GUIA PARA LA EJECUCION DE PROCESOS DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS EN TECNOLOGIAS DE INFORMACION USANDO LA NORMA ISO 31000

INVESTIGADOR

MIGUEL ANGEL ESTREMOR HERRERA

UNIVERSIDAD DE CARTAGENA

FACULTAD DE INGENIERÍA

PROGRAMA INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS D. T y C., 2016

GUIA PARA LA EJECUCION DE PROCESOS DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS EN TECNOLOGIAS DE INFORMACION USANDO LA NORMA ISO 31000

GRUPO DE INVESTIGACIÓN:

GIMATICA

LINEA DE INVESTIGACIÓN:

TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

DIRECTOR - INVESTIGADOR

ING. YASMÍN MOYA VILLA, MSc. (Universidad de Cartagena)

ASESOR

ING. CAMILO ANDRÉS VELASQUEZ (Corplas)

ESTUDIANTE - INVESTIGADOR

MIGUEL ANGEL ESTREMOR HERRERA

UNIVERSIDAD DE CARTAGENA

PROGRAMA INGENIERÍA DE SISTEMAS

FACULTAD DE INGENIERÍA

CARTAGENA DE INDIAS D. T y C., 2016

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

En las últimas décadas se ha notado un aumento del uso de las tecnologías de Información (En algunos casos se denominará TI) (ITU, 2012), debido a que estas facilitan muchos procesos, que de otro modo costarían más dinero y tiempo, además con el uso de estas tecnologías se ha logrado más precisión y mejor rendimiento en relación con el trabajo totalmente manual, de allí que según estadísticas de la Unión Internacional de Telecomunicaciones (ITU) (ITU, 2012). A partir del crecimiento de estas tecnologías se ha hecho evidente una serie de causas de riesgos y amenazas que colocan en peligro la infraestructura de TI utilizada y por ende exponen a riesgos y problemas a quien las utilice, en este caso específico las organizaciones. Algunos de los riesgos que traen consigo las TI no se pueden evitar, ignorarlos o descuidarlos puede causar graves daños y/o pérdidas dentro de las organizaciones, debido a que estas tecnologías suelen soportar procesos importantes, que podrían salir gravemente afectados si ocurre algún fallo.

Este proyecto tuvo como objetivo el desarrollo de una guía, en la que se describe una secuencia de instrucciones para la ejecución de un proceso de evaluación de riesgos de TI, que contribuye con las organizaciones, a realizar de forma correcta el proceso de evaluación de sus riesgos y así colaborar con el cumplimiento de sus objetivos y metas. Este desarrollo se llevó a cabo partiendo de conocimientos existentes para su aplicación. La investigación se enmarcó en una teoría internacionalmente aceptada de la cual se expusieron los conceptos más importantes; finalmente, la situación descrita se evaluó a la luz de esta teoría y se propuso una secuencia de actividades que se encuentran en la guía desarrollada.

El producto final conseguido constituye una guía metodológica que describe procesos y actividades a ejecutar en la gestión de riesgos de TI. Acompañada de otras herramientas desarrolladas (diagramas de flujos, planillas, tablas, etc.) para facilitar su aplicación.

Todo el desarrollo de la guía fue acompañado por personal del área de TI, perteneciente a la entidad CORPLAS (Corporación Plástica S.A.S) del sector productivo de la Región Caribe.

PALABRAS CLAVES

Evaluación de riesgos, Tecnologías de la información, Marcos de trabajo, Estándares.

ABSTRACT

In the last decades there has been an increased use of information technology (in some cases will be referred TI) (International Telecommunication Union, 2012), because these facilitate many processes, which otherwise would cost more money and time, in addition with the use of these technologies it has achieved more precision and better performance in relation to the fully manual work, hence according to statistics from the International Telecommunication Union (ITU) (International Telecommunication Union, 2012). From the increase of these technologies has become evident a number of causes of risks and threats that put in danger the infrastructure used and therefore exposed to risks and problems who use them, in this specific case the organizations. Some of the risks they bring IT can´t avoid, ignore or neglect can cause serious damage and / or loss within organizations, because these technologies are supporting processes of great importance, which could be badly affected if it occurs some failure.

This project aimed at the development of a guide, in which a sequence of instructions for executing a process of risk assessment IT, which contributes organizations, to correctly perform the evaluation process of the described risks and thus collaborate with the fulfillment of its objectives and goals. This development was carried out on the basis of existing knowledge for implementation. The research was part of an internationally accepted theory of which the most important concepts were exposed; finally, the situation described was evaluated in the light of this theory and a sequence of activities that are in the guide developed was proposed.

The final product obtained is a methodological guide describing processes and activities to be implemented in IT risk management. Accompanied by other tools developed (flowcharts, lists, tables, etc.) to facilitate their implementation.

The whole development of the guide was accompanied by staff in the IT area, belonging to the CORPLAS (Plastic Corporation S.A.S) entity of the productive sector of the Caribbean Region.

KEY WORDS:

Risk assessment, Information Technology, Frameworks, Standards

DEDICATORIA

A Dios por recordarme que soy su hijo y brindarme día a día una oportunidad para alcanzar los logros que me he propuesto.

A mi familia por acompañarme, apoyarme e instarme cada día a ser mejor persona y ayudarme a alcanzar cada una de las metas que me he propuesto. A mis padres por su apoyo, por estar presentes en cada momento de este proceso y motivarme en los momentos que sentí desfallecer.

A la ingeniera Yasmìn Moya, por guiarme y acompañarme en la construcción de este proyecto.

A mis amigos por hacer de este período de mi vida más ameno, alentarme y acompañarme a cumplir mis objetivos.

AGRADECIMIENTOS

A Dios primeramente gracias por ser el dador de la vida, y por guiar cada uno de los pasos de esta investigación. A mi familia por motivarme cada vez que sentía desfallecer y acompañarme durante todo este proceso.

A la Empresa Corporación Plástica S.A.S por el espacio y tiempo brindado en el desarrollo de este proyecto.

A la ingeniera Yasmìn Moya Villa, quién durante toda la construcción de este proyecto estuvo ahí para indicarme los aciertos y los errores, guiándome hasta llegar a completarlo todo.

A los evaluadoes, Ing. Humberto Caicedo e Ing. Martín Monroy, por sus aportes y correcciones para sacar adelante este proyecto.

INTRODUCCIÓN

El presente documento, corresponde al proyecto titulado "GUIA PARA LA EJECUCION DE PROCESOS DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS EN TECNOLOGIAS DE INFORMACION USANDO LA NORMA ISO 31000", el cual tuvo como objetivo el desarrollo de una guía de apoyo para las organizaciones del sector industrial de Cartagena en procesos de identificación y evaluación de riesgos en tecnologías de información.

A partir del crecimiento del uso de las tecnologías de la información se ha hecho evidente una serie de causas de riesgos y amenazas que colocan en peligro la infraestructura de TI utilizada y por ende exponen a riesgos y problemas a quien las utilice, en este caso específico las organizaciones. Algunos de los riesgos que traen consigo las TI no se pueden evitar y descuidarlos puede causar graves daños y/o pérdidas dentro de las organizaciones, debido a que estas tecnologías suelen soportar procesos importantes. Por esto es de suma importancia para las organizaciones ejercer controles sobre los riesgos de tecnologías de información que se pueden presentar, según la norma ISO 31000 los riesgos se relacionan directamente con el cumplimiento de los objetivos organizacionales, es decir, controlar los riegos es importante no solo por el factor de prevención que ejerce sobre los activos de la empresa sino también por el aporte al cumplimiento de objetivos. Con base en lo anterior los procesos seleccionados para llevar a cabo la identificación y evaluación de los riesgos deben ser procesos bien fundamentados en los estándares y normas existentes para garantizar la correcta gestión de riesgos. Por ello se planteó la siguiente pregunta de investigación **¿Cómo facilitar el proceso de identificación y evaluación de riesgos de tecnologías de información dentro de las organizaciones siguiendo estándares actuales y usando metodologías de mejora continua?**

Como solución y aporte a la ejecución de estos procesos, se desarrolló una guía fundamentada en normas, modelos y/o estándares de gestión de riesgos de tecnologías de información actuales, que facilita la ejecución de los procesos comprendidos por la gestión de riesgos hasta el proceso de evaluación de riesgos, esta guía fue desarrollada tomando como base principal la norma ISO 31000 y la metodología PHVA, para hacer de estos procesos un ciclo de mejora continua, que al mismo tiempo vincula la evaluación y gestión de los riesgos con el cumplimiento de los objetivos, además contiene un conjunto de planillas estructuradas facilitadoras en la ejecución de los procesos descritos.

Este proyecto hace parte de la área temática TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES del grupo de investigación GIMATICA[1] de la Universidad de Cartagena, para el desarrollo de este proyecto se utilizó temática correspondiente a fundamentos de auditoria de sistemas, específicamente lo concerniente al análisis de los procesos internos de las organizaciones.

1GIMATICA: Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, del Programa Ingeniería de Sistema de la Facultad de Ingeniería de la Universidad de Cartagena.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Desarrollar una guía de apoyo para las organizaciones en los procesos de identificación y evaluación de riesgos en tecnologías de información según los lineamientos de la norma ISO 31000, garantizando su aplicación y mejoramiento a través de la metodología PHVA.

1.2. OBJETIVOS ESPECÍFICOS

- Desarrollar el estado del arte sobre la identificación y evaluación de riesgos de tecnología de información en las organizaciones.

- Describir todas las normas y metodología a utilizar en el proyecto, destacando sus ventajas y desventajas en identificación y evaluación de riesgos de tecnologías de información.

- Definir los procesos de: identificación y clasificación de activos informáticos, identificación, clasificación y evaluación de riesgos teniendo en cuenta la norma ISO 31000 y la aplicación de la metodología PHVA

- Desarrollar una guía donde se describan de forma organizada los pasos que se deben seguir para realizar los proceso de identificación y clasificación de activos e identificación, clasificación y evaluación de riesgos de tecnologías de Información descrito en el objetivo anterior

- Realizar pruebas, mediante la aplicación del proceso descrito en la guía desarrollada, en la Empresa Corporación Plástica S.A.S – CORPLAS, con el fin de verificar y documentar los resultados obtenidos.

2. ALCANCE

La solución propuesta y desarrollada en este proyecto, será de apoyo a las organizaciones del sector industrial en lo correspondiente a la gestión de riesgos, esta puede ser concebida como: un conjunto "*Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo"(ISO, 2011),* dentro de estas actividades deben estar incluidos al menos:

a) Identificación y Clasificación de Activos
b) Identificación de Riegos
c) Análisis o Clasificación de Riesgos
d) Evaluación de Riesgos
e) Desarrollo de Estrategias de control de riesgos
f) Implementación de las estrategias desarrolladas
g) Monitoreo de Riegos

Este conjunto de actividades se realizan de forma cíclica, cada determinado tiempo. La norma ISO 31000 toma los ítems anteriores, de la sección (b) a la sección (d) como el núcleo central de la gestión de riesgos, por ello estos ítems han sido tomados como objetos de estudio en este proyecto, además a los ítems seleccionados se anexará el ítem correspondiente a la sección (a), es necesario realizar la identificación y clasificación de activos para tratar los riesgos, debido a que los riesgos son inherentes a los activos que poseen las organizaciones.

Este proyecto coloca al alcance de las organizaciones principalmente locales, una descripción pertinente de cada una de las actividades seleccionadas como objeto de estudios, estas fueron recopiladas en una guía, en conjunto con un grupo de planillas que se diseñaron para estas actividades, para facilitar su ejecución, es decir, que el alcance de este proyecto contempló la descripción y documentación de las actividades de gestión de riesgos seleccionadas y la elaboración de planillas de apoyo.

Este proyecto se ejecutó en los seis meses correspondientes al segundo semestre del año 2015.

2.1. APORTE

Los aportes que esta guía ofrece, se limitan a brindar apoyo en la ejecución de las actividades o procesos correspondientes a la identificación y evaluación de riesgos, además las actividades mencionadas anteriormente como necesarias para la ejecución de estas últimas.

Específicamente los aportes que la guía ofrece son los siguientes:

- Descripción y documentación del proceso de identificación de activos tecnológicos, junto con su correspondiente planilla de apoyo.
- Descripción y documentación del proceso de clasificación de activos tecnológicos, junto con su correspondiente planilla de apoyo.
- Descripción y Documentación del proceso de identificación de riesgos de tecnologías de información, junto con su correspondiente planilla de apoyo.
- Descripción y Documentación del proceso de clasificación de riesgos de tecnologías de información, junto con su correspondiente planilla de apoyo.
- Descripción y Documentación del proceso de evaluación de riesgos de tecnologías de información, junto con su correspondiente planilla de apoyo.

Todo esto para colocar al servicio de las organizaciones del sector Industrial y productivo, locales y nacionales una estructurada y metodológica guía que les permita controlar sus riesgos tecnológicos de forma óptima.

2.2. LIMITACIONES

Este proyecto solo tomó como objeto de estudio algunas de las actividades correspondientes a la gestión de riesgos (las mencionadas anteriormente), las otras actividades restantes, especialmente la “Implementación de las estrategias desarrolladas”, no será tratada en este proyecto por el costo en términos de tiempo que esta demanda, debido a que es una actividad continua, que para ser verificada debe ser a puesta a prueba por un tiempo largo. Y la “creación de estrategias” depende en gran manera de los

criterios de interpretación de los resultados de la evaluación de riesgos que posean quienes lleven a cabo la gestión de riesgos.

De acuerdo con estas limitaciones se plantea como futura investigación la construcción de un sistema experto, usando reglas de inferencia, que a partir de los resultados obtenidos de la evaluación de riesgos proponga distintas estrategias para implementarlas en los procesos de gestión de riesgos en las organizaciones.

3. ESTADO DEL ARTE Y ANTECEDENTES HISTORICOS

En cada acción o actividad que desarrolla el ser humano, se puede encontrar de forma implícita el riesgo. La sociedad actual, inmersa en un mundo altamente soportado en tecnología y donde la información ha llegado a ser parte fundamental de muchas actividades, la dependencia hacia las TI ha aumentado notablemente y las ha convertido en un factor de riesgos para quien las use, especialmente para las empresas, a medida que estas han adoptado el uso de tecnologías de información en sus procesos de negocio, además de sus beneficios se han detectado fallos que suceden por circunstancias que de algún modo u otro vienen implícitas en el uso de estas tecnologías.

3.1. ANTECEDENTES HISTORICOS

Algunas empresas han tenido que experimentar situaciones amargas, que hicieron notoria la necesidad de ejecutar procesos de gestión de riesgos de TI, una de esas empresas que le toco afrontar este tipo de situaciones fue: Comair, quien en diciembre de 2004, sufrió un percance en su sistema de planeación de horarios (Westerman & Hunter, 2007). Este sistema de vital importancia en el modelo del negocio presentó fallos, interrumpiendo con esto todos los vuelos, causando una enorme pérdida económica, equivalente a las utilidades de un trimestre.

Otro caso significativo le tocó afrontarlo a “CardSystems Solutions Inc.”, procesadora de tarjetas de crédito, quien para el año 2005 informó que desconocidos entraron arbitrariamente a la información correspondiente a transacciones de cuarenta millones de usuarios portadores de tarjetas, después de este lamentable suceso MasterCard y Visa clientes de esta empresa, cancelaron sus convenio con esta, y posteriormente fue vendida. (Westerman & Hunter, 2007).

El ocho de Julio de 2015 a tempranas horas de la mañana, la aerolínea United Airlines tuvo que mantener en tierra durante un par de horas unos tres mil quinientos vuelos en todo el mundo, todo esto debido a un fallo en su sistema de información encargado de realizar las reservas, embarque y emisión de boletos, la empresa tuvo que comprometerse con todas los usuarios afectados a reacomodarlos en otras rutas alternas. Poco después la bolsa de Nueva York (NYSE), sufrió un error informático que forzó a detener las cotizaciones de esta importante dependencia de Wall Street por un periodo cercano a las

cuatro horas. En un comunicado el NYSE informó que el problema que experimentaron fue causado por problemas técnicos internos y no el resultado de un ciberataque, a raíz de esto, muchos agentes de bolsas decidieron redirigir sus compras a otros mercados que permanecieron activos.

Un caso particular, del sector bancario sucedió en Colombia, específicamente a la entidad Financiera Bancolombia, en el año 2011 mes de febrero se presentó una caída de la red del banco, lo que trajo como consecuencia un cese de actividades, caos y retraso con los clientes, esto por cerca de una hora ocasionó pérdidas, tanto financieras como de fiabilidad en sus servicios por parte de sus clientes (Gallo, 2011).

Cada una de estas organizaciones sufrieron por hacer una inapropiada gestión de los riesgos de TI, lastimosamente las consecuencias de estos hechos fueron más allá de afectar las TI, llegando a afectar también a departamentos operacionales y hasta el cumplimiento de la misión y objetivos corporativos, demostrando una vez más que el riesgo inherente a las TI, no es perjudicial únicamente al departamento de TI, sino que puede afectar a los demás departamentos de una organización.

A partir de allí se ha pensado en procesos que permitan anticiparse a los fallos que se presentaban, por esto han surgido mecanismos que intentan implementarlos, tales como marcos de trabajos, normas internacionales, metodologías estratégicas, entre otros.

3.2. SOLUCIONES PROPUESTAS

A nivel nacional e internacional se pueden mencionar varios intentos que se han realizado para controlar estos riesgos basándose en la normativa de su época de desarrollo. En Estados Unidos el año de 1992 fue publicado uno de los principales mecanismos de auditoria y tratamiento de riesgos, el marco COSO[2], aunque este inicialmente no concebía dentro de sus políticas un mecanismo de administración y evaluación de riesgos de TI, más adelante se incorporó un componente llamado “Información y Comunicación” que

[2] COSO, Committee of Sponsoring Organizations

junto con el componente de “Evaluación de riesgos” eran utilizados para el proceso de evaluación de riesgos (Fernández, 2003).

El Año 1996, en Estados Unidos, ISACA[3] publicó la primera edición del marco COBIT[4], este integraba los conceptos de TI con los Objetivos de la organización, aunque propiamente en esta edición no se hablaba de riesgos de TI, ya se mostraba la relevancia que existía entre ambos, luego en nuevas ediciones se han incorporado nuevos componentes con el fin de abarcar este campo, en diciembre de 2012 se lanzó una versión 5 que se enfocaba en modelos de negocio para la seguridad de la información, esto se consideró como un gran avance (ISACA, 2012).

Estos marcos de trabajo y otros tales como el Marco FAIR[5], han tratado de cubrir el proceso de evaluación de riesgos, estos se han involucrado en este tema, apoyados por normas como la ISO 27000, 27001, 27002, entre otras. Estas normas han sido fundamentales en este ámbito, ya que tratan aspectos como los riesgos de la información (Disterer, 2013), su aplicación ha sido correcta, y ha arrojado buenos resultados en el tratamiento de la información, pero ha dejado de lado un poco otros aspectos de la tecnología, tales como la infraestructura y otros activos de información, por lo que han existido algunas organizaciones que han optado por aplicar lo que existe en cuanto a riesgos de información y anexar otro proceso de evaluación de riesgos para intentar cubrir las falencias que dejan los marcos y metodologías existentes.

Algunas de las organizaciones que poseen mayor complejidad y cantidades de activos de información son las del sector económico tales como bancos, fiducias y las pertenecientes al sector educación, entre otras, por ello estas han pasado rápidamente a la acción en cuanto a gestión y evaluación de riesgos de TI.

