesada**			
	¿Están determinadas las partes interesadas y sus requisitos con respecto al sistema de gestión?			1	
4.3	**Determinación del alcance del sistema de gestión de la calidad**	**Determinación del alcance del sistema de gestión de la seguridad de la información**			
	¿Existe información documentada del alcance del sistema de gestión y se encuentra disponible?		1		
	¿El alcance considera las cuestiones internas y externas que influyen con su propósito y direccionamiento estratégico?		1		
	¿El alcance considera los requisitos de las partes		1		

	interesadas del sistema?				
	¿El alcance considera los productos y servicios de la organización?		1		
	Sistema de gestión de la calidad y sus procesos	**Sistema de gestión de la seguridad de la información**			
	¿La organización tiene definidos los procesos necesarios y sus interacciones?		1		
	¿Están determinadas las entradas y salidas de los procesos?		1		
	¿Existen métodos o criterios para asegurarse que la operación es eficaz y los procesos están controlados?		1		
4.4	¿Se determinan recursos suficientes para cada uno de los procesos y se tiene asegurada su disponibilidad?		1		
	¿Los procesos cuentan con responsables y autoridad definidas?		1		
	¿Los riesgos y oportunidades están determinados y cuentan con acciones a tomar?			1	
	¿Se evalúan los procesos para asegurarse de que cumplen los resultados previstos?			1	
	¿Se mantiene información documentada que apoye la operación de los procesos?		1		
	¿Se conserva información documentada de la operación de los procesos?			1	
	TOTAL CAPITULO		**10**	**6**	
5	**Liderazgo**				
5.1	**Liderazgo y compromiso**	**Liderazgo y compromiso**			

	¿La alta dirección asume la responsabilidad y la obligación de rendir cuentas con respecto al sistema de gestión?			1	
	¿La alta dirección se asegura de que la política y los objetivos del sistema de gestión son compatibles con el contexto y la dirección estratégica de la organización?			1	
	¿La alta dirección se asegura de la integración de los requisitos del sistema de gestión con los procesos del negocio?			1	
	¿Se comunica la importancia de un sistema de gestión eficaz de acuerdo a los requisitos del sistema?			1	
	¿Se logran los resultados previstos del sistema de gestión?			1	
	¿Se dirige y apoya a las personas para lograr los objetivos del sistema de gestión?			1	
	Enfoque al cliente				
	¿Se determinaron los requisitos del cliente y los legales aplicables?	N/A		1	Están definidos los requisitos legales aplicables, pero no los específicos del cliente
	¿Se determinaron los riesgos y oportunidades que pueden afectar la conformidad de los productos y servicios?	N/A		1	
	¿El personal está enfocado en el aumento de la satisfacción del cliente?	N/A	1		

	Política	**Política**			
5.2	¿La política es apropiada al contexto de la organización y apoya su dirección estratégica?			1	No e1iste planificación estratégica
	¿La política proporciona un marco de referencia para establecer los objetivos del sistema de gestión?			1	
	¿La política Incluye un compromiso de cumplir con los requisitos aplicables?		1		
	¿La política incluye un compromiso de mejora continua?		1		
	¿La política de encuentra documentada y está disponible?		1		
	¿Se comunica, entiende y aplica la política?		1		
	¿Está disponible para las partes interesadas?			1	
5.3	**Roles, responsabilidades y autoridades en la organización**	**Roles, responsabilidades y autoridades en la organización**			
	¿Se cuenta con los roles definidos para asegurarse que el sistema de gestión es conforme con los requisitos?			1	
	¿Las responsabilidades y autoridades están asignadas y son comunicadas para asegurarse de que los procesos están generando las salidas previstas?		1		
	¿Las responsabilidades y autoridades están designadas para informar sobre el desempeño del sistema a la alta dirección, promoviendo el enfoque al cliente y asegurando la integridad del sistema de gestión?			1	
		TOTAL CAPITULO	**6**	**13**	
6.1	**Acciones para abordar**	**Acciones para tratar**			

	riesgos y oportunidades	**riesgos y oportunidades**			
	¿Se asegura que el sistema de gestión pueda lograr los resultados deseados?			1	
	¿Se toman acciones para aumentar los efectos deseables?			1	
	¿Se toman acciones para prevenir los efectos no deseables?			1	
	¿Se planifica la manera de integrar e implementar las acciones de los procesos?			1	
	¿Se evalúa la eficacia de estas acciones?			1	
	¿Existe alguna metodología para valorar los riesgos de seguridad de la información?				
	¿Existe algún método para realizar el tratamiento a los riesgos con respecto a la seguridad de la información?			1	
6.2	**Objetivos de la calidad y planificación para lograrlos**	**Objetivos de seguridad de la información y planes para lograrlos**			
	¿Los objetivos son coherentes con la política?			1	
	¿Los objetivos son medibles?			1	
	¿Se tienen en cuenta lo requisitos aplicables?			1	
	¿Están de acuerdo para aumentar la satisfacción del cliente?			1	
	¿Son objeto de seguimiento?			1	
	¿Se comunican dentro de la organización?			1	
	¿Se encuentran documentados los objetivos?			1	

	¿Se planifica que se va a hacer con los objetivos?			1	
	¿Se tienen determinados que recursos requerirán?			1	
	¿Están definidos los responsables de lograr los objetivos?			1	
	¿Se estimó la fecha de terminación del objetivo?			1	
	¿De qué manera se evalúan los resultados?			1	
6.3	**Planificación de los cambios**	**N/A**			
	¿Se considera el propósito de los cambios?	N/A		1	
	¿Se considera la integridad de los sistemas de gestión?	N/A		1	
	¿Se considera la disponibilidad de recursos?	N/A		1	
	¿Se considera la asignación o reasignación de responsabilidades?	N/A		1	
	TOTAL CAPITULO		**0**	**22**	
7	**Apoyo**	**Soporte**			
7.1	¿La organización proporciona los recursos necesarios para el sistema de gestión?			1	
	¿Se consideran las capacidades y limitaciones de los recursos internos?			1	
	¿Se tiene en consideración las necesidades de la organización respecto a lo que los proveedores ofrecen?			1	
	¿La organización cuenta con las personas necesarias para la implementación eficaz del sistema y la operación y control de sus procesos?			1	
	¿La organización cuenta con la infraestructura				

	necesaria para la operación de sus procesos lograr productos y servicios conformes?	1		
	¿El ambiente en el que operan los procesos es adecuado para lograr la conformidad de los productos y servicios?	1		
	¿Se asignan recursos necesarios para asegurar la validez y fiabilidad de los resultados cuando se realiza seguimiento y medición?		1	En estos casos la organización por tratarse de una empresa de tecnología, realiza controles de verificación y validación en sus procesos.
	¿Los recursos asignados son apropiados?		1	
	¿Se mantienen para asegurar la idoneidad de su propósito?		1	
	¿Están determinados que conocimientos son necesarios para la operación de los procesos?	1		
	¿Estos conocimientos están a disposición cuando es necesario?	1		
	¿La organización considera los cambios y las nuevas tendencias y determina como adquirir o acceder a los conocimientos adicionales?		1	
7.2	**Competencia** **Competencia**			
	¿La organización determino la competencia necesaria de las personas que realizan trabajos que afectan el desempeño y la eficacia del sistema de gestión?		1	
	¿La organización se asegura de que estas personas son competentes basándose en educación, formación o experiencia apropiadas?		1	
	¿Se toman acciones para adquirir la competencia		1	

	adecuada y evaluar su eficacia?			
	¿Se conserva información documentada de la competencia de las personas?		1	
7.3	**Toma de conciencia** **Toma de conciencia**			
	¿Las personas son conscientes de la política y los objetivos de la organización?		1	
	¿Las personas son cocientes de su contribución al sistema de gestión y los beneficios de mejorar el desempeño?		1	
	¿Las personas son conscientes de las consecuencias incumplir los requisitos?		1	
7.4	**Comunicación** **Comunicación**			
	¿La organización determino que, cuando, a quien, como y quien comunica interna y externamente lo pertinente al sistema de gestión?		1	
	¿se tiene determinado el contenido de las comunicaciones y el proceso para llevarlas a cabo?		1	
7.5	**Información documentada** **Información documentada**			
	¿La organización cuenta con información documentada para garantizar la eficacia del sistema de gestión?		1	E1iste información documentada que parcialmente gestiona la eficacia del sistema.
	¿La información documentada está protegida contra modificaciones?		1	
	¿La información documentada contiene la identificación, descripción y formato según las necesidades?			
	¿Se revisa y aprueba la información documentada?		1	
	¿La información documentada está disponible y es	1		

	idónea para su uso cuando se necesite?				
	¿Se protege adecuadamente?			1	
	¿El control de distribución, almacenamiento y preservación se realiza?			1	
	¿Se realizan control de cambios?			1	
	TOTAL CAPITULO		**5**	**23**	
8	**Operación**				
8.1	**Planificación y control operacional**	**Planificación y control operacional**			
	¿Se determinaron los requisitos de productos y servicios?		1		
	¿Existen criterios para los procesos y la aceptación de productos y servicios?			1	
	¿Se tienen destinados recursos para lograr conformidad de los requisitos de productos y servicios?			1	
	¿De acuerdo a los criterios de los procesos, existen controles implementados?			1	
	¿Se conserva información documentada para demostrar que los procesos se han llevado según lo planificado y que los productos y servicios son conformes?			1	
	¿Se tiene control de los procesos contratados externamente?			1	
8.2	**Requisitos para los productos y servicios**	**Valoración de riesgos de la seguridad de la información**			
	¿La organización proporciona información relativa a		1		

	los productos y servicios ofrecidos?				
	¿La organización trata las consultas, contratos, pedidos o cambios?		1		
	¿La organización obtiene retroalimentación de los clientes en relación a sus productos o servicios?			1	
	¿la organización manipula o controla la propiedad del cliente?		1		
	¿La organización establece planes o acciones de contingencia en casos específicos?			1	
	¿Se llevan a cabo a intervalos planificados valoraciones de riesgos y se conservan registros?				
	¿La organización define los requisitos para los productos y servicios incluyendo los legales y reglamentarios aplicables?	N/A	1		
	¿La organización se asegura de cumplir con los productos y servicios ofrecidos?	N/A	1		
	¿Antes de comprometerse a suministrar productos y servicios la organización se asegura de poder cumplir con lo ofrecido a los clientes?	N/A		1	
	¿Se revisan los requisitos especificados por el cliente, incluyendo los requisitos para actividades en entrega y posteriores?	N/A		1	

	¿Se revisan los requisitos no establecidos por el cliente, pero necesarios para el uso previsto cuando sea necesario?	N/A		1	
	¿Se revisan los requisitos especificados por la organización?	N/A		1	
	¿Se revisan los requisitos legales y reglamentarios aplicables?	N/A	1		
	¿Se revisan y resuelven las diferencias existentes entre lo solicitado y lo expresado previamente?	N/A	1		
	¿Se conserva información documentada sobre los resultados de la revisión y requisitos nuevos para los productos y servicios?	N/A		1	
	¿Cuándo se cambian los requisitos, la información documentada es modificada y el personal involucrado es consciente de los cambios?	N/A		1	
8.3	**Diseño y desarrollo de los productos y servicios**				

	¿Se determinan las etapas del proceso requeridas, incluyendo revisiones?	N/A		1	
	¿Se cuenta con actividades planificadas de verificación y validación del diseño y desarrollo?	N/A	1		
	¿Se designaron las responsabilidades y autoridades dentro del proceso de diseño y desarrollo?	N/A		1	
	¿Se designan recursos internos y externos para el diseño y desarrollo?	N/A	1		
	¿Se tiene en cuenta la necesidad de controlar las interfaces entre personas que participan en el proceso de diseño y desarrollo?	N/A		1	
	¿Participan clientes y usuarios en el proceso de diseño y desarrollo?	N/A	1		
	¿Se determinan requisitos para la posterior provisión de productos y servicios?	N/A	1		
	¿Los clientes y otras partes interesadas poseen algún nivel de control dentro del proceso de diseño y desarrollo?	N/A		1	