La universidad Simón Bolívar es una institución pública de educación superior, ubicada en Caracas, Estado Miranda, Venezuela, como toda organización, no está exenta de riesgos. Por poseer grandes volúmenes de datos muchas veces es blanco de ataques, exteriores, por personal totalmente ajeno a la institución, e interiores por personal con

[3] ISACA, Information Systems Audit and Control Association
[4] COBIT, Control Objectives for Information and related Technology
[5] FAIR, Factor analysis of information risk

algún tipo de vínculo bien sea estudiante, docente o administrativo. Se tomó como activo principal, la información, se crearon políticas de riesgos que permitieran asegurar la información, y de paso benefició a la institución al darle mejor manejo a la información existente, finalmente la aplicación de políticas de riesgos mejoró significativamente los procesos internos de la universidad. Este estudio fue realizado a la luz de los controles de la ISO 17799:2007. Con este proyecto se logró "*promover el establecimiento, implantación, operación, monitoreo, mantenimiento y mejoramiento de ISO 27001:2007 en la Universidad Simón Bolívar*." (Freitas, 2009)sin embargo el uso de estas normas, limita la gestión de riesgos, debido a que se suele tomar como activo solo la información, descuidándose otros activos como la infraestructura física.

En estudios realizados específicamente sobre una organización del sector informático, se destacó la importancia de definir, correctas y pertinentes políticas que se relacionen estrechamente con los objetivos planteados por la organización, desarrollados en su estrategia empresarial, visión y misión. Los riesgos por estar relacionados con los objetivos ameritan un estudio exhaustivo que incluye el "*revisar, evaluar y actualizar el control efectivo de la administración de riesgos de TI*". Al finalizar este estudio se logró concluir lo siguiente "*La Administración de Riesgos de TI es importante ya que es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir*" (Maxitana & Naranjo, 2005).

El sector bancario, como se mencionó con anterioridad es también uno de los sectores más interesados en esta temática, debido a que el flujo de información que maneja es de vital importancia y la cantidad de procesos que están soportados en tecnologías de información.

En Colombia, la Universidad de los Andes desarrolló una guía de buenas prácticas de gestión de riesgos de TI en el sector bancario, para el buen desarrollo de esta, se tomó en cuenta cuatro bancos distintos, a pesar de pertenecer al mismo sector manejan distintos intereses organizacionales, Al inicio, se plantearon cuatro factores como eje central de la investigación que fueron: disponibilidad, acceso, agilidad y precisión, con esto se planteó un perfil de riesgos. Este proyecto se realizó con base en el código de práctica de gestión

de riesgos bs31100, que a su vez está basado en la norma ISO 31000. Al finalizar el desarrollo del mismo, una de las conclusiones a la cual se llegó fue que: "*los riesgos de TI siempre van a existir, ya sea que estos sean detectados o no por las organizaciones. No es posible eliminarlos totalmente, así que se debe buscar la mejor manera de gestionarlos. La gestión de riesgos de TI debe ser vista como un habilitador no como un inhibidor ya que ofrece protección contra la pérdida de valor y adicionalmente es un generador de valor al negocio."* (Figueroa et al., 2010).

La gestión de riesgos de TI ha sido un tema al que se le ha dado importancia, a este se le ha dedicado mucho estudio, y algunos han escrito sobre él, un concepto acertado acerca de este tema dice de la siguiente manera, *"La gestión de riesgos y controles en sistemas de información (GRCSI) es una actividad importante en los sistemas de gestión. No obstante, aunque en las organizaciones parece haber interés en su aplicación, la GRCSI aún no logra el impacto deseado, debido en gran parte a la falta de entendimiento de su sentido o propósito y a la ausencia de los procesos de cambio organizacional necesarios para su implantación. Este artículo presenta una revisión sobre los estándares de GRCSI más relevantes, con el fin de plantear una propuesta de integración de los roles y las actividades que las organizaciones deben desarrollar, y de analizar los niveles de riesgo y sus implicaciones frente a los sistemas de información"* (Guerrero & Gómez, 2010).

Se puede apreciar actualmente cuan ligados se encuentran la gestión de riesgos de TI con los objetivos de las organizaciones, hasta el punto de afirmarse que la gestión de riesgos es un factor clave para el cumplimiento de los objetivos en una organización (Quintero, 2011). Por ello se debe plantear un plan o modelos de administración de riesgos, que mediante un control de riesgos de acuerdo a los objetivos organizaciones, promueva el cumplimiento de dichos objetivos.

La mayoría de las investigaciones realizadas concernientes a este tema se centran en estudios y comparaciones entre normas y estándares, además muchas de estas investigaciones se han realizado tomando como marco de referencia normas antiguas.

3.3. ANALISIS DE CASOS DE ESTUDIOS, DE ESTANDARES Y NORMAS RELACIONADAS

3.3.1. CASOS DE ESTUDIOS SOBRE GESTIOS DE RIESGOS DE TECNOLOGIAS DE INFORMACIÓN

Nombre del Proyecto: Guía de Buenas Prácticas en Gestión de riesgos de TI en el sector Bancario Colombiano

Presentado por: Luis Carlos Figueroa Medina

Asesorado por: Olga Lucia Giraldo y Andrea Herrera

Universidad: Universidad de los Andes

Fecha: Mayo 2010

Objetivo General: "*Construir una guía de buenas prácticas de gestión de riesgos de TI en el sector bancario colombiano, visto desde los procesos de negocio y analizado desde los marcos de trabajo de gestión de riesgos BS 31100, y los marcos de gestión de riesgos de TI A4, y Risk IT del ITGI enmarcados dentro del cumplimiento de la reglamentación colombiana existente, específicamente la circular 052 de la SFC***"** (Figueroa et al., 2010).

Nombre del Proyecto: Implementación de un sistema de gestión de riesgo con base en correlación de logs de auditoría

Presentado por: Rony Mitshiu González Sánchez

Asesorado por: José Carrillo

Universidad: Universidad Católica de Colombia

Fecha: 2013

Objetivo General: "*Implementar el monitoreo de activos de información en la infraestructura del Banco Falabella, que permita el análisis de logs en los dispositivos que los generan a través de herramientas que permitan automatizar el proceso.***" (**Gonzales, 2013)

Nombre del Proyecto: Metodología de Implantación de un SGSI en un grupo empresarial jerárquico

Presentado por: Gustavo Pallas Mega

Universidad: Universidad de la Republica

Fecha: Diciembre 2009

Enfoque: "… *En el presente trabajo, abordamos la problemática que se plantea al momento de implantar, operar y mantener de forma evolutiva, un Sistema de Gestión de Seguridad de la Información (SGSI) para una empresa u organización perteneciente a*

*un grupo empresarial, en una relación de subordinación con otra empresa principal.***"** (Pallas, 2009)

Nombre del Proyecto: Gestión de riesgos corporativos de ti en Guatemala
Presentado por: Neftalí Esaú López Marcos
Asesorado por: Juan Carlos Morales Baten
Universidad: Universidad de San Carlos de Guatemala
Fecha: Octubre 2011
Objetivo General: "*Apoyar a los ingenieros que asumen responsabilidades de dirección en la gerencia de tecnologías de información y a los responsables de la gestión de riesgos del área de informática, por medio de un marco de trabajo, aplicable en el entorno guatemalteco.***"** (Lopez, 2011)

3.3.2. PUBLICACIONES

Nombre del Artículo: Metodología y gobierno de la gestión de riesgos de tecnologías de la información.
Autores: Ricardo Gómez, Diego Hernán Pérez, Yesid Donoso y Andrea Herrera.
Universidad: Universidad de los Andes
Base de Datos/Revista: Revista de Ingeniería
Fecha: 2010.

Nombre del Artículo: Gestión de riesgos en COBIT
Autores: Senén J. Pájaro Novoa
Entidad: Fundación Dintel
Base de Datos/Revista: Revista Dintel
Fecha: 2009.

Nombre del Artículo: Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT
Autores: Gonzalo Andrés Vanegas Devia y César Jesús Pardo, Ph.D.
Universidad: Universidad Icesi

Base de Datos/Revista: Redalyc
Fecha: 2014.

Nombre del Artículo: Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios
Autores: Alexandra Ramírez Castro y Zulima Ortiz Bayona
Universidad/Revista: Universidad Distrital Francisco José de Caldas.
Base de Datos: Dialnet
Fecha: 2011.

Nombre del Artículo: Riesgos de origen tecnológico: apuntes conceptuales para una definición, caracterización y reconocimiento de las perspectivas de estudio del riesgo tecnológico
Autor: Omar Javier Ramírez
Universidad: Universidad Nacional Abierta y a Distancia
Base de Datos/Revista: Scielo
Fecha: 29 de Julio del 2009

Nombre del Artículo: The Market's Perception of the Transactional Risks of Information Technology Outsourcing Announcements
Autores: Wonseok Oh, Michael J. Gallivan y Joung W. Ki
Base de Datos/Revista: ACM DL
Fecha: 2006

Nombre del Artículo: Accounting quality, information risk and implied volatility around earnings announcements
Autores: Seraina C. Anagnostopoulou y Andrianos E. Tsekrekos
Base de Datos/Revista: ScienceDirect
Fecha: Enero 2015

3.3.3. ANALISIS DE LA INFORMACIÓN EXISTENTE SOBRE GESTIÓN DE RIESGOS DE TI

En general es mucha la información que se encuentra sobre publicaciones y trabajos realizados sobre el marco del tema de gestión de riesgos de tecnologías de la información, pero existen varios factores que fueron fundamentales a la hora de ejecutar este proyecto, dichos factores son los siguientes:

- **Falta de Investigación y aplicación al sector productivo e industrial** Gran parte de la información existente sobre aplicación de modelos de gestión de riesgos de TI, está orientada hacia el sector bancario y educación, que generalmente son los sectores más interesados en este tipo de estudios y uno de los motivos principales de la ejecución de este proyecto tenía que ser la aplicabilidad al sector productivo e industrial.

- **Falta de uso de normas recientes tales como la ISO 31000** Una de las ideas fundamentales para la ejecución de este proyecto consistía en utilizar, normativa reciente y verificada, por ello se tomó la decisión que se trabajaría con la norma ISO 31000, y muy pocos son los trabajos realizados tomando como base esta norma internacional.

- **Falta de información que facilite la implementación de modelos de gestión de riesgos**

Con respecto a la información obtenida, se encontró que gran parte era casos de estudios puntuales, otra eran compendios de buenas prácticas que son muy útiles, pero que no facilitan la ejecución de un proceso de gestión de riesgos, ya que no explican con detalles las actividades y pasos a ejecutar que es el principal objetivo del desarrollo de esta guía.

4. MARCO TEÓRICO

4.1. MARCO CONCEPTUAL

ISO 31000: Es un nuevo estándar aceptado internacionalmente para la gestión del riesgo, junto con un nuevo vocabulario. Estos fueron desarrollados a través de un proceso de consenso por más de cuatro años, tiene como objetivo ayudar a las organizaciones de todo tipo y tamaño a gestionar los riesgos con efectividad.

La norma ISO 31000 contiene un compendio de términos y definiciones que serán utilizadas en este proyecto, además se utilizaran algunos de los términos contenidos en la norma ISO 27001, algunos de estos términos son:

Riesgos: "Efecto de la incertidumbre sobre los objetivos" (ISO, 2011)

Gestión de riesgos: "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo" (ISO, 2011)

Políticas para la gestión de riesgos: "Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo" (ISO, 2011)

Activos: "Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización". (ISO, 2005)

Amenazas: "Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización". (ISO, 2005)

Análisis de Riesgo: "Uso sistemático de la información para identificar fuentes y estimar el riesgo" (ISO, 2005)

Ataque: "Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información". (ISO, 2005)

Confidencialidad: "Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso". (ISO, 2005)

Disponibilidad: “Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados”. (ISO, 2005).

Evaluación de Riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo”.

Impacto: “Es el daño potencial sobre un sistema cuando una amenaza se presenta. Este daño puede ser expresado en términos cuantitativos o cualitativos”.

Metodología PHVA

La metodología PHVA es un ciclo dinámico, que puede ser utilizado dentro de los procesos de las organizaciones, es una herramienta sencilla que cuando se aplica adecuadamente puede ayudar mucho en la realización de actividades de forma eficiente y organizada. De forma breve la metodología se puede describir así:

1. **Planificar**: Establecer objetivos y procesos necesarios para lograr los resultados esperados por la organización

2. **Hacer**: Implementar los procesos o actividades necesarias para la consecución de los objetivos.

3. **Verificar**: Realizar seguimiento, comparar los resultados obtenidos actualmente con los objetivos planteados.

4. **Actuar**: Realizar acciones para mejorar el desempeño de los procesos o actividades ejecutadas.

4.2. ESTANDARES Y NORMAS RELACIONADAS CON LA GESTIÓN DE RIESGOS DE TI

ISO 27005

Esta norma proporciona directrices para la gestión de riesgos de seguridad de la Información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información (ISO/IEC, 2011a).

ISO 31000

Es una norma publicada por la Organización Internacional de Normalización [ISO] y la Comisión Electrotécnica Internacional [IEC] enfocada en la gestión de riesgos.

Su propósito es brindar información basada en pruebas y análisis para tomar decisiones sobre cómo seleccionar y determinar el tratamiento de los riesgos. El marco de gestión del riesgo de esta norma proporciona las políticas, los procedimientos y las disposiciones organizativas que integran la gestión de riesgos en toda la organización a todos los niveles. Como parte de este marco, la organización debe tener una política o estrategia para decidir cuándo y cómo los riesgos deben ser evaluados (ISO/IEC, 2011b).

ITIL v3

Fue desarrollada al reconocer que las organizaciones dependen cada vez más de la informática para alcanzar sus objetivos corporativos, lo que ha dado como resultado la creciente necesidad de servicios informáticos de calidad que correspondan a los objetivos del negocio y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar en el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones (Axwloa, 2011).

MAGERIT

Es un método formal para investigar los riesgos que soportan los sistemas de información. Es una norma establecida por el Gobierno español con el fin de brindar una metodología

de sistemas de información de riesgos en su análisis y gestión. El propósito de MAGERIT está relacionado con el uso de medios electrónicos, informáticos y tecnológicos, sujetos a ciertos riesgos que se deben minimizar con medidas de seguridad, para mitigar la desconfianza en el uso de estos medios. Su utilización está enfocada en las personas que utilizan los sistemas de información y sobre los riesgos y vulnerabilidades a que está expuesta la información (MHAP, 2012).

OCTAVE

Es una técnica efectiva de evaluación de riesgos desarrollada en el Centro de Coordinación CERT en Carnegie Mellon University. Octave es un conjunto de herramientas, técnicas y métodos para la evaluación del riesgo. Tiene en cuenta también la definición de los activos incluyendo: personas, hardware, software, información y sistemas. Hay tres componentes que conforman la base de su cuerpo de conocimiento: Octave, en su metodología original, definida para las grandes empresas, que describe conjuntos de criterios (i.e., principios, atributos y resultados); Octave-S, similar a la original, pero dirigido a empresas con garantía limitada; y Octave Allegro, un enfoque simplificado para la evaluación de la información de seguridad y garantía (CERT, 2008). Octave proporciona una línea base que se puede utilizar para enfocar la mitigación y mejorar de actividades; asimismo, equilibra los riesgos operativos, las prácticas de seguridad y la tecnología, lo cual permite tomar decisiones de protección de información con base en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados con la información crítica (CERT, 2008). Existen varios criterios de Octave que definen un conjunto de enfoques para la evaluación de los riesgos en una organización, en la seguridad de la información, utilizando un conjunto de principios, atributos y salidas (CERT, 2008).

RISK IT

Es un marco de trabajo a nivel mundial enfocado a las TI y publicado por ISACA. RISK IT proporciona una visión global sobre los riesgos empresariales asociados con todas las actividades relacionadas con TI. RISK IT pretende ser una herramienta práctica para la gestión de riesgos basada en los conceptos de valor y beneficios que la

organización obtiene a través de sus iniciativas de TI. Al igual que COBIT, RISK IT se concentra en el cumplimiento de los objetivos de la organización. Este modelo puede personalizarse para cualquier tipo de empresa en cualquier ubicación geográfica. RISK IT se define como una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados (ISACA, 2013).

MODELO	ORGANIZACIÓN	PUBLICACIÓN	ACTUALIZACIÓN	PAÍS	ESTRUCTURA
AS/NZS ISO 31000	ISO	2004	2009	Australia/Nueva Zelanda	11 Principios /5 procesos
COBIT	CCTA	2003	-	Reino Unido	5 principios/ 37 procesos
ISO/IEC ISO 27005	ISO	2008	-	Suiza	6 procesos
ITIL	ITIL	2001	2011	Suiza	5 principios
MAGERIT	Gobierno de España	2006	2012	España	Vol. 1, Método/ Vol. 2 , Catalogo/ Vol. 3,Guia
OCTAVE	SEI	2001	2007	Estados unidos	Octave: 3 fases/ Octave s: 3 fases/ Octave Allegro: 4 fases
RISK IT	ISACA	2009	2011	Estados unidos	3 Principios

Tabla 1 Tabla de comparación de modelos

5. METODOLOGÍA

5.1. TIPO DE INVESTIGACIÓN

Por sus características investigativas, el proyecto desarrollado se puede catalogar como una Investigación Aplicada, porque partió de conocimientos existentes para su aplicación, utilizando los resultados prácticos de los conocimientos, los cuales serán de utilidad para las organizaciones durante los procesos de identificación, clasificación y evaluación de riesgos de tecnologías de información.

Esta investigación comenzó con la descripción de la situación problema, luego se enmarcó en una teoría internacionalmente aceptada de la cual se expusieron los conceptos más importantes y pertinentes; finalmente, la situación descrita se evaluó a la luz de esta teoría y se propuso una secuencias de acción o actividades que se encuentran consagradas en la guía desarrollada como objetivo general de este proyecto.

5.2. TÉCNICAS DE RECOLECCION Y DE INFORMACIÓN

Se propuso como actividad metodológica el diseño y aplicación de instrumentos de recolección de información, debido a que se investigaría y definiría procesos correspondientes a evaluación de riesgos de tecnologías de información.

Pensando en la recolección de información se llevaron a cabo las siguientes actividades:

- ✓ *Recopilación Documental:* se logró recopilar una cantidad de información suficiente, relacionada con la temática tratada en este proyecto como es la gestión de riesgos de TI (ver capítulo 3 y 4. Estado del arte y Marco teórico respectivamente y Bibliografía), para luego construir con base a toda esta teoría internacionalmente aceptada una nueva guía que orientará el proceso de aplicación de modelos de gestión de riesgos de TI en las organizaciones del sector productivo e industrial.
- ✓ *Entrevistas:* Se llevaron a cabo de manera informal con el coordinador del departamento de tecnologías de la información de la empresa Corporación Plástica S.A.S – CORPLAS, para conocer su percepción sobre los riesgos que corren los activos que están bajo su responsabilidad y el contexto actual del departamento de TI (Ver Anexos No.1).

Con la información recolectada se prosiguió a su consolidación y análisis, siguiendo los procesos definidos para cada una de las fases de la gestión de riesgos que se abordaron

en la ejecución de este proyecto, a partir del análisis de la información recolectada y la obtenida mediante la ejecución de los procesos descritos se procedió a comparar y documentar los resultados obtenidos.

El análisis de la información se hizo utilizando las siguientes técnicas:

- ✓ Análisis Cuantitativo: se utilizaron principios de estadística para la realización de pronósticos a partir de incidentes presentados anteriormente y la frecuencia de ocurrencia de estos, con base en este análisis se construyeron las tablas de probabilidad e impacto para la gestión de riesgos (Ver Figura 4 y 5).
- ✓ Análisis Cualitativo y de Contenidos: se construyeron marcos comparativos para analizar las normas, modelos y estándares estudiados, además se diseñaron planillas y tablas de referencia, que buscaban ilustrar al usuario con respecto a la implementación de los procesos descritos, además, se diseñaron diagramas de flujo para mostrar el orden de las actividades entre los distintos procesos de gestión.

5.3. RESUMEN DE ACTIVIDADES GUIADAS POR LOS OBJETIVOS

Se recolectó información concerniente a la evaluación de riesgos de tecnología de información, posteriormente se realizó una búsqueda de artículos y trabajos desarrollados sobre normas y modelos y/o estándares aplicados a la evaluación de riesgos que sirvieran de apoyo para el desarrollo de este proyecto, luego se investigó exactamente sobre la norma ISO 31000, esta además de ser actual, permitió ligar la evaluación de riesgos a los objetivos organizacionales y la metodología PHVA que son las bases principales de esta guía.