	¿Se cuenta con información documentada para demostrar que se han cumplido los requisitos del diseño y desarrollo?	N/A		1	
	¿Se determinaron cuáles son los requisitos funcionales y de desempeño?	N/A	1		
	¿Existe información previa de actividades de diseño y desarrollo similares?	N/A	1		
	¿Se tiene en cuenta los requisitos legales y reglamentarios?	N/A	1		
	¿Se consideran normas o códigos de prácticas que la organización se ha comprometido a implementar?	N/A		1	
	¿Se consideran las posibles consecuencias potenciales de fallar?	N/A		1	
	¿Se conserva información documentada de estas actividades?	N/A		1	
	¿Se tienen definidos los resultados a lograr?	N/A	1		

	¿Se realiza revisión para evaluar la capacidad de los resultados del diseño y desarrollo?	N/A		1	
	¿Se realizan actividades de verificación durante el diseño y desarrollo?	N/A	1		
	¿Se realizan actividades de validación durante el diseño y desarrollo?	N/A	1		
	¿Se toman acciones para solucionar los problemas presentados durante las revisiones, verificaciones o validaciones?	N/A	1		
	¿Se conserva información documentada de las actividades?	N/A		1	
	¿Las salidas cumplen los requisitos de las entradas?	N/A	1		
	¿Las salidas son adecuadas para los procesos posteriores?	N/A	1		
	¿Se incluye o hace referencia a los requisitos de seguimiento y medición?	N/A	1		
	¿Se especifican características de los productos y servicios esenciales previstos?	N/A	1		

	¿Se conserva información documentada de estas actividades?	N/A		1	
	¿Se conserva información documentada sobre los cambios, los resultados, la autorización, y las acciones tomadas?	N/A		1	
8.4	**Control de los procesos, productos y servicios suministrados externamente**				
	¿Se cuenta con un control cuando los productos y servicios de proveedores externos están destinados a incorporarse al producto o servicio propios?	N/A		1	
	¿Se controlan los productos o servicios proporcionados directamente a los clientes, por proveedores externos en nombre de la organización?	N/A		1	
	¿Se tiene control cuando un proveedor externo proporciona un proceso o una parte de un proceso?	N/A		1	
	¿Se cuenta con un proceso de evaluación y selección de proveedores?	N/A		1	

	¿La organización se asegura que cuando tiene procesos suministrados externamente, permanecen dentro del control de su sistema de gestión?	N/A		1	
	¿La organización tiene definidos los controles a aplicar a proveedores externos y a las salidas resultantes?	N/A		1	
	¿Se ha determinado la verificación para asegurarse que los procesos o servicios suministrados externamente cumplen los requisitos?	N/A		1	
	¿La organización comunica a los proveedores externos los requisitos para: aprobar productos, servicios, métodos, procesos, equipos y la liberación de productos y servicios?	N/A	1		
	¿Se comunica la competencia requerida de las personas?	N/A	1		
	¿Se comunica las interacciones del proveedor con la organización?	N/A	1		

	¿Se comunica del control y el desempeño del proveedor externo a aplicar por parte de la organización?	N/A		1	
	¿Se comunican las actividades de verificación y validación que se pretenden llevar a cabo en las instalaciones del proveedor externo?	N/A		1	
8.5	**producción y provisión del servicio**				
	¿Se cuenta con información documentada que defina las características de los productos y los resultados a alcanzar?	N/A		1	
	¿Se dispone de recursos de seguimiento y medición adecuados?	N/A		1	
	¿Se tiene implementado actividades de seguimiento y medición para verificar el cumplimiento de los criterios del control de los procesos o sus salidas?	N/A		1	
	¿Se tiene la infraestructura necesaria para la operación de los procesos?	N/A	1		

	¿Están designadas las personas competentes?	N/A	1		
	¿Se valida y revalida la capacidad para alcanzar los resultados planificados cuando las salidas no puedan verificarse mediante seguimiento y medición?	N/A	1		
	¿Se cuentan con acciones implementadas para prevenir errores humanos?	N/A		1	
	¿Existen implementadas actividades de liberación y entrega?	N/A		1	
	¿Se identifican las salidas de cada proceso?	N/A		1	
	¿Se identifica el estado de cada salida de los procesos?	N/A		1	
	¿Se controla con una identificación única las salidas de los procesos y se conserva información documentada de estas actividades?	N/A		1	
	¿se identifica, verifica, protege y salvaguarda la propiedad de los clientes o proveedores externos?	N/A	1		
	¿se comunican las novedades como perdidas,	N/A	1		

	daños, deterioros de la propiedad y se conservan registros de ello'				
	¿Se protegen las salidas durante la producción o prestación del servicio?	N/A	1		
	¿Las actividades posteriores a la entrega establecen los requisitos legales y reglamentarios, las consecuencias potenciales no deseadas, la naturaleza, uso y vida útil del producto, los requisitos y la retroalimentación del cliente?	N/A		1	
	¿Se conserva información documentada de los resultados de la revisión de los cambios, las personas que autorizaron y cualquier acción necesaria?	N/A		1	
8.6	**Liberación de los productos y servicios**				
	¿La organización conserva evidencia de la conformidad con los criterios de aceptación?	N/A	1		
	¿Se tiene información documentada de la	N/A	1		