Además se hicieron estudios concernientes a las normas, modelos y/o estándares seleccionados como apoyo para el desarrollo de este proyecto, luego se describieron cada una de las normas, modelos y/o estándares que se aplicaron, posterior a esto se construyeron cuadros comparativos entre estos para justificar su utilización en cada fase del desarrollo de este proyecto, luego se definió el proceso de identificación de activos informáticos, además se elaboraron unas planillas estructuradas que permitieran ilustrar y diligenciar este proceso. Finalizado esto se definió el proceso específico para clasificar los activos identificados y se elaboraron planillas estructuradas para ilustrar y diligenciar este proceso. Posteriormente se definió el proceso para la identificación de los riesgos existentes sobre los activos clasificados, a partir de esto se elaboraron planillas para

identificar los riesgos sobre la clasificación de activos planteada. Después se procedió a definir el proceso de clasificación de riesgos, luego se elaboró una planilla que facilitara este proceso. Seguido a esto se definió el proceso para ejecutar la evaluación de riesgos y se elaboraron unas planillas que facilitaran la comprensión y ejecución de este proceso. Todos los procesos que se definieron para dar cumplimiento a los objetivos fueron planteados con base en la norma ISO 31000, permitiendo así que los procesos para la evaluación de riesgos se pudieran ligar a los objetivos de las organizaciones, además, fueron estructurados de acuerdo a la metodología PHVA.

Después se describieron y documentaron los procesos anteriormente descritos para la identificación y clasificación de activos informáticos. Luego se describieron y documentaron los procesos desarrollados de identificación y clasificación de riesgos. Por último se describió y documentó el proceso de evaluación de riesgos planteado, todo esto para completar el desarrollo de la guía propuesta.

Finalmente como fase de validación de los procesos desarrollados, se puso en marcha, durante un mes, cada uno de estos de la siguiente forma: en las primeras dos semanas se aplicó el proceso de identificación y clasificación de activos, luego se efectuó el proceso de identificación y clasificación de riesgos en un periodo de dos semanas, y por último en dos semanas se ejecutó el proceso de evaluación de riesgos de TI, esto se llevó a cabo en la empresa local: Corporación Plástica S.A.S – CORPLAS.

6. DESARROLLO DEL PROYECTO

El desarrollo de este proyecto se llevó a cabo tal como se describe en la metodología, exactamente en la sección 5.3 "*Resumen de actividades guiadas por objetivos*", inicialmente se construyó un estado del arte (Ver Capitulo 3), que sirviera de base para el desarrollo de este proyecto.

6.1. NORMA Y MARCOS DE TRABAJO PARA EL DESARROLLO

La norma ISO 31000 ofrece principios y directrices genéricas sobre gestión de riesgos. La norma no es específica de ninguna industria o sector y puede ser utilizada por cualquier organización pública o privada, grande o pequeña, esto lo expresó de la siguiente manera Kevin W. Knight, quien estuvo a cargo del grupo de trabajo de ISO que desarrolló esta norma: "*Todas las organizaciones, no importa si son grandes o pequeñas, se enfrentan a factores internos y externos que le quitan certeza a la posibilidad de alcanzar sus objetivos. Este efecto de falta de certeza es* ***el riesgo*** *y es inherente a todas las actividades*". Además esta norma puede aplicarse a cualquier tipo de riesgo en una amplia serie de actividades y operaciones. ISO 31000 es la referencia mundial en sistemas de gestión de riesgos, y elegirla coloca a la vanguardia del mercado.

La norma ISO 31000 fue desarrollada para ayudar a las organizaciones a *(ISO, 2011)*:

- ✓ *Aumentar la probabilidad de lograr los objetivos*
- ✓ *Fomentar la gestión proactiva*
- ✓ *Ser conscientes de la necesidad de identificar y tratar el riesgo en toda la organización.*
- ✓ *Mejorar en la identificación de oportunidades y amenazas*
- ✓ *Mejorar la confianza de los grupos de interés*
- ✓ *Mejorar la información financiera*
- ✓ *Mejorar la eficiencia y eficacia operacional*
- ✓ *Minimizar las pérdidas*
- ✓ *Mejorar el aprendizaje organizacional*
- ✓ *Establecer una base confiable para la toma de decisiones y la planificación*
- ✓ *Mejorar la gobernabilidad*
- ✓ *Entre otras.*

Esta norma trabaja con base en tres aspectos fundamentales denominados de la siguiente forma: **los principios para la gestión de riesgos**, **el marco de referencia** y **los procesos**

de gestión de riesgos. La relación existente entre estos tres aspectos puede ser resumido mediante la siguiente figura:

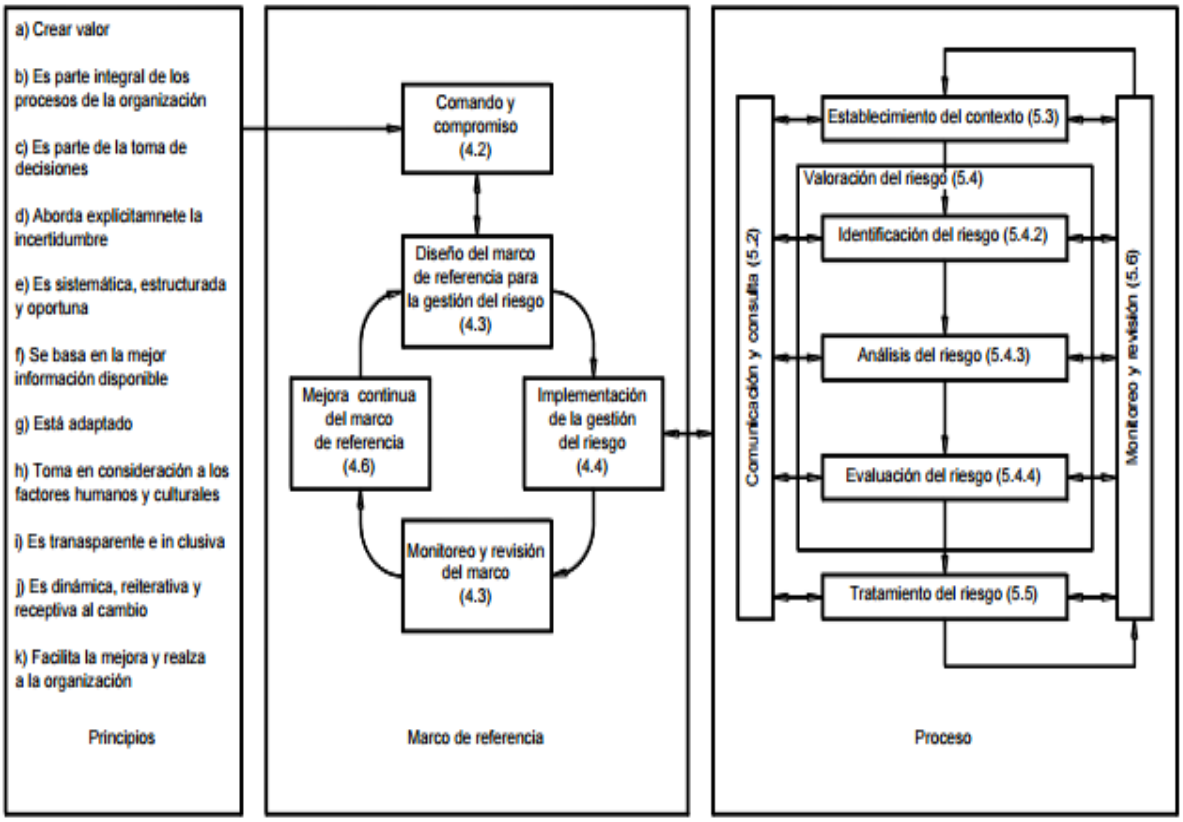


Figura 1. Relación entre los principios, marco de referencia y procesos de gestión de riesgos (Tomado de documentación oficial de la norma ISO 31000 ICONTEX)

6.1.1. PRINCIPIOS PARA LA GESTIÓN DE RIESGOS

La norma ISO 31000 afirma que para obtener un mejor rendimiento se hace necesario que la gestión de riesgos en una organización se lleve a cabo bajo los principios:

a. Crear valor.

b. Estar integrada a todos los procesos de la organización.

c. Forma parte de la toma de decisiones.

d. Tratar explícitamente la incertidumbre.

e. Ser sistemática, estructurada y oportuna.

f. Estar basada en la información disponible más pertinente.

g. Estar hecha a la medida.

h. Ser transparente e inclusiva

i. Ser dinámica, iterativa y sensible al cambio

j. Facilitar la mejora continua de la organización.

6.1.2. MARCO DE TRABAJO

Un elemento fundamental en la aplicación de la norma ISO 31000 es el marco de trabajo o marco de referencia, el cual es el encargado de integrar los proceso de gestión de riesgos. La norma recomienda utilizar un marco de trabajo basado en la mejora continua y de ese modo ayude en la tarea de integración de los procesos de gestión. El marco de trabajo que por defecto suministra la norma es el correspondiente a la metodología PHVA (como se puede apreciar en la Figura 2.); Este marco de trabajo también fue asumido en el desarrollo del presente proyecto.

El ciclo o metodología PHVA cuenta con cuatro fases (Ver Marco Teórico), son las siguientes:

I. Planear: el marco de trabajo diseñado debe contar con los siguientes aspectos
   a. Comprender el contexto de la organización, tanto interno como externo.
   b. Política de gestión de riesgos
   c. Integración con los procesos de la organización
   d. Rendición de cuentas
   e. Recursos

II. Hacer: en la implementación del marco de trabajo se debe tener en cuenta:
   a. Implementación del marco de trabajo para la gestión de riesgos
   b. Implementación del proceso de gestión de riesgos

III. Verificar: en la fase de verificación se debe tener en cuenta:
   a. Monitoreo y revisión de la efectividad del marco de trabajo.
   b. Establecimiento de las medidas de desempeño.
   c. Revisión periódica de los avances y desviaciones.
   d. Informes y revisión de la efectividad del marco de trabajo.

IV. Actuar: esta fase hace referencia a la mejora continua del marco de trabajo para la gestión de riesgos.

A continuación se describen los procesos de gestión correspondientes a las fases del marco de trabajo, para el caso de este proyecto, ya se mencionó previamente que el marco usado es PHVA

6.1.3. Procesos correspondientes a la gestión de riegos acorde a la norma ISO 31000

El tercer aspecto de la gestión de riesgos, direccionada por la norma ISO 31000 es el proceso de "gestión de riesgos", en esta fase se desarrollan tres etapas importantes (ver figura 3), estas son:

- ✓ **Establecimiento del contexto**
- ✓ **Evaluación de riesgos**
- ✓ Tratamiento de riesgos

Previo al desarrollo de este proyecto, se estableció en el alcance que se trabajaría sobre las primeras dos etapas (ver Alcance).

Establecimiento del contexto

El establecimiento del contexto en el que trabaja la organización es de vital importancia, porque se trata de definir la forma como la organización busca alcanzar sus objetivos, también incluye la tarea de establecer los procesos para gestionar los riesgos y la definición de los criterios de evaluación para dichos riesgos. (Ornella, 2014).

Evaluación de riesgos

Esta fase puede ser considerada como principal durante todo el proceso de gestión de riesgos (ver fig. 2), a la vez está constituida por otros subprocesos, como se muestra en la siguiente figura:

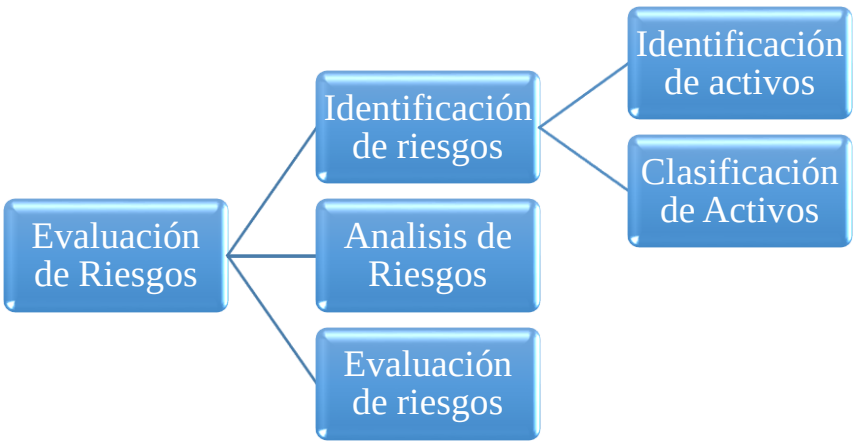


Figura 2. Evaluación de riesgos

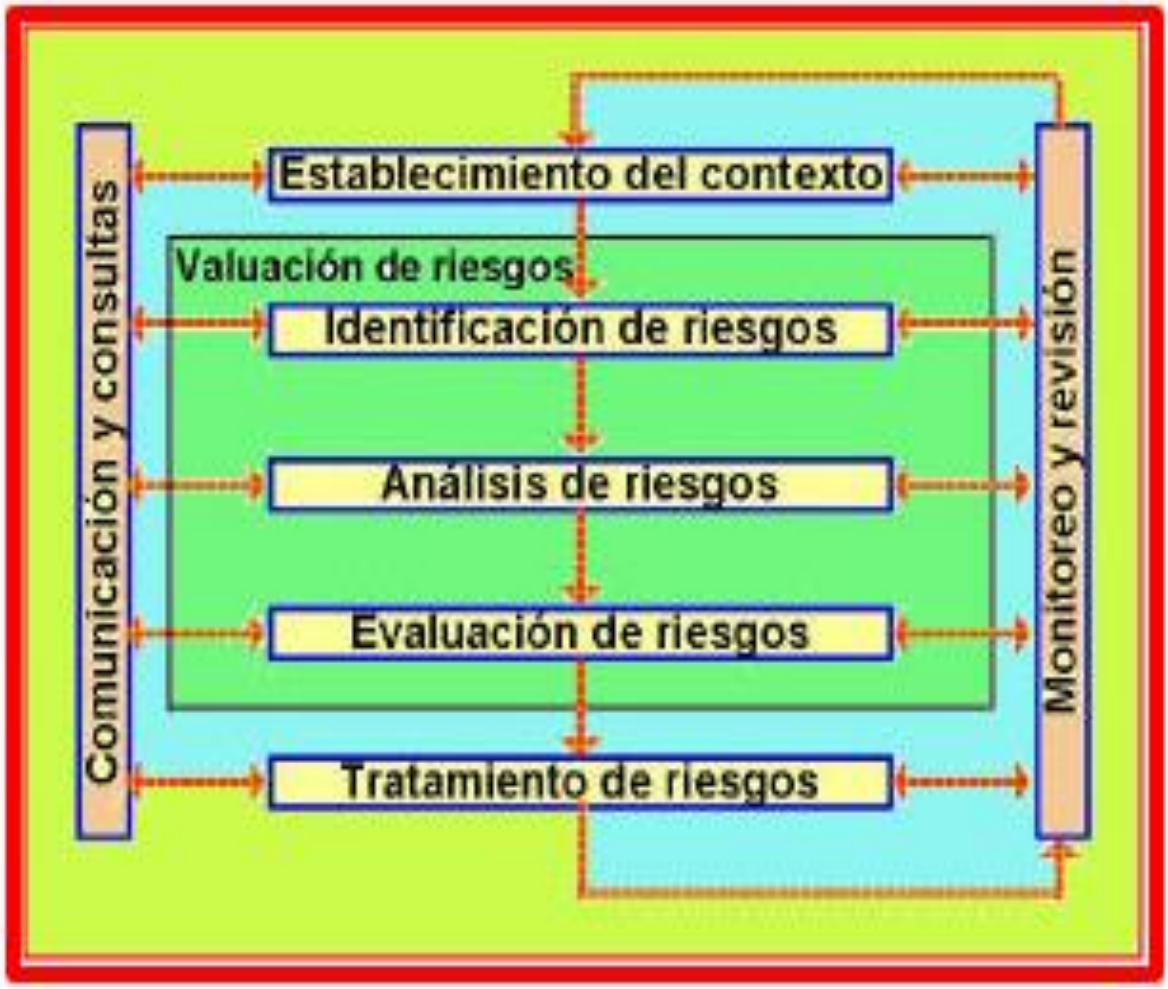


Figura 3. Procesos de gestión de riesgos (Ornella, 2014).

En este importante aspecto de la gestión de riesgos se usará también los conceptos contenidos en la norma ISO 27005, puesto que la ISO 31000 permite gestionar los riesgos de forma general e independiente del tipo de organización y de riesgos, mientras que la ISO 27005 ofrece pautas concretas para la gestión de riesgos de la información, útiles cuando se trate el activo "Información" en la aplicación de la guía desarrollada en este proyecto.

A continuación la siguiente tabla refleja el grado de compatibilidad en los procesos de gestión de las normas ISO 31000 e ISO 27005.

Procesos de gestión ISO/IEC 27005		Procesos de gestión ISO/IEC 31000			
		Establecimiento el contexto	**Identificación de Riesgos**	**Análisis de riegos**	**Evaluación de riegos**
	Establecimiento el contexto	**TOTAL**			
	Identificación de Riesgos		**TOTAL**		
	Análisis de riegos			**MEDIO**	
	Evaluación de riegos				**TOTAL**

Tabla 2 Relación de procesos de gestión entre las normas ISO 31000 e ISO 27005. Vanegas, G. & Pardo. C. (2014).

6.2. DEFINICIÓN Y DESCRIPCION DE LOS PROCESOS DEL MODELO DE GESTIÓN DE RIESGOS

A continuación se encuentra la definición y descripción de los procesos del modelo de gestión de riesgos, contemplados en la Guía desarrollada en este proyecto. Para iniciar con la descripción de los procesos del modelo de gestión de riesgos, se identificaron un conjunto de actividades y procesos necesarios para la correcta evaluación de riesgos de tecnologías de la información y que abarcaban todo este proceso, en vista de esto se planteó una cadena de valor, en la que se identificaron: macroproceso, procesos y procesos de gestión, donde se evidencia la aplicación de la norma ISO 31000 y la metodología PHVA.

✓ **MACROPROCESO**: Es la tarea principal, que se busca implementar, con la ejecución del contenido de la guía metodológica.

❖ Gestión de Riesgos de Tecnologías de Información.

✓ **PROCESOS:** Son los proceso que evidencian la implementación de la metodología PHVA, en la que cada proceso representa una fase del ciclo de esta metodología.

❖ Diseño de marco de referencia para la gestión de riesgos
❖ Implementación del Marco de referencia
❖ Monitorización y revisión del Marco de referencia
❖ Mejora continua del marco de referencia.

✓ **PROCESOS DE GESTIÓN:** Son los proceso que reúnen en su contenido, todas las actividades a ejecutarse a lo largo de la implementación de la guía de evaluación de riesgos.

❖ Establecimiento de mecanismos de comunicación y consulta,
❖ Establecimiento del contexto
❖ Identificación de riesgos
❖ Análisis de riesgos

- Evaluación de riesgos
- Tratamiento de los riesgos
- Medición periódica del progreso del plan de gestión de riesgos
- Estudio sobre mejoras del marco de referencia
- Aplicación de mejoras al marco de referencia

Además se realizó una representación gráfica de la cadena de valor diseñada para el desarrollo e implementación de la guía de trabajo. (Ver Tabla 3)

MACROPROCESO	PROCESOS	PROCESOS DE GESTIÓN
GESTION DE RIESGOS DE TECNOLOGÍAS DE INFORMACION	Diseño de marco de referencia para la gestión de riesgos	Establecimiento de mecanismos de comunicación y consulta
		Establecimiento del contexto
	Implementación del Marco de referencia	Identificación de riesgos
		Análisis de riesgos
		Evaluación de riesgos
	*Monitorización y revisión del Marco de referencia	**Tratamiento de los riesgos
		**Análisis del plan de gestión de riesgos
	*Mejora continua del marco de referencia	**Análisis de mejoras del marco de referencia
		**Aplicación de mejoras al marco de referencia

Tabla 3. Cadena de Valor

(*) Estos procesos no serán tratados a fondo, tal como se planteó en el alcance, al inicio de este proyecto.