	trazabilidad de las personas que autorizan la liberación?				
	Control de las salidas no conformes				
8.7	¿Se identifican y se controlan las salidas no conformes para prevenir su uso no intencional?	N/A		1	
	¿Las salidas no conformes se tratan de alguna manera?	N/A		1	
	¿Se conserva información documentada de la no conformidad, las acciones y la autoridad con respecto a esta?	N/A		1	
	TOTAL CAPITULO		**34**	**47**	
9.	**Evaluación del desempeño**				
9.1	**Seguimiento, medición, análisis y evaluación**	**Seguimiento, medición, análisis y evaluación**			
	¿Se tiene determinado que necesita seguimiento y medición, incluyendo los controles de seguridad de la información?			1	
	¿Existen métodos de seguimiento, medición, análisis y evaluación?			1	
	¿Se cuenta con frecuencias para llevar a cabo el seguimiento y medición?			1	
	¿Se cuenta con una frecuencia para analizar y evaluar los resultados?			1	
	¿La organización hace seguimiento a las percepciones de los clientes, del grado en el que se			1	

	cumplen sus necesidades y expectativas?			
	¿Se analizan y evalúan los datos que surgen del seguimiento y la medición?		1	
9.2	**Auditoria interna** **Auditoria interna**			
	¿Se llevan a cabo auditorías a intervalos planificados?		1	
	¿Se cuenta con un programa de auditoria?		1	
	¿Se definen los criterios de auditoria?		1	
	¿Existe un equipo de auditores para llevar a cabo las mismas?		1	
	¿Se informan los resultados de las auditorías a la dirección pertinente?		1	
	¿Se realizan correcciones y acciones correctivas sin demora injustificada?		1	
	¿Se conserva información documentada de estas actividades?		1	
9.3	**Revisión por la dirección** **Revisión por la dirección**			
	¿La alta dirección revisa periódicamente el Sistema de Gestión, para asegurar que haya conveniencia, adecuación y eficacia continua?		1	
	¿Se conservan los registros de la revisión por la dirección?		1	
	¿Las revisiones incluyen la evaluación de oportunidades de mejora y las necesidades de los cambios a efectuar en el Sistema de Gestión?		1	
	¿Se consideran como entradas en la revisión los resultados de las auditorías internas y evaluaciones de cumplimiento de los requisitos legales y otros?		1	
	¿Se consideran como entradas en la revisión las		1	

	comunicaciones de las partes interesadas externas?				
	¿Se consideran como entradas en la revisión el desempeño del sistema de gestión de la organización?			1	
	¿Se consideran como entradas en la revisión el grado de cumplimiento de los objetivos y metas?			1	
	¿Se consideran como entradas en la revisión el estado de las acciones correctivas y preventivas?			1	
	¿Se consideran como entradas en la revisión el seguimiento de las acciones resultantes de las revisiones previas por parte de la dirección?			1	
	¿Se consideran como entradas en la revisión los cambios en las circunstancias, incluyendo la evolución de los requisitos legales y otros requisitos relacionados con el sistema de gestión?			1	
	¿Se consideran como entradas en la revisión las recomendaciones para la mejora?			1	
	¿Los resultados de la revisión por parte de la dirección incluyen las decisiones y acciones tomadas relacionadas con los posibles cambios en la política, objetivos, metas y otros elementos del Sistema de Gestión?			1	
	TOTAL CAPITULO		**0**	**25**	
10.1	**Mejora (generalidades)**				
	¿La organización determina y selecciona oportunidades de mejora con el fin de aumentar la satisfacción del cliente?	N/A		1	
10.2	**No conformidad y acción correctiva**				
	¿La organización reacciona ante las no			1	

	conformidades y toma acciones para corregirlas?			
	¿Evalúa la necesidad de acciones para eliminar sus causas?		1	
	¿Implementa las acciones determinadas?		1	
	¿Revisa la eficacia de la acción?		1	
	TOTAL CAPITULO	**0**	**5**	

ANEXO C.

CARACTERIZACIÓN DEL PROCESO DE GESTIÓN COMERCIAL				
1. OBJETIVO: Determinar *las necesidades del cliente en sus requerimientos específicos en el momento de su compra en diseño, mantenimiento o suministros. Teniendo en cuenta los servicios en base a la seguridad de la información.*		**2. ALCANCE:** *Este proceso aplica para las etapas de selección, vinculación, retiro y capacitación de personal de La Casa del Ingeniero.*		
3. RESPONSABLE: *Coordinador de talento humano*		**4. PARTICIPANTES:** *Coordinador de talento humano*		
REQUISITOS				
ISO 9001:2015: 7.4, 7.5, 8.2, 8.5.5, 9.1.2		**ISO 27001:2013:** 7.4, 7.5, 9.1		
5. PROVEEDOR	**6. ENTRADAS**	**7. ACTIVIDADES**	**8. SALIDAS**	**9. CLIENTE**

Cliente	Solicitud de servicio	Presentación del portafolio de los productos y servicios de la casa del ingeniero.	Solicitud de cotización	Cliente
Cliente	Necesidades y requisitos	Análisis de los requisitos y diseño de la propuesta comercial	Propuesta comercial	Cliente
Cliente	Entrega de información de requerimientos	Documentar los requerimientos especificando las características solicitadas para los módulos o el desarrollo del software.	Orden de compra y especificación de requerimientos	Gestión comercial
Gestión comercial	Especificación de requerimientos	Realización del contrato de trabajo y condiciones de la prestación del servicio	Contrato de prestación de servicios	Cliente
Gestión comercial	Seguimiento a requerimientos	Ejecutar un seguimiento a la satisfacción en el cumplimiento de los requisitos solicitados	Encuesta de satisfacción	Cliente

10. DOCUMENTOS: ○ *Procedimiento de gestión comercial* ○ *Portafolio de productos y servicios*	**11. RECURSOS:** • *Humanos* ○ *Personal* • *Físicos* ○ *Oficinas* ○ *Puestos de trabajo*	○ *Equipos de computo* ○ *papelería* • *Tecnológicos* ○ *Software* ○ *Internet* ○ *Dispositivos móviles*
12. REGISTROS: • *Cotización* • *Orden de compra* • *Especificación de requerimientos* • *Encuestas de satisfacción*	**13. INDICADORES:** • *Incrementar el número de clientes* • *Incrementar el portafolio* • *Incrementar los puntos de atención.* • *Aumentar las oportunidades*	