(**) Estos procesos de gestión no serán tratados a fondo, tal como se planteó en el alcance, al inicio de este proyecto.

6.2.1. PLANEAR: "*DISEÑO DE MARCO DE REFERENCIA PARA LA GESTION DE RIESGOS"*

El objetivo de este proceso es establecer los lineamientos básicos para una óptima implementación del marco de referencia, teniendo en cuenta el contexto organizacional y garantizando la comunicación, a través de mecanismos apropiados para ello.

El proceso diseño de marco de referencia para la gestión de riesgos busca evaluar y entender el contexto, tanto externo como interno de la organización, ya que este puede influir directamente sobre el diseño de dicho marco, además es en este proceso que se especifica el orden del flujo de la información y recursos entre el equipo encargado de la ejecución del macroproceso, además establece los tiempos apropiados para ello.

Para este proceso se identificaron los siguientes actores:

- ✓ Director o Encargado de Tecnologías de la información
- ✓ Representante o encargado de departamento
- ✓ Gerencia o Dirección general de la organización

A petición del usuario final se incluyó entre la descripción que guía la ejecución de este proceso tablas de ENTRADA-SALIDA, para facilitar la comprensión de esta información. Para este proceso se prepararon las siguientes tablas

Cliente: Director o Encargado de tecnologías de la información	
ENTRADA	**SALIDA**
Información concerniente a los departamentos de la organización	Documento Justificación de aplicación de Gestión de riesgos de TI
Lista de Actividades a realizar + Planilla de Asignación de personal	Planilla de Actas de Reunión
Planilla de contexto Interno + Mapa de procesos	Lista de procesos organizacionales documentados

Tabla 4. E/S del encargado de tecnologías de la información en el proceso No. 1

Cliente: Representante o encargado de departamento	
ENTRADAS	**SALIDAS**
Lista de Departamentos + Lista de Empleados por departamentos	Planilla de Asignación de personal
Planillas de Asignación de Personal + Lista de Departamentos + Lista de procesos por departamentos	Planilla de Contexto Interno
Lista de Departamentos + Planilla de Asignación de personal	Encuestas de Mecanismos de Comunicación
Cronograma de Reuniones + Plan de Comunicación + Planilla de Asignación de personal	Formatos de Compromisos para la disposición de recursos (Tiempo, Espacio, económicos, personal, ETC)

Tabla 5. E/S del encargado del departamento en el proceso No. 1

Cliente: Gerencia o Dirección general de la organización	
ENTRADAS	**SALIDAS**
Lista de Departamentos + Lista de empleados	Planilla de Asignación de Personal
Lista de Actividades a realizar para la gestión de riesgos	Cronograma de Reuniones
Cronograma de reuniones + Planilla de Asignación de personal	Plan de Comunicación

Tabla 6- E/S de la gerencia en el proceso No. 1

Bajo este proceso se ejecutaran dos procesos de gestión que son los siguientes:

- ✓ Establecimiento de mecanismos de comunicación y consulta.
- ✓ Establecimiento del contexto.

6.2.1.1. ESTABLECIMIENTO DE MECANISMOS DE COMUNICACIÓN Y CONSULTA.

El objetivo de este proceso de gestión es establecer los mecanismos de comunicación y consulta que usará la organización para la ejecución del modelo de evaluación de riesgos.

Con respecto a este proceso la norma ISO 31000 sugiere que este debe garantizar que:

- ✓ *"los componentes claves del marco para la gestión de riesgo y todas las modificaciones posteriores se comunican de manera correcta"*
- ✓ *"existe un reporte interno adecuado acerca del marco, su eficacia y resultados"*
- ✓ *"La información pertinente derivada de la aplicación de la gestión del riesgo está disponible en los niveles y los momentos convenientes "*
- ✓ *"existen proceso para la consulta con las partes involucradas internas"*
- ✓ *"se use la comunicación para generar confianza en la organización"*
- ✓ *"Se brinde retroalimentación e informes sobre la comunicación y las consultas"*

- ✓ *"exista comunicación con las partes involucradas en el evento de una crisis o contingencia"(ISO, 2011)*

Para la puesta en marcha de este proceso de gestión el director o encargado del área de Tecnologías de la información con base en información suministrada por los distintos departamentos, concerniente a los principales obstáculos para la consecución de sus objetivos, debe estudiar y justificar ante la organización la importancia de la implementación de un modelo de evaluación de riesgos de TI, luego debe solicitar al ente encargado en la organización de actualizar el mapa de procesos o de procedimientos de la organización que se incluya como actividad a ejecutar la implementación de modelos evaluación de riesgos de TI, ya que una de las ideas principales de la norma ISO 31000 consiste en incluir dentro de las políticas estratégicas y organizacionales el modelo de gestión de riesgos.

Posteriormente el director o encargado de Tecnologías de la información debe solicitar a la organización que se le proporcione recursos, tales como personal, tiempo y espacio para la implementación del modelo de evaluación de riesgos, seguido a esto la organización debe comprometerse a asignar los recursos necesarios para la realización del proceso, esto puede hacerse si es necesario por medio de actas de compromisos, luego informar al director o encargado de tecnologías de información la asignación de recursos requeridos para dicha ejecución, finalmente El director o encargado de Tecnologías de información junto al personal asignado para ejecutar esta guía desarrollará un cronograma de actividades para asignarle tiempo a cada una de las actividades a realizar y a los medios establecidos para rendición de cuentas.

6.2.1.2. ESTABLECIMIENTO DEL CONTEXTO

El objetivo de este proceso de gestión es realizar un estudio del contexto interno y externo de la organización que permita el reconocimiento de sus procesos y analizar como las tecnologías de información son de apoyo para dichos procesos, todo esto a partir del diligenciamiento de planillas por departamento de la organización y socialización de la relación entre los procesos y las tecnologías de Información

La norma ISO 31000 en su documentación correspondiente indica que el establecimiento del contexto puedo incluir entre otros:

- ✓ *"El ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo bien sea internacional, nacional, regional o local"*
- ✓ *"Gobierno, estructura de la organización, funciones y responsabilidades"*
- ✓ *"Políticas, objetivos y las estrategias implementadas para lograrlo"*
- ✓ *"Capacidades, entendidas en términos de recursos y conocimientos (por ejemplo capital, tiempo, personas, procesos sistemas y tecnologías)"*
- ✓ *"La cultura organizacional"*
- ✓ *"Normas, directrices y modelos adoptados por la organización*
- ✓ *"Sistemas de información, flujos de información y proceso de toma de decisiones (tanto formales como informales)"*
- ✓ *"Las relaciones con las partes involucradas interna y sus percepciones y valores"*
- ✓ *"Forma y extensión de las relaciones contractuales"(ISO,2011)*

Para la ejecución de este proceso cada departamento, con su respectiva representación asignada, debe hacer un estudio de los procesos organizacionales internos y externos correspondientes a su departamento, identificando cuáles están relacionados con tecnologías de información para su desarrollo; luego de haberlos identificado se debe proceder a especificar de qué forma se emplean las tecnologías de la información en el desarrollo de los mismos y finalmente en una reunión presidida por el director o encargado del departamento de Tecnologías de Información y conformada por cada uno de los representantes de los distintos departamentos se deben analizar los procesos identificados y descritos por cada representación y a juicio de quien preside la reunión se seleccionaran los procesos que manifiesten mayor dependencia de las tecnologías de la información y con base en estos se trabajará en la siguiente fase de implementación de este modelo de gestión de riesgos.

6.2.2. HACER: *"IMPLEMENTAR EL MARCO DE REFERENCIA"*

El objetivo de este proceso es valorar el nivel de riesgo en que se encuentra la organización con respecto a la relación entre los procesos organizacionales y los activos tecnológicos.

El proceso implementación de marco de referencia para la gestión de riesgos busca identificar los riesgos a los que están expuestos los activos tecnológicos usados para la ejecución de procesos de vital importancia para la organización, además en este proceso debe especificarse la forma de analizar y clasificar los riesgos según su nivel de relevancia, impacto, probabilidad de ocurrencia. Finalmente debe establecerse mecanismos para evaluar los riesgos, ponderándolos, y estableciéndoles una zona de riesgo según los criterios de clasificación usados en la etapa de análisis.

Para este proceso se identificaron los siguientes actores:

- ✓ Director o Encargado de Tecnologías de la información
- ✓ Representante o encargado de departamento

A petición del usuario final se incluyó entre la descripción que guía la ejecución de este proceso tablas de ENTRADA-SALIDA, para facilitar la comprensión de esta información, para este proceso se prepararon las siguientes tablas

Cliente: Director o Encargado de tecnologías de la información	
ENTRADA	**SALIDA**
Lista de procesos críticos	Planilla Procesos/Activos
Planilla Procesos-Activos	Inventario de Activos (Historial)
Planilla Procesos-Activos + Lista de procesos críticos	Planilla Riesgo/Causa

Tabla 7. E/S del encargado de TI en el proceso No. 2

Cliente: Representante o encargado del departamento	
ENTRADA	**SALIDA**
Tabla de Impacto + Planilla Riesgo/Causa + Planilla Procesos/Activos	Planilla de Impacto
Tabla de probabilidad + Planillas Riesgo/Causa + Planilla Procesos/Activos	Planilla de Probabilidad
Planilla de Impacto + Planilla de probabilidad	Planilla de Análisis de Riesgo
Planilla de Análisis de Riesgo + Tabla de Categorías	Planilla de Categorización
Planilla de Categorización + Planilla de Análisis de Riesgo	Planilla de Severidad de riesgo

Tabla 8. E/S del encargado del departamento en el proceso No. 2

Bajo este proceso se ejecutarán los siguientes tres procesos de gestión:

- ✓ Identificación de riesgos
- ✓ Análisis de riesgos
- ✓ Evaluación de riesgos

6.2.2.1. IDENTIFICACIÓN DE RIESGOS

El objetivo de este proceso de gestión es determinar con base en los procesos y activos, las fuentes de riesgos, áreas de impacto, eventos, causas y consecuencias potenciales que puedan afectar la organización.

Este proceso de gestión fue descrito tomando como fundamento los siguientes conceptos que ofrece la norma ISO 31000:

"*La organización debería identificar las fuentes de riesgos, las áreas de impacto, los eventos (incluyendo los cambios en las circunstancias) y sus causas y consecuencias potenciales. El objeto de esta fase es general una lista exhaustiva de riesgos con base en aquellos eventos."* (ISO, 2011)

"La organización debería aplicar herramientas y técnicas para la identificación de riesgos que sean adecuadas a sus objetivos y capacidades, y a los riesgos que se enfrentan. La información pertinente y actualizada es importante para identificar los riesgos. Esta información debería incluir, siempre que sea posible, la información básica. En la identificación del riesgo se deberían involucrar las personas con el conocimiento apropiado." (ISO, 2011)

Para la ejecución de este proceso de gestión cada equipo de trabajo, escogido para representar cada departamento debe seleccionar dentro del conjunto de procesos bajo su responsabilidad un grupo de procesos críticos o principales para ser tratados y estudiados, esta actividad debe ser guiada por el encargado de tecnologías de la información para este proceso, luego los equipos de trabajo de los distintos departamentos, analizaran todos los procesos seleccionados previamente para proceder con la identificación de todos los activos de tecnologías de la información que están relacionados e involucrados en la ejecución de dichos procesos, seguido a esto el encargado de tecnologías de información tomará de cada uno de los representantes de los diferentes departamentos la información concerniente a los activos implicados en el ejercicio de sus respectivas funciones, y serán compilados para mantener un historial de ellos y posteriormente ser utilizado en nuevas aplicaciones de este macroproceso, finalmente los representantes de cada uno de los departamentos tomaran cada uno de los procesos que seleccionaron anteriormente, luego tomando como base los activos tecnológicos relacionados con dichos procesos procederán a identificar los riesgos a los que se encuentran expuestos los activos, que de algún modo podrían afectar los procesos, para esta actividad es vital identificar no solo los riesgos, sino también las causas y consecuencias potenciales.

6.2.2.2. ANALISIS DE RIESGO

El principal objetivo de este proceso de gestión es establecer la probabilidad de ocurrencia de los riesgos y su impacto en la organización, a partir de esto clasificarlos y estimar el nivel de ellos.

Este proceso de gestión fue descrito tomando como fundamento los conceptos que ofrece la norma ISO 31000, tales como los siguientes:

"El análisis del riesgo involucra la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas, y la probabilidad de que tales consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y la probabilidad. El riesgo es analizado determinando las consecuencias y su probabilidad, y otros atributos del riesgo. Un evento puede tener consecuencias múltiples y puede afectar a objetivos múltiples. También se deberían considerar los controles existentes y su eficacia y eficiencia" (ISO, 2011)

"El análisis del riesgos se puede realizar con diversos grados de detalles, dependiendo del riesgo, el propósito del análisis y la información, datos y recursos disponibles. El análisis puede ser cualitativo, semicuantitativo o cuantitativo o una combinación de ellos, dependiendo de las circunstancias" (ISO, 2011)

Para la ejecución de este proceso de gestión cada representación de los diferentes departamentos debe tomar cada uno de los riesgos identificados previamente para cada proceso y a partir de una tabla de probabilidad (Ver Figura 4) podrán determinar la probabilidad de ocurrencia de dichos riesgos, esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos si no se materializado, además deberán tomar cada uno de los riesgos identificados previamente para cada proceso y a partir de una tabla de impacto (ver Figura 5) determinar el impacto sobre la organización en caso de ocurrencia de dichos riesgos, luego el encargado de tecnología de información debe presidir una reunión en la que se analicen los riesgos de cada proceso de los diferente departamentos, esta preferiblemente debe hacerse por independiente con cada departamento. La clasificación debe hacerse siguiendo como norma una matriz de zona de riesgo.

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en cualquier momento	Al menos una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Figura 4. Imagen de Tabla de probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Figura 5. Imagen de la tabla de impacto

6.2.2.3. EVALUACION DE RIESGO

El principal objetivo de este proceso de gestión es facilitar la toma de decisiones, con base en la severidad de los riesgos y de esta forma considerar su respectivo tratamiento.

Este proceso de gestión fue descrito tomando como fundamento los siguientes conceptos que ofrece la norma ISO 31000:

"*La evaluación del riesgo implica la comparación del nivel de riesgo observado durante el proceso de análisis y los criterios del riesgos establecidos al considerar el contexto. Con base en esta comparación, se puede considerar la necesidad del tratamiento."* (ISO, 2011)

"En algunas circunstancias, la evaluación del riesgo puede llevar a la decisión de emprender un análisis adicional. La evaluación del riesgo también puede tener como resultados la decisión de no tratar el riesgo de ninguna manera diferente del mantenimiento de los controles existentes. Esta decisión estará influida por la actitud de la organización hacia el riesgo y por los criterios del riesgo que se han establecidos" (ISO, 2011)

Para la ejecución de este proceso de gestión cada representación de cada departamento tomara todos los riesgos que se identificaron y analizaron y los enumerará para facilitar su evaluación y tratamiento, luego cada representación de los departamentos asignara a cada riesgo indexado con anterioridad una categoría, para ello debe hacerse uso de una planilla específica y estándar, para ello debe guiarse de una tabla de categorización (ver Figura 6) que debe ser diseñada de acuerdo al contexto de la organización, seguidamente el encargado de tecnologías de información debe tomar de cada uno de los departamentos las planillas de categorización, de probabilidad de ocurrencia y de impacto generado completamente diligenciadas y con base en estas calculará la severidad de los riesgos absolutos a los que está expuesta la organización.

Categoría	Descripción
Gestión	Riesgos relacionados con la ausencia o aplicación incorrecta de métodos de gestión de las tecnologías de información y comunicaciones.
Operación	Incumplimiento de directrices, procedimientos y metodologías y estándares en los procesos operativos.
Infraestructura	Riesgos relacionados con las fallas potenciales de la infraestructura tecnológica utilizada.
Seguridad	Eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información.
Recursos Humanos	Relacionados con el desempeño y regularidad de los recursos humanos.

Figura 6. Imagen de Tabla de categorización

6.2.3. VERIFICAR: “MONITORIZACIÒN Y REVISIÒN DEL MARCO DE REFERENCIA”

El objetivo principal de este proceso es garantizar que la gestión del riesgo sea eficaz y continua, a través del tratamiento de los riesgos y la medición del desempeño del marco de referencia durante la implementación del mismo.

El proceso Monitorización y revisión del Marco de referencia busca medir el desempeño de la gestión del riesgo frente a los indicadores, los cuales se revisan para determinar su idoneidad, además se busca aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo, durante la ejecución se revisa si el marco de referencia, la política y el plan para la gestión de riesgos sigue siendo adecuado para el contexto organizacional, y se establece los tiempos apropiados para el flujo de información y recursos.

Para este proceso se identificaron los siguientes actores:

- ✓ Director o Encargado de Tecnologías de la información
- ✓ Representante o encargado de departamento

A petición del usuario final se incluyó entre la descripción que guía la ejecución de este proceso tablas de ENTRADA-SALIDA, para facilitar la comprensión de esta información, para este proceso se prepararon las siguientes tablas

Cliente: Director o Encargado de tecnologías de la información	
ENTRADAS	**SALIDAS**
Planilla de caracterización	Planilla de establecimiento de controles
Constancia de Aplicación de controles + Planilla de severidad de riesgos absolutos	Planilla de severidad de riesgos controlados
Planilla de severidad de riesgos absolutos + Planilla de severidad de riesgos controlados	Planilla de verificación de mejora

Tabla 9. E/S del encargado de TI en el proceso No. 3

Cliente: Representante o encargado del departamento	
ENTRADAS	**SALIDAS**
Planilla de Aplicación de controles	Constancia de Aplicación de Controles
Planilla de Sugerencias	Formato de Sugerencia (Planilla de Sugerencias diligenciada)

Tabla 10. E/S del encargado del departamento en el proceso No. 3

Bajo este proceso se ejecutaran los siguientes procesos de gestión:

- ✓ Tratamiento de riesgos
- ✓ Análisis de mejoras del marco de referencia

6.2.3.1. TRATAMIENTO DE RIESGOS

El objetivo de este proceso de gestión es diseñar controles que una vez implementados permitan modificar los riesgos y sus efectos sobre la organización.

Según la norma ISO 3100, el tratamiento del riesgo debe incluirse en un proceso cíclico de:

- ✓ *"Valoración del tratamiento de riesgo"*
- ✓ *"Decisión sobre si los niveles de riesgo residual son tolerables"*
- ✓ *"Si no son tolerables, generación de un nuevo tratamiento para el riego"*

Además "l*as opciones del tratamiento de riesgo no necesariamente son mutuamente excluyente ni adecuada en todas las circunstancias. Las opciones pueden ser algunas de estas:"*

- ✓ *"Evitar el riesgo al decidir no inicia o continua la actividad que lo origino"*
- ✓ *"Tomar o incrementar el riesgo para perseguir la oportunidad"*
- ✓ *"Retirar la fuente de riesgo"*
- ✓ *"Cambiar la probabilidad"*
- ✓ *"Cambiar las consecuencias"*
- ✓ *"Retirar el riesgo mediante una decisión informada"*

Para la ejecución de este proceso de gestión el encargado de tecnologías de la información en compañía de los representantes de cada departamento debe sugerir un conjunto de controles para aminorar el efecto de los riesgos sobre la organización o cualquier otra opción que el equipo de trabajo seleccione para determinado riesgo, luego la representación de cada departamento guiará esta puesta en marcha en sus respectivos departamentos, inicialmente se debe hacer entrega de los controles al personal de la organización encargado de ejecutar el proceso al cual pertenece el riesgo y estos aplicaran los controles, después de esto el encargado de tecnologías de la información junto con la representación de los departamentos harán un nuevo proceso de análisis y evaluación de riesgos, pero únicamente de aquellos riesgos a los que se le aplicaron los controles, para verificar los resultados son de acuerdo a los esperado, para esto el encargado de tecnologías de la información debe comparar los riesgos absolutos con los riesgos controlados.

6.2.3.2. ANÁLISIS DEL PLAN DE GESTIÓN DE RIESGOS

El objetivo de este proceso de gestión es permitir la valoración del marco de referencia utilizado a todos los miembros de la organización.

Para la ejecución de este proceso de gestión es recomendable implementa un modelo PQRS (Peticiones, Quejas, Reclamos y Sugerencia) de la siguiente forma:

Cualquier personal de la organización que se relacione con algún proceso tratado en la aplicación del modelo de riesgo podrá diligenciar un formato PQRS para su posterior revisión, este formato será estudiado primero por la representación del departamento al que está vinculado quien realiza la petición, queja, reclamo o sugerencia.

Luego el formato deberá ser entregado al encargado de Tecnologías de la información para entrar en una fase de análisis y revisión

6.2.4. ACTUAR: “MEJORA CONTINUA DEL MARCO DE REFERENCIA”

El objetivo principal de este proceso es implementar mecanismos que permitan hacer el marco de referencia más eficiente frente a las demandas de la organización y del mercado en general.

El proceso mejora continua del marco de referencia busca ajustarse a la realidad de la organización y a sus necesidades mediante la toma de decisiones acertadas acerca de lo requerido por sus integrantes, además busca aplicar los cambios necesarios en el marco de referencia.

Para este proceso se identificó el siguiente actor:

- ✓ Director o Encargado de Tecnologías de la información

A petición del usuario final se incluyó entre la descripción que guía la ejecución de este proceso tablas de ENTRADA-SALIDA, para facilitar la comprensión de esta información, para este proceso se preparó la siguiente tabla:

Cliente: Director o Encargado de tecnologías de la información	
ENTRADAS	**SALIDAS**
Planilla PQRS	Planilla de Indexación /PQRS
Planilla PQRS + Planilla de Indexación /PQRS	Planilla de Solución/PQRS

Tabla 11. E/S del encargado de TI en el proceso No. 4

Bajo este proceso se ejecutaran dos procesos de gestión que son los siguientes:

- ✓ Análisis de mejoras del marco de referencia
- ✓ Aplicación de mejoras al marco de referencia

6.2.4.1. ANALISIS DE MEJORAS DEL MARCO DE REFERENCIA

El objetivo de este proceso de gestión es dar solución oportuna a las peticiones, quejas, reclamos y sugerencias interpuestas por todos los integrantes de la organización.

La norma ISO 31000 provee el siguiente concepto para este proceso de gestión:

"*Con base en los resultados del monitoreo y las revisiones, se deberían tomar decisiones sobre la forma en que se podrían mejorar el marco de referencia, la política y el plan para la gestión del riesgo. Estas decisiones deberían originar mejoras en la gestión del riesgo de la organización y en su cultura de la gestión del riesgo"* (ISO, 31000)

Para la ejecución de este proceso de gestión el encargado de tecnologías de la información en conjunto con su equipo de trabajo, estudiarán cada una de las solicitudes hechas, inicialmente las indexarán para tener un mejor manejo de ellas, Finalmente el encargado de tecnologías de la información en conjunto con su equipo de trabajo, darán solución a cada una de las solicitudes hechas.

6.2.4.2. APLICACIÓN DE MEJORAS AL MARCO DE REFERENCIA

El objetivo de este proceso de gestión es aplicar al marco de referencia las soluciones planteadas para dar respuesta a inconsistencias presentadas.

La norma ISO 31000 provee el siguiente concepto para este proceso de gestión:

"*Con base en los resultados del monitoreo y las revisiones, se deberían tomar decisiones sobre la forma en que se podrían mejorar el marco de referencia, la política y el plan para la gestión del riesgo. Estas decisiones deberían originar mejoras en la gestión del riesgo de la organización y en su cultura de la gestión del riesgo"* (ISO, 31000)

Para la ejecución de este proceso de gestión el encargado de tecnologías de la información en conjunto con su equipo de trabajo, aplicarán donde lo crean conveniente mejoras al marco de referencia, basándose en las soluciones planteadas a las solicitudes PQRS, luego en caso de ser necesario el encargado de tecnologías de la información en conjunto con su equipo de trabajo, modificaran de forma parcial o completa el marco de referencia, incluyendo sus procesos, procesos de gestión etc. De esta forma buscarán adaptar el marco de referencia al contexto actual de la organización.

6.3. CONSTRUCCION DE LA GUIA DE EVALUACIÓN DE RIESGOS POR PROCESOS DE GESTIÓN

Seguido a la definición de cada proceso y proceso de gestión se concertó una reunión en la que se socializó cada uno de estos con el usuario final (Corporación Plástica S.A.S., Corplas), para corroborar su idoneidad (Ver Anexo No.2), en esta reunión se hicieron algunas sugerencias, tal como la expresada en el capítulo anterior, correspondiente a la inclusión de tablas que ilustraran las entradas y salidas de cada proceso, Además de esta se hicieron las siguientes sugerencias:

✓ *Incluir en la guía diagramas de flujos convencionales que para indicar el orden del flujo de las actividades a ejecutar en cada proceso de gestión*

✓ *Anexar conjuntos de planillas para ilustrar los procesos.*

✓ *Añadir a las tablas de zona de riesgo y gestión del mismo, colores tradicionales para dar a entender con mayor facilidad el estado actual de los riesgos.*

Con base en lo sugerido por el usuario final e investigaciones del tema, se planteó la construcción de la guía de la siguiente manera:

MACROPROCESO	PROCESO	PROCESOS DE GESTION
✓ **Cadena de Valor**	✓ **Introducción** ✓ **Caracterización** ❖ **Objetivo** ❖ **Política** ❖ **Responsable/Líder del proceso** ❖ **Proceso de gestión** ❖ **Entradas y Salidas del proceso** ✓ **Anexos**	✓ **Introducción** ✓ **Objetivo** ✓ **Alcance** ✓ **Explicación detallada del proceso de gestión.** ✓ **Roles de cada actor presente en este proceso de gestión** ✓ **Diagrama de flujo (Únicamente para los proceso planteados como objeto de estudio en el alcance del proyecto)**

Tabla 12. Aspectos de la guía

6.3.1. PROCESO: “DISEÑO DE MARCO DE REFERENCIA PARA LA GESTIÓN DE RIESGOS”

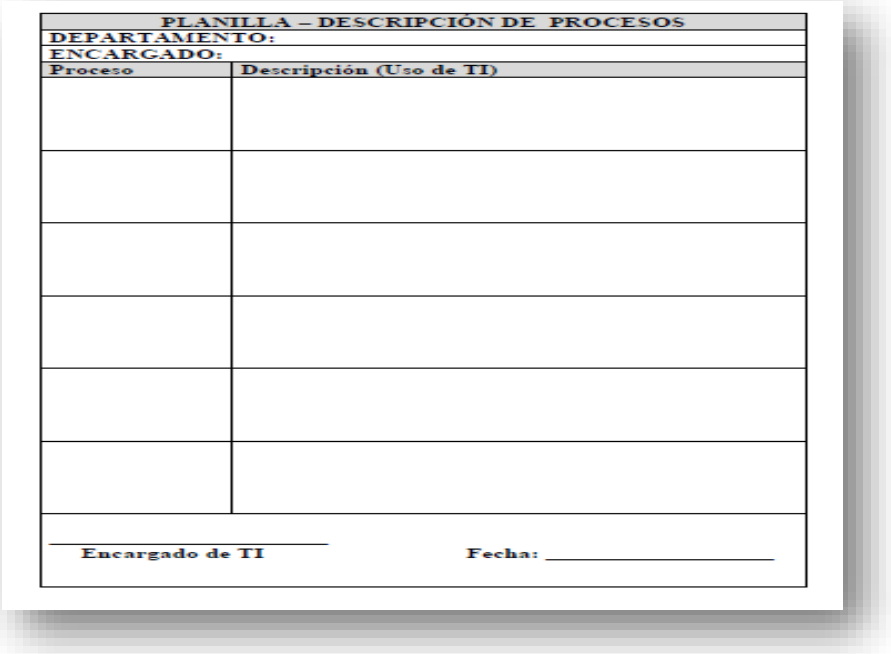
Para la ejecución y desarrollo de este proceso se diseñaron las siguientes planillas, que facilitarán e ilustrarán la implantación pueden ser encontradas en la sección de anexos de la guía:

Planilla de Asistencia

PLANILLA DE ASISTENCIA							
OBJETIVO:							
FECHA:		HORA:			LUGAR:		
RESPONSABLE:							
N°	Nombre y Apellidos	Documento de Identidad	Cargo	Departamento	Teléfono	Correo	Firma

Figura 7. Imagen de planilla de asistencia

Planilla para descripción de procesos

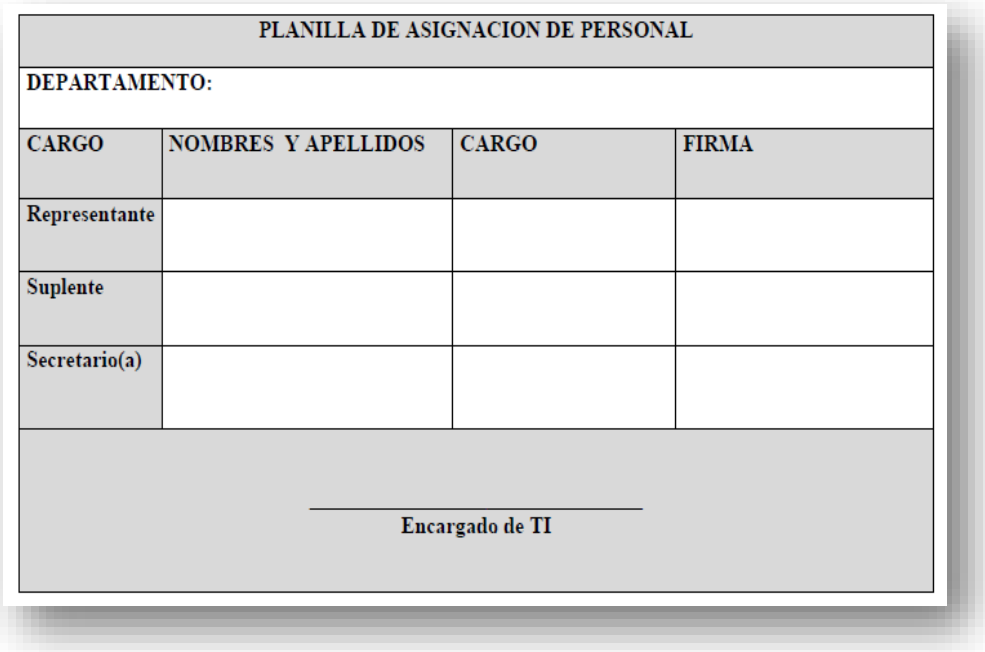


PLANILLA – DESCRIPCIÓN DE PROCESOS	
DEPARTAMENTO:	
ENCARGADO:	
Proceso	Descripción (Uso de TI)

Encargado de TI Fecha: _____

Figura 8. Imagen de planilla de descripción de proceso

Planilla de asignación de personal



PLANILLA DE ASIGNACION DE PERSONAL			
DEPARTAMENTO:			
CARGO	NOMBRES Y APELLIDOS	CARGO	FIRMA
Representante			
Suplente			
Secretario(a)			

Encargado de TI

Figura 9. Imagen de Planilla de asignación de personal

Planilla de contexto interno

PLANTILLA – CONTEXTO INTERNO			
DEPARTAMENTO:			
ENCARGADO:			
PROCESO	SOPORTADO CON TI		RESPONSABLE
	SI	NO	
	SI	NO	
	SI	NO	
	SI	NO	
	SI	NO	
	SI	NO	
	SI	NO	
RECIBIDO			
Encargado de TI		Representante Del Departamento	

Figura 10. Imagen de planilla de contexto interno

Estas planillas son de especial apoyo a los procesos de gestión pertenecientes a este proceso:

2.4. PROCESOS DE GESTIÓN
• Establecimiento de mecanismos de comunicación y consulta. • Establecimiento del contexto.

Figura 11. Imagen de procesos de gestión del proceso No.1

6.3.1.1. PROCESO DE GESTION: "ESTABLECIMIENTO DE MECANISMOS DE COMUNICACIÓN Y CONSULTA"

El proceso de gestión inicia con el desarrollo de la justificación de la implementación de un modelo de evaluación de riesgos en la organización y finaliza con el desarrollo de un cronograma de actividades y un plan de comunicación.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Justificar la necesidad de implementación de un modelo de evaluación de riesgos de TI.
- ✓ Solicitar inclusión del desarrollo de un modelo de riesgos de TI en los mapas de procesos o de procedimientos ejecutados por la organización.
- ✓ Solicitar asignación de recursos.
- ✓ Asignar recursos para la implementación del modelo de evaluación de riesgos de TI.
- ✓ Diseñar plan de comunicación y socializar métodos de rendición de cuentas.

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Director de Tecnologías de la información	Dirigir todo el proceso, hacer las solicitudes correspondientes y desarrollar cada una de las actividades y elementos establecidos
Organización	Estudiar las solicitudes hechas, analizar los resultados de los elementos y actividades desarrolladas

Figura 12. Imagen de tabla de roles del proceso de gestión establecimiento de mecanismos de comunicación y consulta

Como cumplimiento a las sugerencias del usuario final se desarrolló un diagrama de flujo para detallar el orden de las actividades.

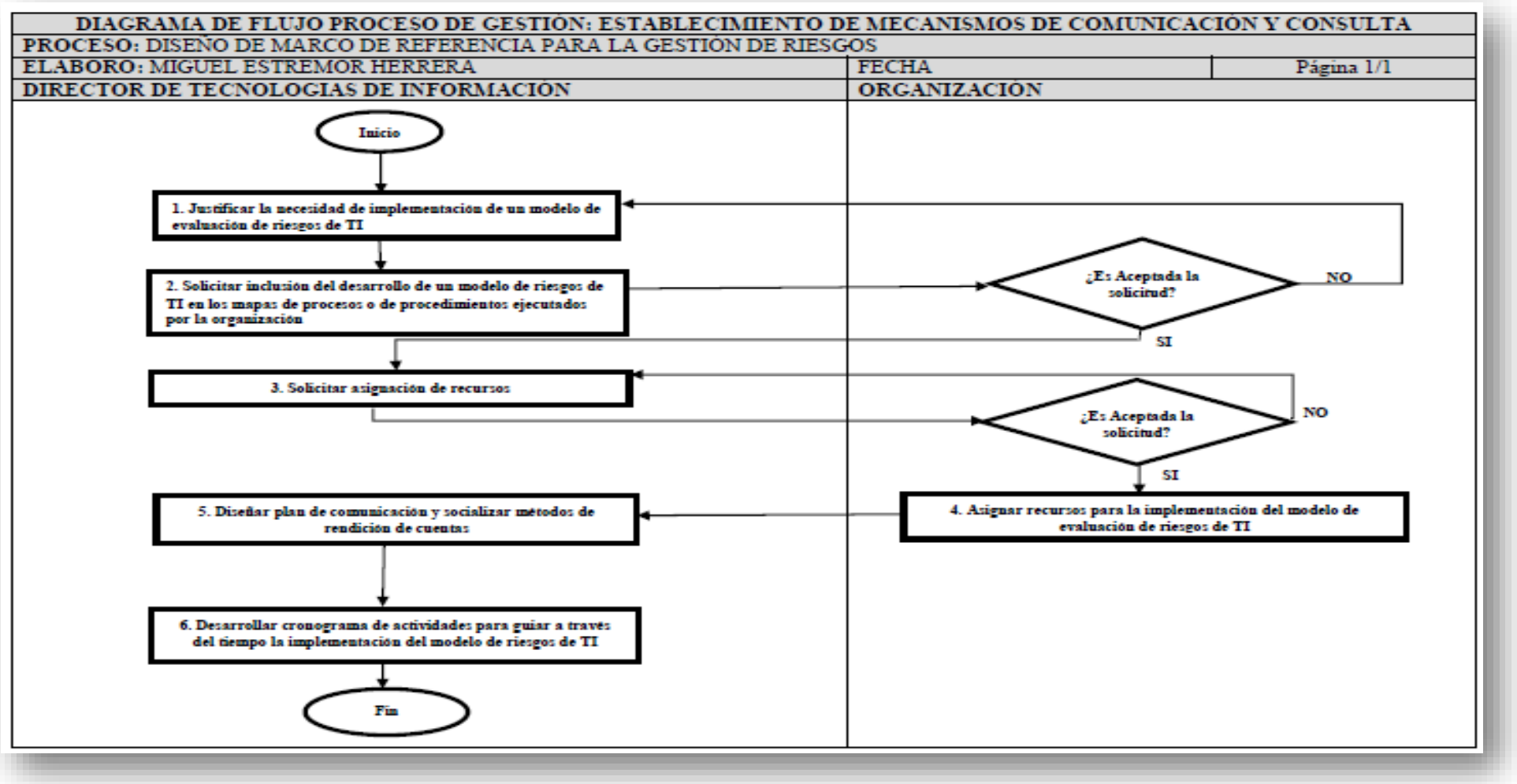


Figura 13. Diagrama de flujo del proceso de gestión "Establecimiento de mecanismos de comunicación y consulta

6.3.1.2. PROCESO DE GESTION: "ESTABLECIMIENTO DEL CONTEXTO"

El proceso de gestión inicia con la identificación de procesos internos de la organización apoyados en tecnologías de información y finaliza con la socialización del contexto interno y externo establecido en consenso por el equipo de trabajo.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Identificar procesos internos de la organización
- ✓ Describir procesos internos de la organización
- ✓ Socializar Contexto interno de la organización
- ✓ Identificar procesos externos de la organización
- ✓ Describir procesos externos de la organización
- ✓ Socializar contexto externo de la organización

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Director de Tecnologías de la información	Guiar la socialización de cada uno de los contextos internos y externos identificados por la representación de los distintos departamentos, y seleccionar los que tengan relaciones más fuertes de dependencia con las tecnologías de información
Representantes de departamentos	Analizar sus respectivos departamentos a nivel de proceso tanto internos como externos y describir de qué forma se relacionan con las tecnologías de información, y luego informar al director de TI de estos.

Figura 14. Imagen de tabla de roles del proceso de gestión establecimiento del contexto

Como cumplimiento a las sugerencias del usuario final se desarrolló un diagrama de flujo para detallar el orden de las actividades.