CARACTERIZACIÓN DEL PROCESO DE DESARROLLO DE SOFTWARE				
1. OBJETIVO: ejecutar las actividades para el diseño, desarrollo, supervisión, implementación y entrega de las soluciones ofrecidas por La Casa del Ingeniero.		**2. ALCANCE:** este proceso aplica para las actividades de diseño, desarrollo, supervisión, implementación y entrega de los productos y servicios ofrecidos y desarrollados por La Casa del Ingeniero.		
3. RESPONSABLE: Coordinador de desarrollo de Software		**4. PARTICIPANTES:** Desarrollador de software		
REQUISITOS				
ISO 9001:2015: 7.4, 7.5, 8.1, 8.3, 8.5, 8.6, 8.7		**ISO 27001:2013**: 7.4, 7.5, 8.1, 9.1		
5. PROVEEDOR	**6. ENTRADAS**	**7. ACTIVIDADES**	**8. SALIDAS**	**9. CLIENTE**
Cliente	Especificación de requerimientos	Recibir y/o especificar el requerimiento.	Requerimiento de desarrollo	Desarrollo de software
Gestión comercial	Especificación de requerimientos	Analizar los requerimientos y priorizarlos.	Acta de reunión	Desarrollo de software

Desarrollo de software	Guias, documentación técnica	Planificar el diseño y/o desarrollo.	Términos de referencia	Desarrollo de software
Desarrollo de software	Guias, documentación técnica	Elaborar el diseño y desarrollo de la solución TIC.	Solicitud de ajustes al modelo	Desarrollo de software
Desarrollo de software	Guias, documentación técnica	Revisar el diseño y desarrollo de la solución TIC.	Solicitud de ajustes al modelo	Desarrollo de software
Desarrollo de software	Guias, documentación técnica	Verificar el diseño y desarrollo de la solución TIC.	Solicitud de ajustes al modelo	Desarrollo de software
Desarrollo de software	Guias, documentación técnica	Validar el diseño y desarrollo de la solución TIC.	Reporte de ajustes y observaciones	Desarrollo de software
Desarrollo de software	Reporte de ajustes y observaciones	Implementar la solución TIC	Acta de aceptación de productos.	Cliente

10. DOCUMENTOS:

- *Procedimiento para diseño y desarrollo de software*
- *Procedimiento para revisión, verificación y validación de diseño y desarrollo.*
- *Procedimiento para implementación de soluciones*

11. RECURSOS:

- *Humanos*
  - *Personal*
- *Físicos*
  - *Oficinas*
  - *Puestos de trabajo*
  - *Equipos de computo*
  - *papelería*
- *Tecnológicos*
  - *Software*
  - *Internet*

12. REGISTROS:

- *Requerimiento de desarrollo*
- *Acta de reunión*
- *Términos de referencia*
- *Reporte de ajustes y observaciones*
- *Acta de aceptación de productos.*

13. INDICADORES:

- *Incrementar el cumplimiento de los acuerdos*
- *Reducir las fallas de software*

CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE MANTENIMIENTO

1. OBJETIVO: *Mantener la plataforma tecnológica de los clientes y la propia, para la prestación oportuna de los servicios de LA CASA DEL INGENIERO, reduciendo la generación de riesgos en cuanto al manejo de información y el uso de la misma.*

2. ALCANCE: *este proceso aplica para las actividades de mantenimiento de hardware y software de La Casa del Ingeniero.*

3. RESPONSABLE: *Coordinador de mantenimiento*

4. PARTICIPANTES: *coordinador de mantenimiento*

REQUISITOS

ISO 9001:2015: 4.4, 8.2, 8.5, 8.6, 8.7

ISO 27001:2013:4.4, 8.1, 8.2, 8.3

5. PROVEEDOR	6. ENTRADAS	7. ACTIVIDADES	8. SALIDAS	9. CLIENTE
Clientes externos y procesos internos.	Inventario de equipos informáticos	Establecer la programación para el soporte y mantenimiento de acuerdo a las necesidades de	Programación de soporte y mantenimiento	Clientes externos y procesos internos

		los clientes y la organización		
Clientes externos y procesos internos.	Programación para soporte y mantenimiento	Realizar el mantenimiento de equipos	Equipos en correcta operación	Clientes externos y procesos internos
Clientes externos y procesos internos.	Programación para soporte y mantenimiento	Realizar el mantenimiento de software	Software funcionando correctamente	Clientes externos y procesos internos
Clientes externos y procesos internos.	Programación para soporte y mantenimiento	Hacer backup a los servidores	Información respaldada	Clientes externos y procesos internos
Direccionamiento estratégico	Informes de gestión	Establecer acciones de mejora para el buen funcionamiento	Plan de acción	Direccionamiento estratégico

10. DOCUMENTOS:
• *Plan de acción*
• *Procedimiento para mantenimiento de hardware*
• *Procedimiento para mantenimiento de software*
• *Procedimiento de recuperación de información*
	11. RECURSOS:
	• *Humanos*
	  ○ *Personal*
	• *Físicos*
	  ○ *Equipos de computo*
	  ○ *papelería*
	• *Tecnológicos*
	  ○ *Software*
	  ○ *Internet*

12. REGISTROS: • *Registro de soporte y mantenimiento*	**13. INDICADORES:** • N/A

CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE TALENTO HUMANO				
1. OBJETIVO: *Suministrar el recurso humano requerido por La Casa del Ingeniero, fortalecer las habilidades y aptitudes del individuo, evaluando y fortaleciendo las Competencias para el cumplimiento de los objetivos misionales así como para el normal funcionamiento de los procesos y el manejo seguro de la información.*			**2. ALCANCE***: este proceso aplica para las actividades de selección, vinculación, capacitación y retiro para los empleados de La Casa del Ingeniero.*	
3. RESPONSABLE: *Coordinador de talento humano*			**4. PARTICIPANTES:** *Coordinador de talento humano*	
REQUISITOS				
ISO 9001:2015: 4.1, 4.2, 5.1, 5.2, 5.3 7.1, 7.2, 7.3, 7.4, 7.5			**ISO 27001:2013:** 4.1, 4.2, 5.1, 5.2, 5.3 7.1, 7.2, 7.3, 7.4, 7.5	
5. PROVEEDOR	**6. ENTRADAS**	**7. ACTIVIDADES**	**8. SALIDAS**	**9. CLIENTE**