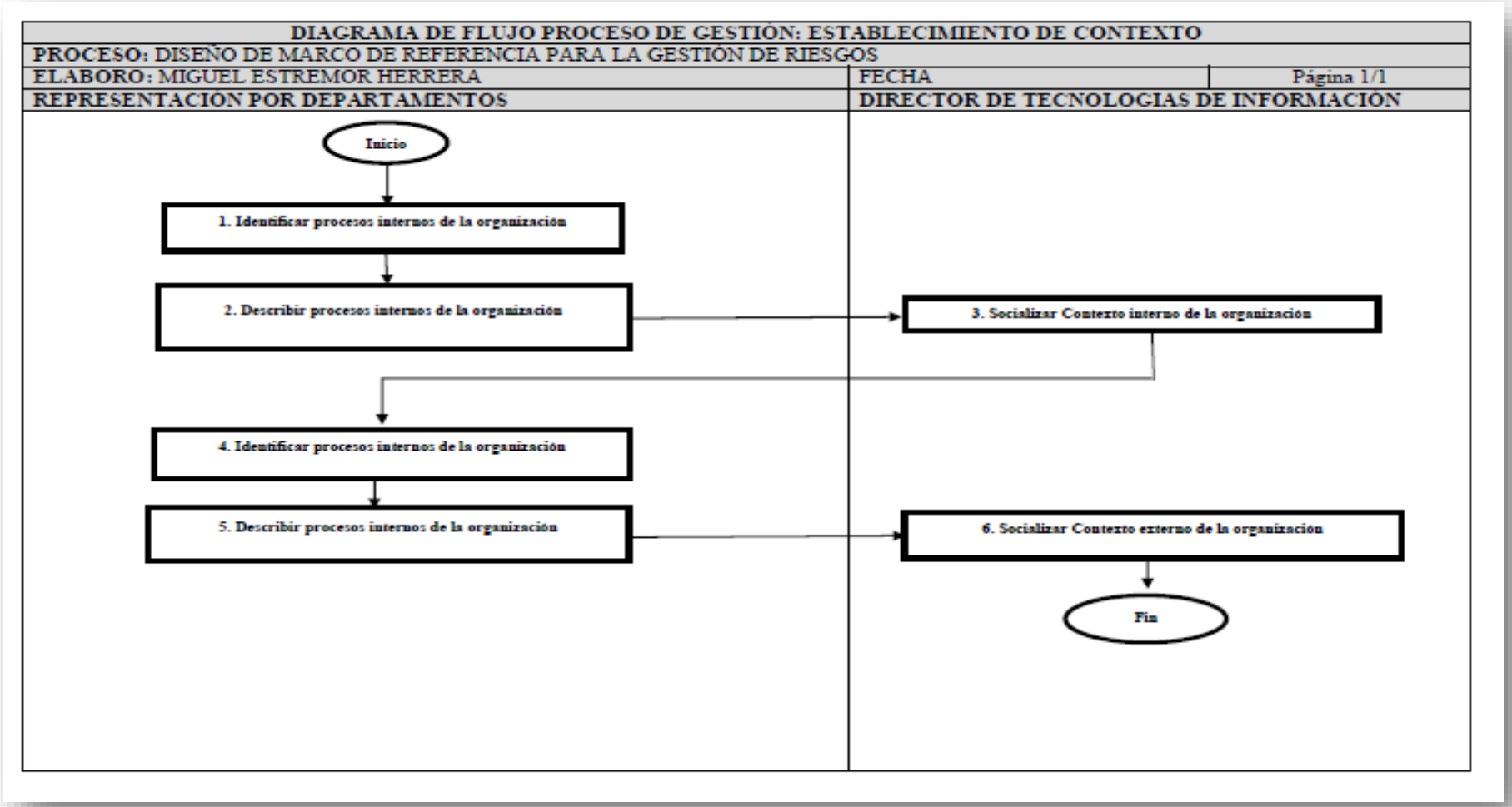


Figura 15. Diagrama de flujo del proceso de gestión establecimiento de contexto

6.3.2. PROCESO: “IMPLEMENTACIÓN DEL MARCO DE REFERENCIA”

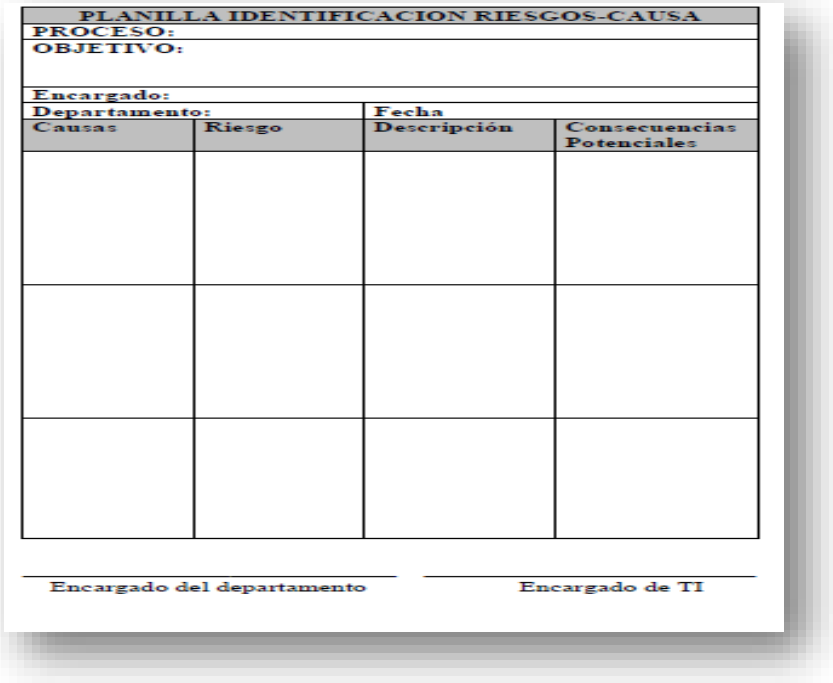
Para la ejecución y desarrollo de este proceso se diseñaron las siguientes planillas, que facilitarán e ilustrarán la implantación pueden ser encontradas en la sección de anexos de la guía:

Planilla de identificación de activos en los procesos

PLANILLA PROCESOS/ACTIVOS	
Departamento:	
Responsable:	
Fecha:	
PROCESO	ACTIVOS
Responsable	Encargado de TI

Figura 16. Imagen de Planilla procesos-activos

Planilla para identificación de causas de riesgos



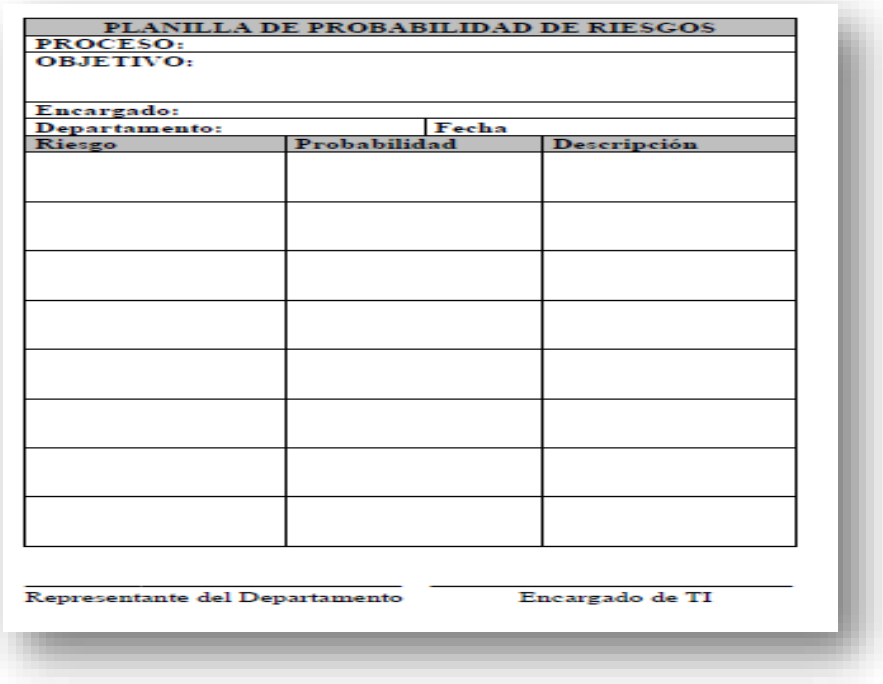
PLANILLA IDENTIFICACION RIESGOS-CAUSA			
PROCESO:			
OBJETIVO:			
Encargado:			
Departamento:		Fecha	
Causas	Riesgo	Descripción	Consecuencias Potenciales

Encargado del departamento

Encargado de TI

Figura 17. Imagen de planillas de identificación de causas de riesgos

Planilla de probabilidad de ocurrencia de riesgos



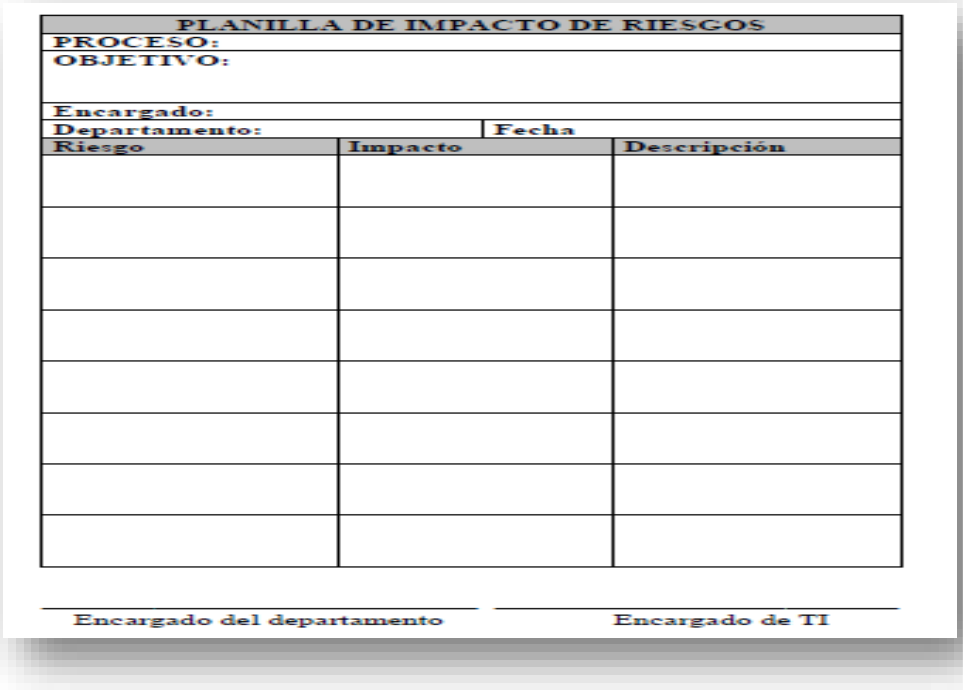
PLANILLA DE PROBABILIDAD DE RIESGOS		
PROCESO:		
OBJETIVO:		
Encargado:		
Departamento:	Fecha	
Riesgo	Probabilidad	Descripción

Representante del Departamento

Encargado de TI

Figura 18. Imagen de planilla de probabilidad

Planilla de Impacto de los riesgos



PLANILLA DE IMPACTO DE RIESGOS

PROCESO:

OBJETIVO:

Encargado:

Departamento: | Fecha

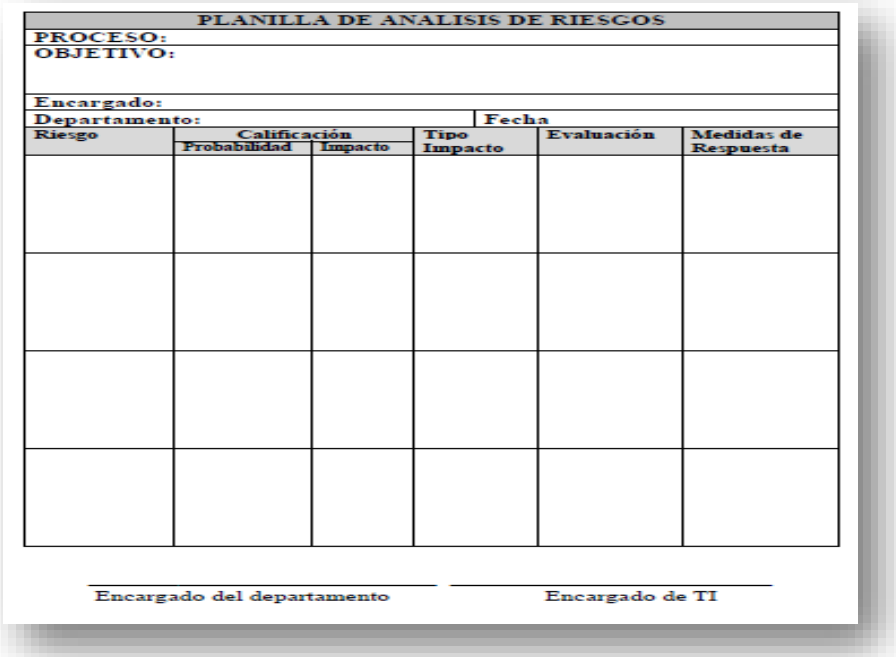
Riesgo	Impacto	Descripción

Encargado del departamento

Encargado de TI

Figura 19. Imagen de planilla de impacto

Planilla de análisis de riesgos



PLANILLA DE ANALISIS DE RIESGOS

PROCESO:

OBJETIVO:

Encargado:

Departamento: | Fecha

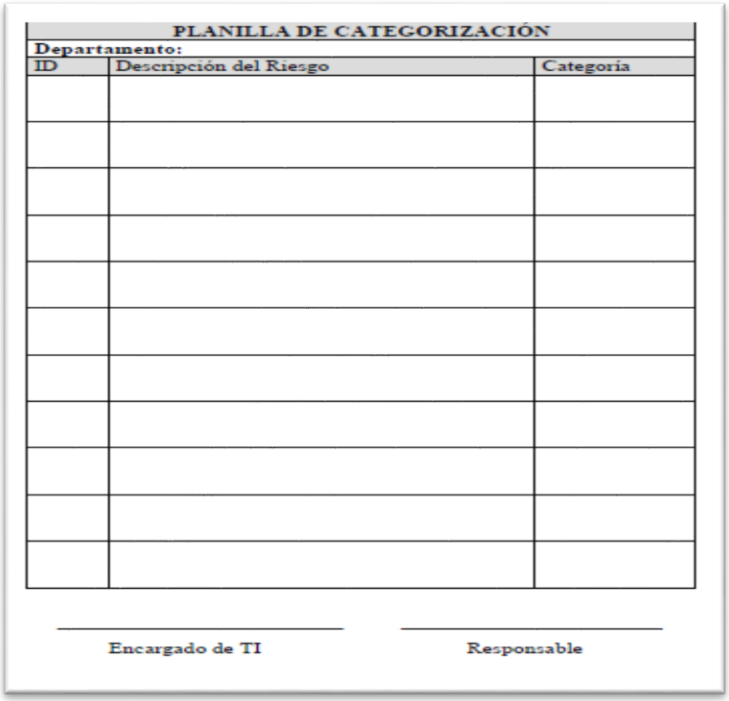
Riesgo	Calificación		Tipo Impacto	Evaluación	Medidas de Respuesta
	Probabilidad	Impacto			

Encargado del departamento

Encargado de TI

Figura 20. Imagen de planilla de análisis de riesgos

Planilla de categorización



PLANILLA DE CATEGORIZACIÓN

Departamento:

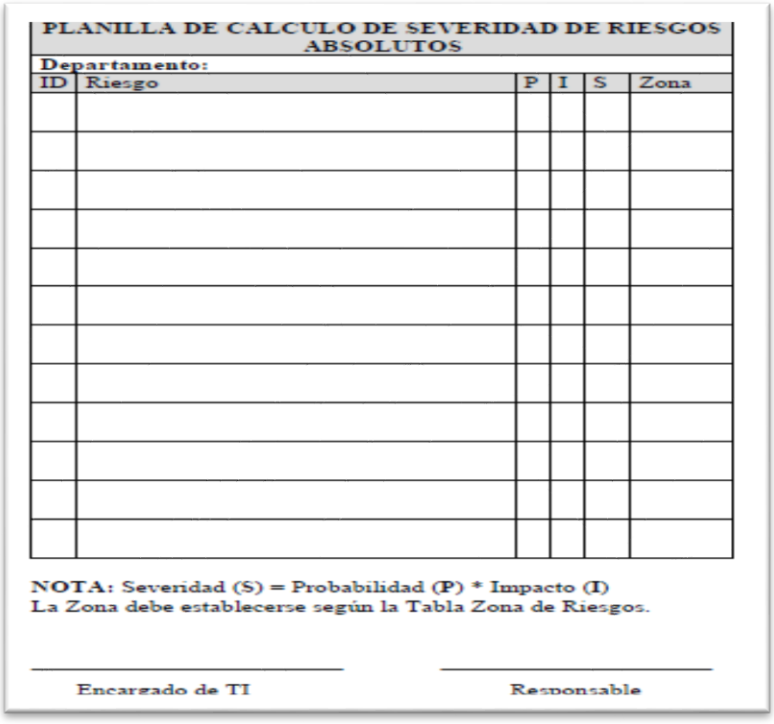
ID	Descripción del Riesgo	Categoría

Encargado de TI

Responsable

Figura 21. Imagen de Planilla de categorización

Planilla de Cálculo de Severidad de riesgos absolutos



PLANILLA DE CALCULO DE SEVERIDAD DE RIESGOS ABSOLUTOS

Departamento:

ID	Riesgo	P	I	S	Zona

NOTA: Severidad (S) = Probabilidad (P) * Impacto (I)
La Zona debe establecerse según la Tabla Zona de Riesgos.

Encargado de TI

Responsable

Figura 22. Imagen de planilla de cálculo de severidad de riesgos absolutos

Tabla de zona de riesgos

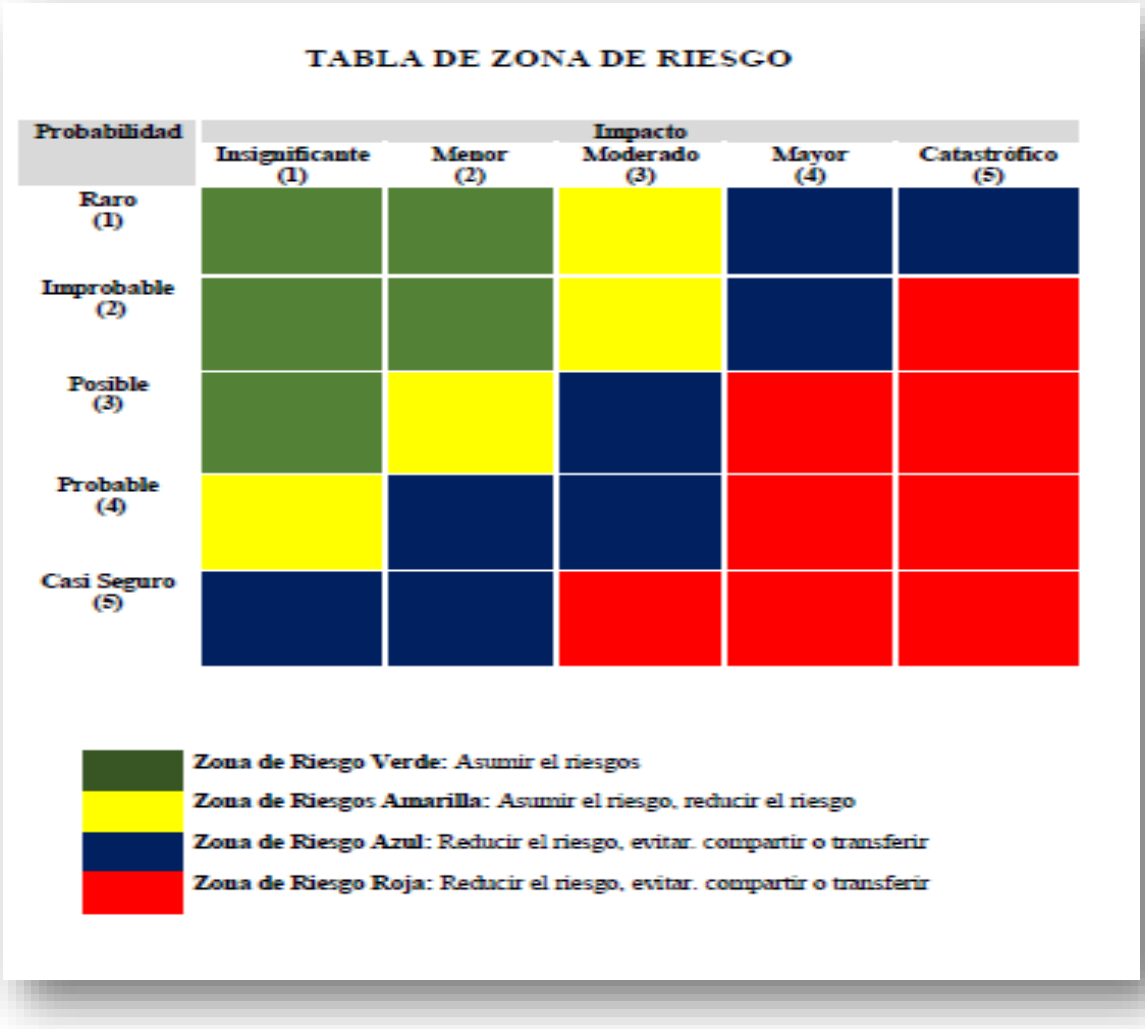


Figura 23. Imagen de Tabla de zona de riesgos

Estas planillas son de especial apoyo a los procesos de gestión pertenecientes a este proceso:

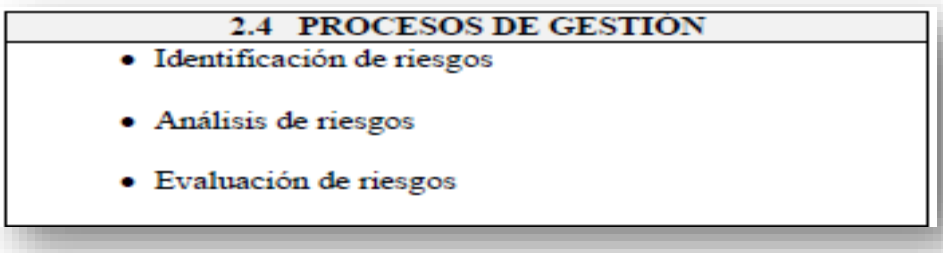


Figura 24. Imagen de tabla de procesos de gestión del proceso No. 2

6.3.2.1. PROCESO DE GESTION: “IDENTIFICACIÓN DE RIESGOS”

El proceso de gestión inicia con la selección de los procesos organizacionales a tratar, a los cuales se les determinaran sus respectivos riesgos y finaliza con un estudio de las causas y consecuencias de los riesgos.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Seleccionar los procesos críticos o principales de la organización para ser tratados y estudiados.
- ✓ Identificar los activos tecnológicos involucrados en la ejecución de los procesos seleccionados para ser tratados.
- ✓ Realizar un inventario de activos tecnológicos con los que cuenta la organización.
- ✓ Analizar cada uno de los procesos organizacionales seleccionados

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Encargado de Tecnologías de la información	Liderar todo el proceso, hacer las solicitudes correspondientes y desarrollar cada una de las actividades y elementos establecidos
Representantes de los departamentos	Ejecutar todas las actividades concernientes a la investigación, identificación y análisis de los procesos que se encuentran a su cargo

Figura 25. Imagen de tabla de roles del proceso de gestión Identificación de riesgos

Como cumplimiento a las sugerencias del usuario final se desarrolló un diagrama de flujo para detallar el orden de las actividades.