Todos los procesos	Requerimiento de personal	Convocatoria para selección y vinculación de personal.	Personas aptas seleccionadas para ocupar una vacante.	Todos los procesos
Gestión de talento humano	Plan de capacitación y bienestar social	Desarrollar actividades de recreación, capacitación e inducción de personal.	Personal aptos y competente	Todos los procesos
Todos los procesos	Novedades de nomina	Atender solicitudes de nomina	Nomina actualizada	Todos los procesos
Direccionamiento estratégico	Sistema de gestión de salud y seguridad en el trabajo	Velar por la salud y seguridad de los trabajadores	Personal saludable y operando en condiciones seguras	Todos los procesos
Direccionamiento estratégico	Políticas del sistema integrado de gestión	Apoyar el desarrollo del Sistema de Gestión integrado	Mantenimiento y conservación de información.	Todos los procesos
Direccionamiento estratégico	Plan de auditorías internas	Realizar el seguimiento y evaluación del Sistema de Gestión integrado.	Informes de cumplimiento	Direccionamiento estratégico

10. DOCUMENTOS:

- *Plan de capacitación y bienestar social*
- *procedimiento de selección y vinculación de personal*
- *procedimiento para elaboración de nomina*

11. RECURSOS:

- *Humanos*
  - *Personal*
- *Físicos*
  - *Oficinas*
  - *Puestos de trabajo*
  - *Equipos de computo*
  - *papelería*
- *Tecnológicos*
  - *Software*
  - *Internet*
  - *Dispositivos móviles*

12. REGISTROS:

- *Contratos laborales*
- *Registro de asistencia de actividades de recreación, capacitación e inducción de personal.*
- *Nomina*
- *Informes de cumplimiento*

13. INDICADORES:

- *Eliminar los contratiempos*
- *Aumentar las ideas*
- *Incrementar el nivel de personal*
- *Comunicación asertiva*

CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE COMPRAS	
1. OBJETIVO: *Adquirir de manera oportuna los bienes y servicios requeridos por La Casa del Ingeniero para garantizar el adecuado funcionamiento de sus operaciones.*	**2. ALCANCE:** *este proceso aplica para las actividades de recepción de solicitudes de suministros y finaliza con la entrega oportuna de los mismos.*
3. RESPONSABLE: *Coordinador de compras*	**4. PARTICIPANTES:** *coordinador de compras*
REQUISITOS	
ISO 9001:2015: 8.4.1, 8.4.2, 8.4.3	**ISO 27001:2013:** N/A

5. PROVEEDOR	6. ENTRADAS	7. ACTIVIDADES	8. SALIDAS	9. CLIENTE
Todos los procesos	Solicitud de compras	Gestionar las solicitudes de compras	Cotizaciones	Gestión de compras
Gestión de compras	Selección de proveedores	Selección, evaluación y reevaluación de proveedores.	Calificación de proveedores	Gestión de compras
Proveedores	Productos y servicios adquiridos	Administrar y controlar los productos adquiridos.	Productos verificados	Todos los procesos
Gestión de compras	Control a productos y servicios	Realizar seguimiento a los servicios contratados.	Informe de seguimiento	Gestión de compras
Gestión de compras	Informes de evaluación y seguimiento	Verificar el cumplimiento de los requisitos de los proveedores.	Informe de cumplimiento	Gestión de compras

10. DOCUMENTOS:
- *Procedimiento de gestión de compras*
- *Procedimiento de selección, evaluación y reevaluación de proveedores*
- *Procedimiento de control y seguimiento a productos y servicios contratados.*

11. RECURSOS:
- *Humanos*
  - *Personal*
- *Físicos*
  - *Oficinas*
  - *Puestos de trabajo*
  - *Equipos de computo*
  - *papelería*
- *Tecnológicos*
  - *Software*
  - *Internet*
  - *Dispositivos móviles*

12. REGISTROS:
- *Cotizaciones*
- *Calificación de proveedores*
- *Informe de seguimiento*
- *Informe de cumplimiento*

13. INDICADORES:
- *Incrementar la calidad de los productos y servicios ofrecidos*

CARACTERIZACIÓN DEL PROCESO DE GESTIÓN CONTABLE	
1. OBJETIVO: *Garantizar la correcta administración, ejecución y control de los recursos financieros de La Casa del Ingeniero, controlando la consolidación de la información.*	**2. ALCANCE:** *aplica para las actividades de planeación, elaboración, administración y ejecución del presupuesto de La Casa del Ingeniero.*
3. RESPONSABLE: *Coordinador de contabilidad*	**4. PARTICIPANTES:** *Coordinador de contabilidad*
REQUISITOS	
ISO 9001:2015: 7.4, 7.5.2, 7.5.3, 8.5.2, 9.2, 9.3	**ISO 27001:2013:** 7.4, 7.5.2, 7.5.3, 9.2, 9.3

5. PROVEEDOR	6. ENTRADAS	7. ACTIVIDADES	8. SALIDAS	9. CLIENTE

Todos los procesos	Presupuesto por proceso	Planificación y consolidación del presupuesto.	Aprobación del presupuesto	Todos los procesos
Clientes	Contratos de prestación de servicios	Planificación de los recaudos por prestación de productos y servicios.	Comprobante de pago	Gestión contable
Cliente	Facturas y/o cuentas de cobro Nómina y provisión de prestaciones sociales	Realizar pagos y transferencias	Comprobantes de egreso	Gestión contable
Gestión contable	Balance general	Pago de impuestos	Declaraciones tributarias	Entidades de control
Gestión contable	Estado de resultados	Rendición de informes	Estados financieros	Gestión contable

10. DOCUMENTOS:

- *Procedimiento de planificación de presupuesto*
- *Procedimiento de recaudos y cartera*
- *Procedimiento de facturación*
- *Procedimiento de pago de impuestos*

11. RECURSOS:

- *Humanos*
  - *Personal*
- *Físicos*
  - *Oficinas*
  - *Puestos de trabajo*
  - *Equipos de computo*
  - *papelería*
- *Tecnológicos*
  - *Software*
  - *Internet*
  - *Dispositivos móviles*

12. REGISTROS:

- *Comprobantes de pago*
- *Comprobantes de egreso*
- *Declaraciones tributarias*
- *Estados financieros*
- *presupuesto*

13. INDICADORES:

- *Incrementar el rendimiento*
- *Incrementar los beneficios*

CARACTERIZACIÓN DEL PROCESO DE GESTIÓN TECNOLÓGICA Y DE LA INFORMACIÓN	
1. OBJETIVO: *asegurar la operatividad de la plataforma tecnológica de La Casa del Ingeniero, manteniendo e implementando las tecnologías de la información.*	**2. ALCANCE:** *este proceso aplica para las actividades de solicitud de requerimientos de hardware o software, soporte a usuarios y administración de la plataforma tecnológica de La Casa del Ingeniero.*
3. RESPONSABLE: *Coordinador de tecnologías de la información.*	**4. PARTICIPANTES:** *coordinador de tecnologías de la información*
REQUISITOS	

ISO 9001:2015: 4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.3, 6.1, 6.2, 6.3, 9.1.3, 9.2, 9.3			**ISO 27001:2013: :** 4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.3, 6.1, 6.2, 8.2, 8.3, 9.1, 9.2, 9.3	
5. PROVEEDOR	**6. ENTRADAS**	**7. ACTIVIDADES**	**8. SALIDAS**	**9. CLIENTE**
Direccionamiento estratégico	Contexto estratégico, mapa estratégico.	Planificar las actividades, responsables, recursos, métodos y controles de manera que pueda mantener la operatividad de la plataforma tecnológica	Plan operativo	Direccionamiento estratégico
Procesos de apoyo	Requerimientos y necesidades de software	Investigar nuevas tecnologías y mejores prácticas en tecnología	Infraestructura tecnológica y sistemas de información implementados	Todos los procesos
Clientes	PQR´s	Atender los requerimientos de usuarios	Requerimientos atendidos	Clientes
Direccionamiento estratégico	Políticas del sistema integrado de gestión	Implementar proyectos de innovación y/o mantenimiento y sostenibilidad de la plataforma tecnológica.	Plataforma tecnológica operando adecuadamente	Todos los procesos
Direccionamiento estratégico	Políticas del sistema integrado de gestión	Apoyar el desarrollo del Sistema de Gestión integrado	Mantenimiento y conservación de información.	Todos los procesos
Direccionamiento estratégico	Plan de auditorías internas	Realizar el seguimiento y evaluación del Sistema de Gestión integrado.	Informes de cumplimiento	Direccionamiento estratégico

10. DOCUMENTOS: • *Plan operativo* • *Plan de auditorías internas* • *Políticas del sistema integrado de gestión*	**11. RECURSOS:** • *Humanos* ○ *Personal* • *Físicos* ○ *Oficinas* ○ *Puestos de trabajo*	○ *Equipos de computo* ○ *papelería* • *Tecnológicos* ○ *Software* ○ *Internet* ○ *Dispositivos móviles*
12. REGISTROS: • *Informes de cumplimiento* • *PQR atendidos*	**13. INDICADORES:** • *Incrementar la oportunidad de respuesta al cliente.* • *Reducir los errores operativos* • *Incrementar la oportunidad de respuesta al cliente.*	

ANEXO D.

MATRIZ DE RIESGOS

IDENTIFICACIÓN	ANÁLISIS Y EVALUACIÓN	TRATAR EL RIESGO

Proceso	Riesgo	Descripción del riesgo	Agente generador	Causa	Efecto	Frecuencia	Impacto	Calificación	Evaluación	Tratamiento	Controles
Desarrollo de software	Fallas en la escritura del lenguaje de programación	Posible incumplimiento de requisitos de calidad de software.	Desarrollador de software	Bajo conocimiento o experiencia	Pérdida económica	2	25	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo implementando el control y aseguramiento de calidad
	Perdidas de información	Posible daño a la propiedad del cliente.	Desarrollador de software	Descuido en el manejo o almacenamiento de la información	Sanción legal o económica	1	75	75	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo creando un plan de contingencias y respaldo de información.
	Falta de oportunidad en la respuesta	Posibles demoras en gestionar los requerimientos del cliente.	Desarrollador de software	Falta de información	Quejas y reclamos	3	25	75	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo midiendo y analizando las causas principales para determinar su solución.
	Fallas en el software	Posibles errores en el diseño o desarrollo de software.	Desarrollador de software	Uso inadecuado	Pérdida económica	3	25	75	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo implementando el control y aseguramiento de calidad
	Robo de información	Posible Utilización indebida de información confidencial	Desarrollador de software	Controles deficientes Descuido en el manejo o almacenamiento de la información	Sanción legal o económica	1	100	100	Grave	Prevenir el riesgo, proteger la empresa o transferir el riesgo.	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma tecnológica. Transferir el riesgo a través de una póliza de seguro.