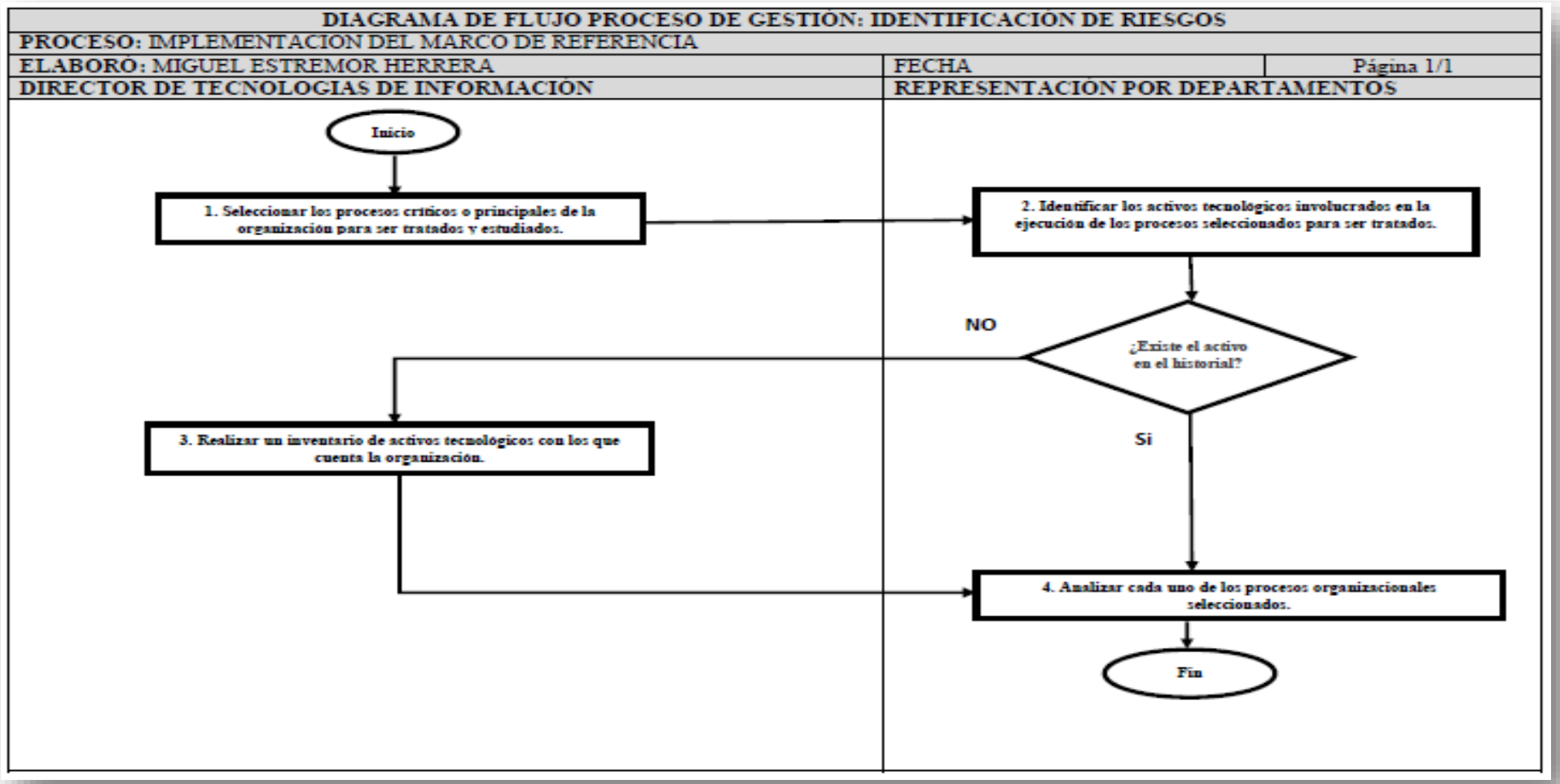


Figura 26. Diagrama de flujo del proceso de gestión Identificación de riesgos

6.3.2.2. PROCESO DE GESTION: “ANALISIS DE RIESGOS”

El proceso de gestión inicia con el establecimiento de probabilidades de ocurrencia de los riesgos previamente identificados, finalmente estos se clasifican y se calcula su nivel con base en el impacto generado y probabilidad de ocurrencia.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Calcular la probabilidad de ocurrencia de los riesgos inherentes a cada proceso.
- ✓ Determinar el Impacto en la organización en caso de ocurrencia de los distintos riesgos de los procesos.
- ✓ Clasificar los riesgos, estableciendo la Zona en la que se encuentran y describir lo que eso implica.

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Encargado de Tecnologías de la información	Liderar todo el proceso Recibir la información de cada uno de los departamentos Definir lo correspondiente a la zona de riesgos, tablas de probabilidad e impacto
Representantes de los departamentos	Ejecutar todas las actividades concernientes al cálculo y definición de las probabilidades de ocurrencia e impactos de los riesgos sobre la organización

Figura 27. Imagen de tabla de roles del proceso de gestión Análisis de riesgos

Como cumplimiento a las sugerencias del usuario final se desarrolló un diagrama de flujo para detallar el orden de las actividades.

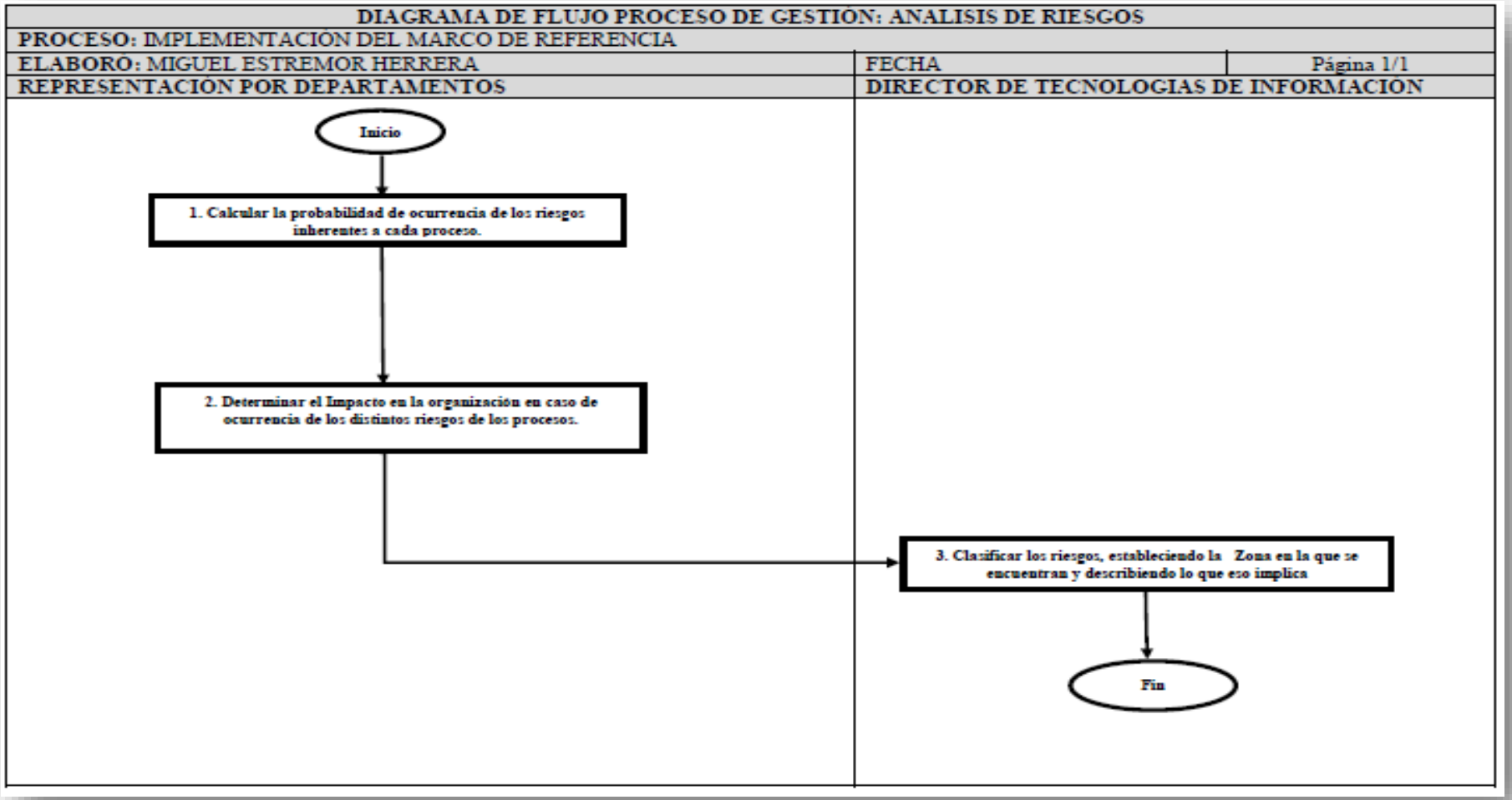


Figura 28. Diagrama de flujo del proceso de gestión análisis de riesgos

6.3.2.3. PROCESO DE GESTIÓN: “EVALUACIÓN DE RIESGOS”

El proceso de gestión inicia con la indexación y categorización de los riesgos previamente analizados, finalmente se calcula la severidad de estos con base en el impacto generado y probabilidad de ocurrencia.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Indexar los riesgos previamente analizados por cada departamento de la organización.
- ✓ Categorizar los riesgos que hayan sido indexados por los diferentes departamentos de la organización.
- ✓ Calcular la severidad de los riesgos analizados, teniendo en cuenta la probabilidad de ocurrencia y el impacto generado en la organización.

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Encargado de Tecnologías de la información	Liderar todo el proceso Recibir la información de cada uno de los departamentos Diligenciar lo correspondiente al cálculo de la severidad de los riesgos.
Representantes de los departamentos	Ejecutar todas las actividades concernientes a la indexación y categorización de los riesgos tratados

Figura 29. Imagen de tabla de roles del proceso de gestión Evaluación de riesgos

Como cumplimiento a las sugerencias del usuario final se desarrolló un diagrama de flujo para detallar el orden de las actividades.

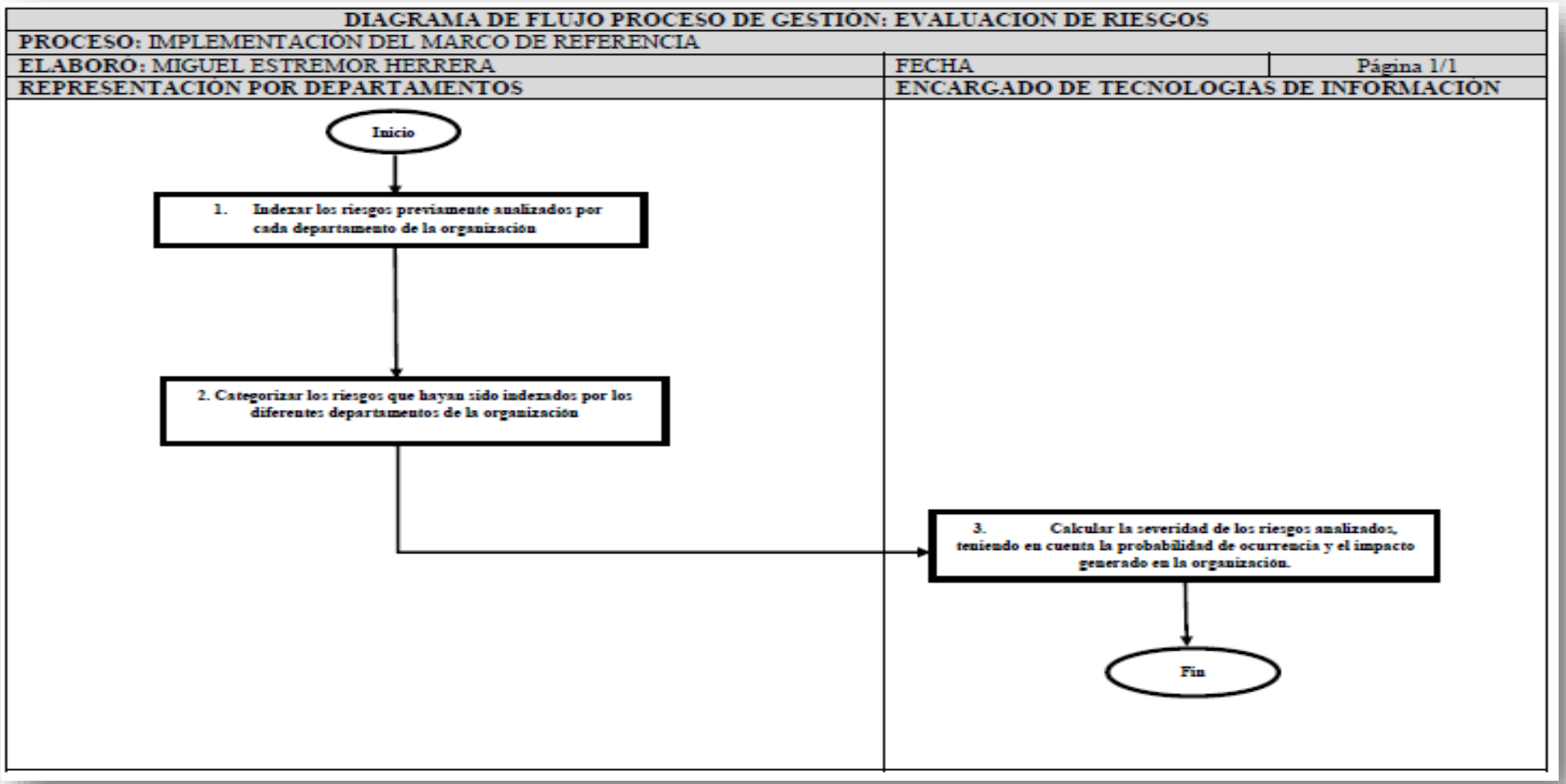
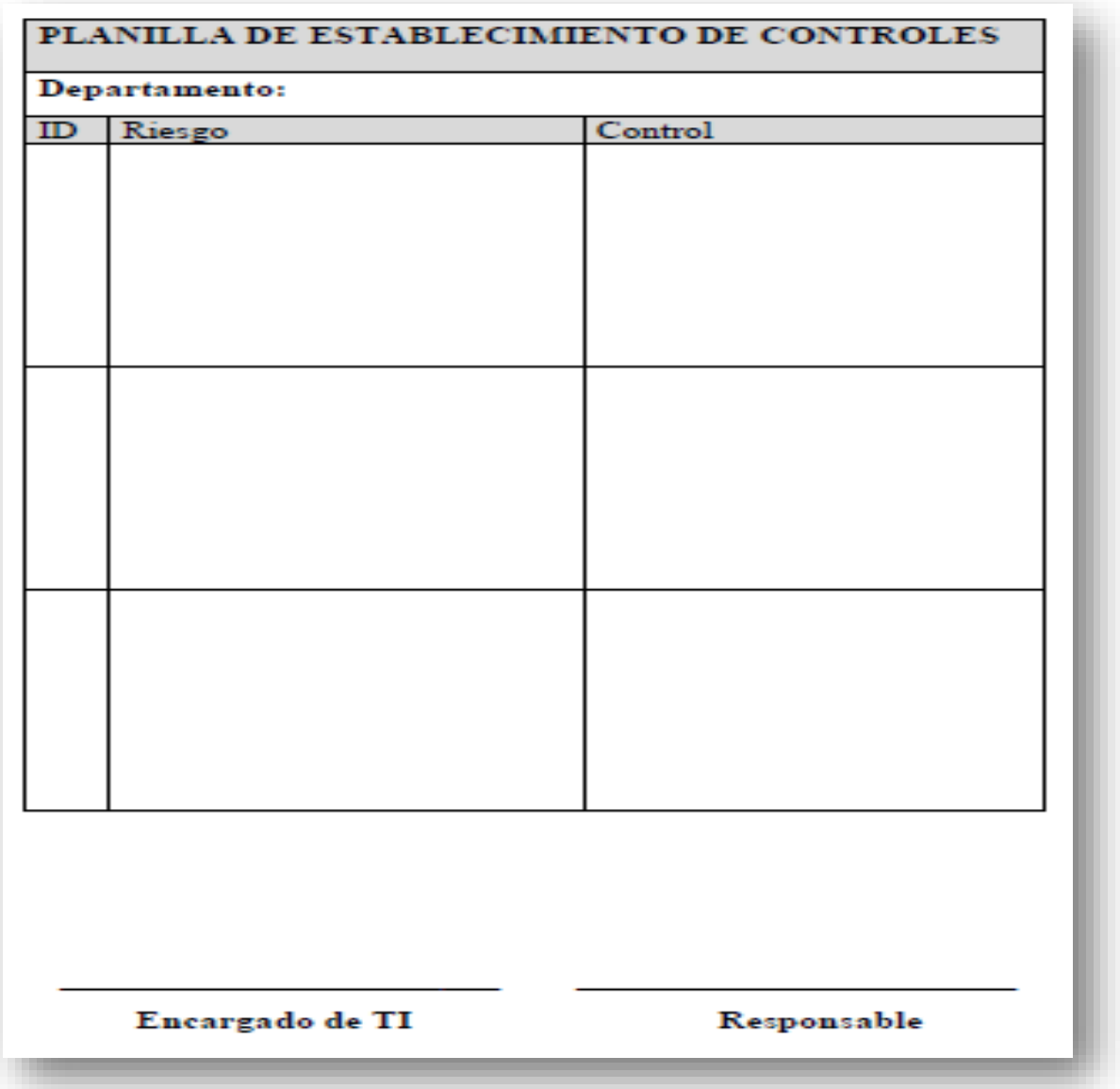


Figura 30. Diagrama de flujo del proceso de gestión Evaluación de riesgos

6.3.3. PROCESO: “MONITORIZACIÓN Y REVISIÓN DEL MARCO DE REFERENCIA”

Para la ejecución y desarrollo de este proceso se diseñaron las siguientes planillas, que facilitarán e ilustrarán la implementación. Pueden ser encontradas en la sección de anexos de la guía:

Planilla de establecimiento de controles



PLANILLA DE ESTABLECIMIENTO DE CONTROLES

Departamento:

ID	Riesgo	Control

Encargado de TI

Responsable

Figura 31, Imagen de planilla de establecimiento de controles

Planilla – Constancia de aplicación de controles

CONSTANCIA DE APLICACIÓN DE CONTROLES				
Departamento:				
ID	Proceso	¿Se Aplicó el Control?		Firma del responsable del Proceso
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	
		SI	NO	

Encargado de TI

Responsable

Figura 32. Imagen de Planilla de constancia de aplicación de controles

Planilla de cálculo de severidad de riesgos controlados

PLANILLA DE CALCULO DE SEVERIDAD DE RIESGOS CONTROLADOS					
Departamento:					
ID	Riesgo	P	I	S	Zona

NOTA: Severidad (S) = Probabilidad (P) * Impacto (I)
La Zona debe establecerse según la Tabla Zona de Riesgos.