Gestión comercial	Error en la descripción de requisitos	Posibles diseño y desarrollo de software inadecuado	Coordinador comercial	Bajo conocimiento o experiencia	Pérdida económica	2	50	100	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo Validando y verificando la información con el cliente antes de enviarla a diseño y desarrollo.
	Cálculos equivocados	Posibles Costos incorrectos de diseño y desarrollo para el cliente	Coordinador comercial	Falta de información	Pérdida económica Quejas y reclamos	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo diseñando una metodología para evaluar la viabilidad de los requerimientos del cliente.
	Pérdida de clientes	Posible migración de clientes hacia la competencia	Coordinador comercial	Bajo conocimiento o experiencia Mala atención	Pérdida económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo haciendo seguimiento a los objetivos estratégicos de la compañía.
Gestión de mantenimiento	Perdida de información	Posibles daños o perdidas de datos irrecuperables	Coordinador de mantenimiento	Bajo conocimiento o experiencia Método de backup inadecuado	Pérdida económica Sanción legal o económica	1	100	100	Grave	Prevenir el riesgo, proteger la empresa o transferir el riesgo.	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma tecnológica. Transferir el riesgo a través de una póliza de seguro.
	Daño en el software	Posibles daños o perdidas de datos irrecuperables	Coordinador de mantenimiento	Bajo conocimiento o experiencia Método de mantenimiento inadecuado	Pérdida económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo creando un plan de contingencias y respaldo de información.
	Daño en el hardware	Posibles daños o pérdidas de datos irrecuperables.	Coordinador de mantenimiento	Bajo conocimiento o experiencia Método de mantenimiento inadecuado	Pérdida económica Sanción legal o económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo creando un plan de contingencias y respaldo de información.

	Interrupciones del servicio	Posible Caída en el servicio de telecomunicaciones.	Coordinador de mantenimiento	Método de mantenimiento inadecuado	Pérdida económica Sanción legal o económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo creando un plan de contingencias y respaldo de información.
Gestión de talento humano	Accidentes de trabajo	Posible Exposición a peligros en el lugar del trabajo.	Coordinador de talento humano	Falta de conciencia del riesgo, equipos de protección inadecuados, actos inseguros.	Pérdida económica Sanción legal o económica	2	50	100	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Proteger a los trabajadores definiendo la matriz de Identificación de Peligros, Valoración de Riesgos y Determinación de Controles en seguridad y salud ocupacional.
	Monotonía	Posibles Trabajos rutinarios	Coordinador de talento humano	Baja rotación de puestos de trabajo	Baja productividad	1	25	25	Aceptable	Aceptar el riesgo.	Proteger la organización realizando actividades como pausas activas o rotación de puestos de trabajo.
	Insatisfacción laboral	Posible ambiente laboral inapropiado Posible ocupación de cargo incorrecta por parte del personal.	Coordinador de talento humano	Ambiente laboral afectado, presiones, insatisfacción salarial, estrés.	Baja productividad	1	25	25	Aceptable	Aceptar el riesgo.	Proteger la organización diseñando un plan de incentivos a los trabajadores.
	Robo de información	Posible Utilización indebida de información confidencial.	Coordinador de talento humano	Controles deficientes	Pérdida económica Sanción legal o económica	1	100	100	Grave	Prevenir el riesgo, proteger la empresa o transferir el riesgo.	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma tecnológica. Transferir el riesgo a través de una póliza de seguro.

	Errores de nómina o liquidación de prestaciones sociales	Posible incumplimiento de las obligaciones contractuales con los empleados.	Coordinador de talento humano	Descuido en el manejo o almacenamiento de la información	Quejas y reclamos	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo enviando la información a un nivel superior en donde pueda ser revisada y autorizada mensualmente.
Gestión de compras	Error de especificación	Posible Compra de productos o servicios inadecuados	Coordinador de compras	Error de comunicación	Perdida económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo validando y verificando la información con desarrollo de software
	Error en cantidad	Posible compra de productos o servicios en cantidades inadecuadas	Coordinador de compras	Error de comunicación	Quejas y reclamos	1	25	25	Aceptable	Aceptar el riesgo.	Prevenir el riesgo validando y verificando la información con desarrollo de software
	Demoras o retrasos	Posibles retrasos en la llegada o prestación del producto o servicio	Coordinador de compras	Falta de seguimiento	Quejas y reclamos	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo haciendo seguimiento a las solicitudes o requerimientos con el proveedor.
Gestión contable	Generación incorrecta de informes	Posible generación de datos irreales de la organización	Coordinador de contabilidad	Incorrecta contabilización de comprobantes	Pérdida económica Sanción legal o económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo manteniendo y controlando un procedimiento específico para generación de informes.
	Error en la declaración de impuestos	Posible generación de Informes irreales	Coordinador de contabilidad	Bajo conocimiento o experiencia	Pérdida económica Sanción legal o económica	1	75	75	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo manteniendo y controlando un procedimiento específico para la declaración de impuestos.
	Generación incorrecta de comprobantes	Posible facturación incorrecta de ítems	Coordinador de contabilidad	Bajo conocimiento o experiencia	Pérdida económica Sanción legal o económica	1	75	75	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo manteniendo y controlando un procedimiento específico para generación de comprobantes

	Liquidez	Posible falta de liquidez para pago de nómina y prestaciones sociales	Coordinador de contabilidad	Cartera retrasada o mora de usuarios	Quejas y reclamos	1	75	75	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo definiendo un nivel mínimo de liquidez para responder con las obligaciones contractuales de los trabajadores.
Gestión tecnológica y de la información	Cambios en la normatividad relacionada con los requerimientos	Posible incumplimiento de requisitos	Coordinador de tecnologías de la información	Descuido o bajo conocimiento	Sanción legal o económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo a través de la inscripción en newsletters de normatividad legal.
	Asignación de recursos insuficientes	Posible establecimiento de necesidades insuficientes para satisfacer los requerimientos de la plataforma tecnológica.	Coordinador de tecnologías de la información	Estimación incorrecta por falta de información	Pérdida económica	1	50	50	Tolerable	Retener las perdidas, proteger la empresa o prevenir el riesgo	Prevenir el riesgo validando y consultando con los demás procesos las necesidades de requerimientos para el normal funcionamiento de la plataforma tecnológica.
	Acceso no autorizado a sistemas de información	Posible Utilización indebida de información confidencial.	Coordinador de tecnologías de la información	Controles deficientes	Pérdida económica Sanción legal o económica	1	100	100	Grave	Prevenir el riesgo, proteger la empresa o transferir el riesgo.	Evitar el riesgo implementando controles de ingreso de usuarios a la plataforma tecnológica.