Encargado de TI

Responsable

Figura 33. Imagen de Planilla de Cálculo de severidad de riesgos controlados

Planilla de verificación de mejora

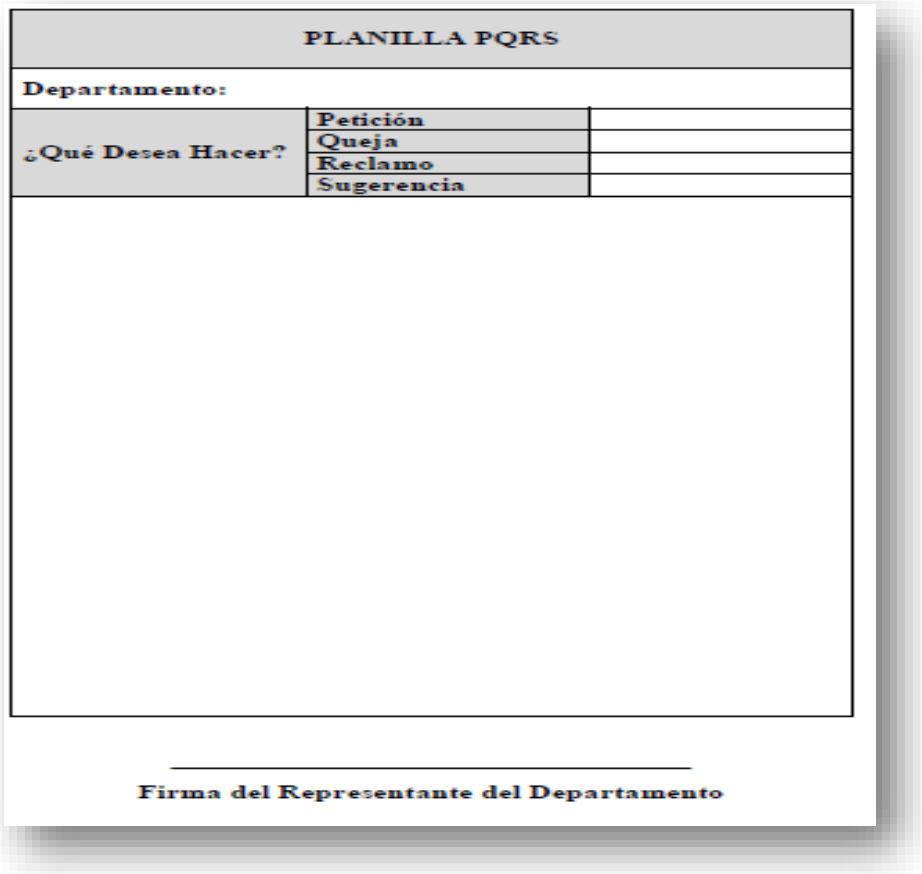
PLANILLA DE VERIFICACION DE MEJORA			
Departamento:			
Proceso	Severidad	Riesgos Absolutos	Riesgos Controlados
	Zona Roja		
	Zona Azul		
	Zona Amarilla		
	Zona Verde		
	Zona Roja		
	Zona Azul		
	Zona Amarilla		
	Zona Verde		
	Zona Roja		
	Zona Azul		
	Zona Amarilla		
	Zona Verde		
	Zona Roja		
	Zona Azul		
	Zona Amarilla		
	Zona Verde		
	Zona Roja		
	Zona Azul		
	Zona Amarilla		
	Zona Verde		
	Zona Roja		
	Zona Azul		
	Zona Amarilla		
	Zona Verde		
	Zona Roja		
	Zona Azul		
	Zona Amarilla		
	Zona Verde		

Encargado de TI

Responsable

Figura 34. Imagen de Planilla de verificación de mejora

Planilla de solicitudes PQRS

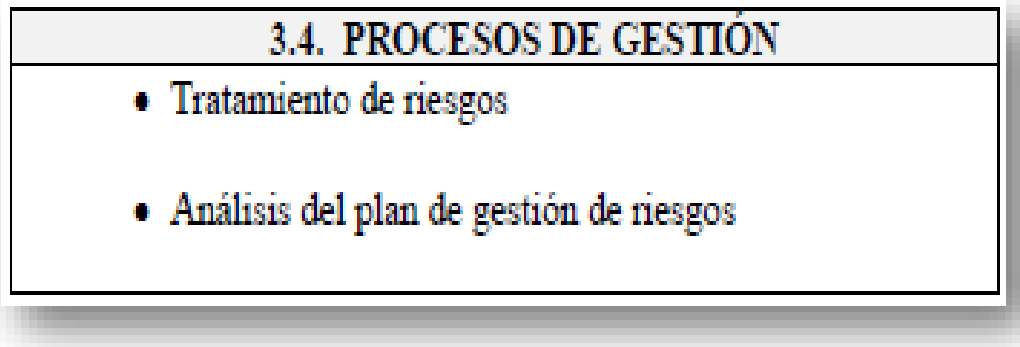


PLANILLA PQRS		
Departamento:		
¿Qué Desea Hacer?	Petición	
	Queja	
	Reclamo	
	Sugerencia	

Firma del Representante del Departamento

Figura 35. Imagen de Planilla PQRS

Estas planillas son de especial apoyo a los procesos de gestión pertenecientes a este proceso:



3.4. PROCESOS DE GESTIÓN
• Tratamiento de riesgos
• Análisis del plan de gestión de riesgos

Figura 36. Imagen de tabla de proceso de gestión del proceso No. 3

6.3.3.1. PROCESO DE GESTION: “TRATAMIENTO DE RIESGOS”

El proceso de gestión inicia con el diseño de los planes o controles que permitan aminorar las consecuencias de estos sobre la organización y finaliza con actividades que permitan la verificación de la mejora por la aplicación de los controles a cada uno de los riesgos.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Diseñar mecanismos de control para los riesgos evaluados.
- ✓ Aplicar los mecanismos de control diseñados para cada uno de los riesgos.
- ✓ Evaluar los riesgos, después de haber aplicado los controles recomendados.
- ✓ Verificar el efecto de los riesgos sobre la organización, después de la nueva evaluación.

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Encargado de Tecnologías de la información	Liderar todo el proceso, hacer las solicitudes correspondientes y desarrollar cada una de las actividades y elementos establecidos
Representantes de los departamentos	Ejecutar todas las actividades concernientes a la asignación de controles para los riesgos Coordinar la aplicación de los controles diseñados.
Personal general de la organización	Aplicar los controles diseñados por el equipo de trabajo.

Figura 37. Imagen de tabla de roles del proceso de gestión Tratamiento de riesgos

Como cumplimiento a las sugerencias del usuario final se desarrolló un diagrama de flujo para detallar el orden de las actividades.

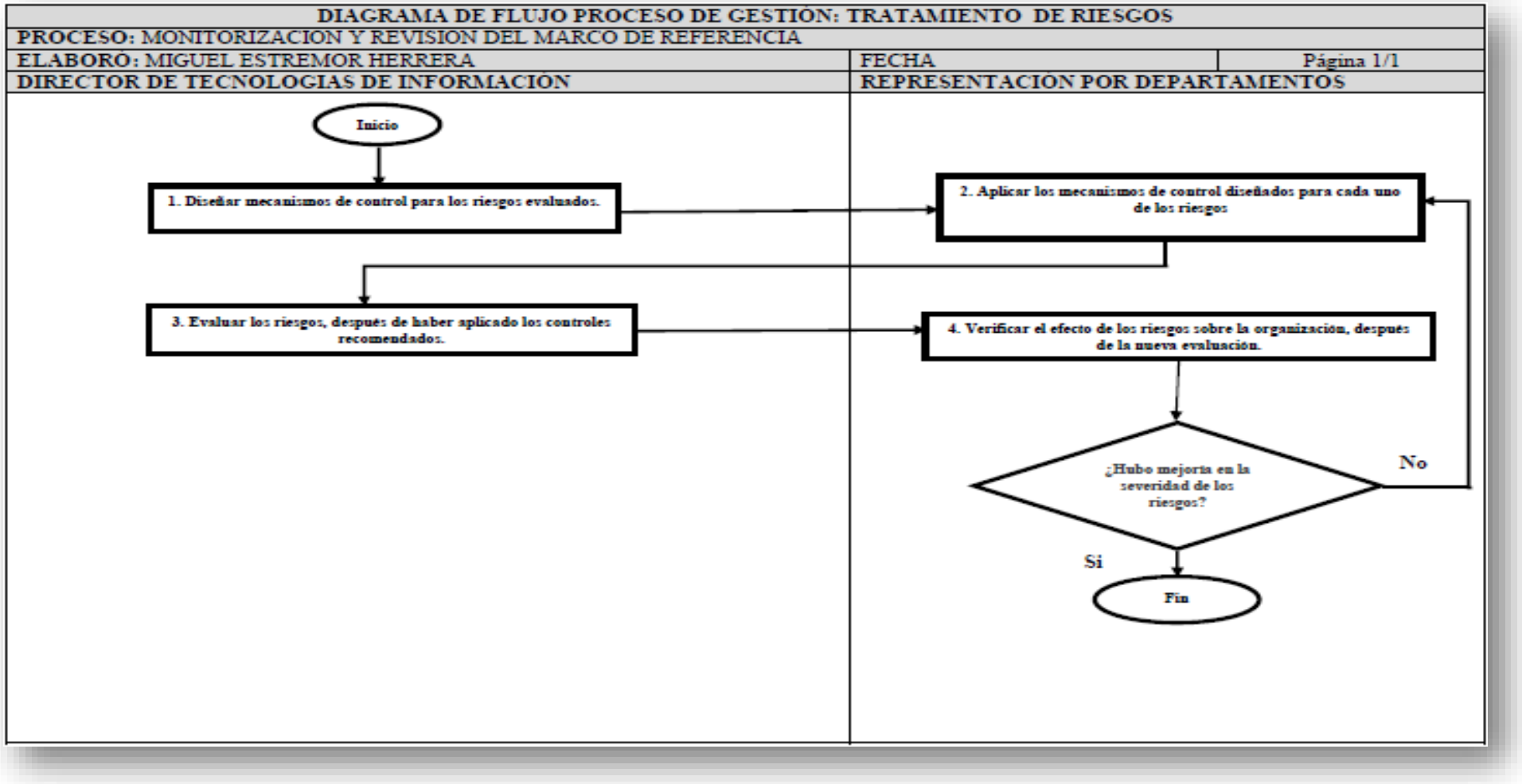


Figura 38. Diagrama de flujo del proceso de gestión Tratamiento de riesgos

6.3.3.2. PROCESO DE GESTION: “ANALISIS DEL PLAN DE GESTIÓN DE RIESGOS”

El proceso de gestión está desarrollado para que los miembros de la organización puedan expresar su opinión acerca de todo lo concerniente al marco de referencia que se está utilizando.

Para efecto de elaboración de la guía, en este proceso de gestión se identificó la siguiente actividad:

- ✓ Formular peticiones, quejas, reclamos o sugerencias sobre el marco de referencia.

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

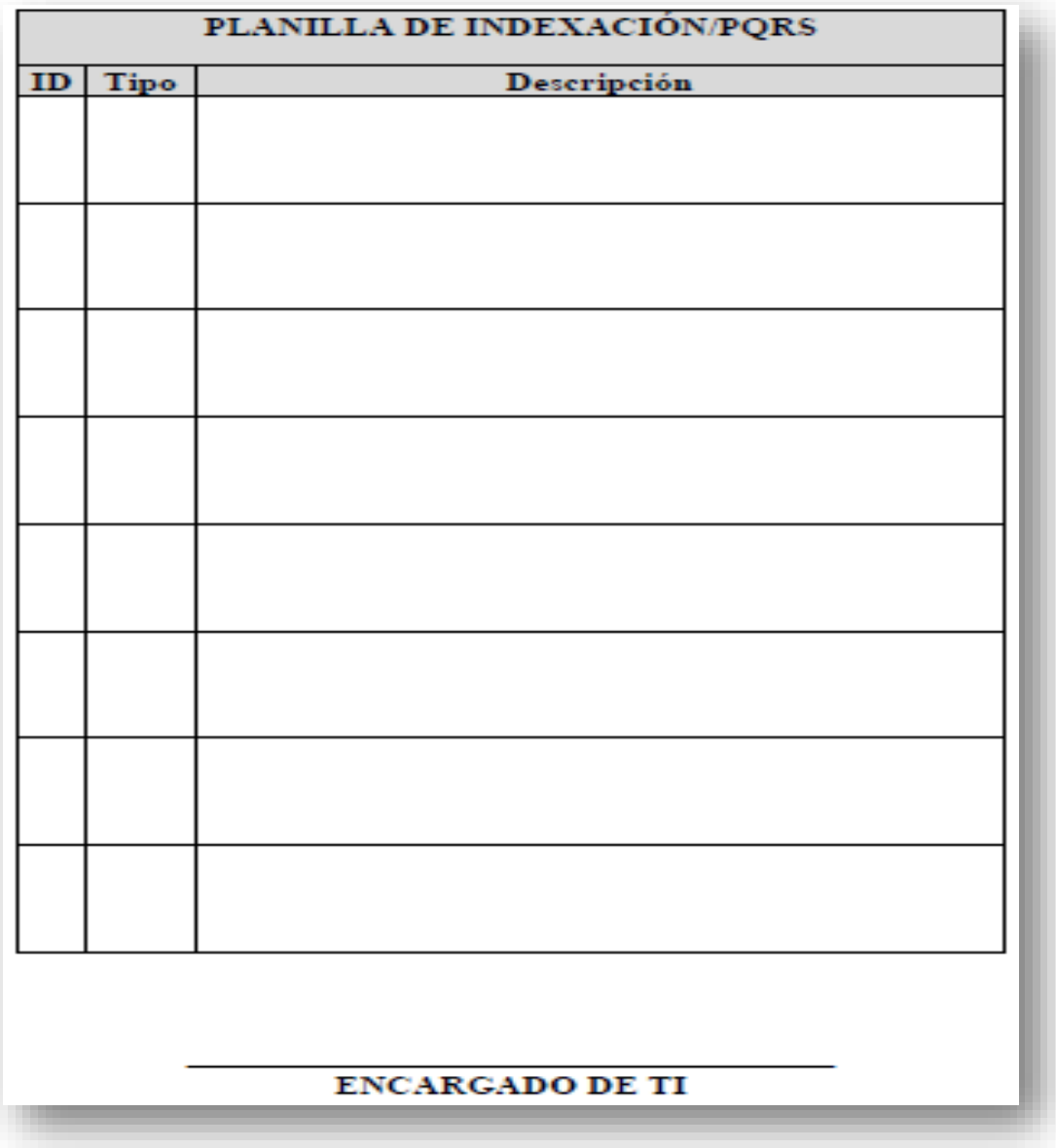
Nombre del Ente	Rol
Encargado de Tecnologías de la información	Liderar el análisis de todas las peticiones, quejas, reclamos y sugerencias interpuestas por todo el personal
Representantes de los departamentos	Recibir las peticiones, quejas, reclamos y sugerencias interpuestas por todo el personal Acompañar el proceso de análisis de todas las peticiones, quejas, reclamos y sugerencias interpuestas por todo el personal
Personal general del organización	Fortalecer el marco de referencia mediante la formulación de peticiones, quejas, reclamos y sugerencias

Figura 39. Imagen de tabla de roles del proceso de gestión Análisis del plan de gestión de riesgos

6.3.4. PROCESO: “MEJORA CONTINUA DEL MARCO DE REFERENCIA”

Para la ejecución y desarrollo de este proceso se diseñaron las siguientes planillas, que facilitarán e ilustrarán la implantación pueden ser encontradas en la sección de anexos de la guía:

Planilla de indexación de solicitud PQRS



PLANILLA DE INDEXACIÓN/PQRS

ID	Tipo	Descripción

ENCARGADO DE TI

Figura 40. Imagen de Planilla de Indexación

Planilla de atención a solicitudes PQRS

PLANILLA DE SOLUCION/PQRS			
ID	Solución	Aplicación	
		SI	NO
		SI	NO
		SI	NO
		SI	NO
		SI	NO
		SI	NO
		SI	NO
		SI	NO

ENCARGADO DE TI

Figura 41. Imagen de Planilla de soluciones a solicitudes PQRS

Estas planillas son de especial apoyo a los procesos de gestión pertenecientes a este proceso:

2.4. PROCESOS DE GESTIÓN
• Análisis de mejoras del marco de referencia
• Aplicación de mejoras al marco de referencia

Figura 42. Imagen de tabla de proceso de gestión del proceso No. 4

6.3.4.1. PROCESO DE GESTION: “ANALISIS DE MEJORAS DEL MARCO DE REFERENCIA”

El proceso de gestión inicia con el análisis de cada petición, queja, reclamo y sugerencia y finaliza con el planteamiento de una solución a las mismas.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Analizar todas las solicitudes PQRS.
- ✓ Dar solución a todas las solicitudes PQRS

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Encargado de Tecnologías de la información	Analizar las solicitudes PQRS Solucionar las solicitudes PQRS
Representantes de los departamentos	Apoyar el Análisis de las solicitudes PQRS Apoyar la búsqueda de soluciones a las solicitudes PQRS

Figura 43.Imagen de tabla de roles del proceso de gestión Análisis de mejoras del marco de referencia

6.3.4.2. PROCESO DE GESTIÓN: "APLICACIÓN DE MEJORAS AL MARCO DE REFERENCIA"

El proceso de gestión inicia con la aplicación de las mejoras propuestas para el marco de referencia y puede llegar hasta la reestructuración del mismo.

Para efecto de elaboración de la guía, en este proceso de gestión se identificaron las siguientes actividades:

- ✓ Aplicar mejoras estudiadas al marco de referencia.
- ✓ Reestructurar el marco de referencia

Además, se identificaron algunos actores principales, con roles específicos en este proceso de gestión:

Nombre del Ente	Rol
Encargado de Tecnologías de la información	Aplicar mejoras al marco de referencia Reestructurar el marco de referencia
Representantes de los departamentos	Apoyar la aplicación de mejoras al marco de referencia Apoyar la reestructuración del marco de referencia

Figura 44. Imagen de tabla de roles del proceso de gestión Aplicación de mejoras al marco de referencia

6.4. PRUEBA, ANALISIS Y RETROALIMENTACION DE LA GUIA

La realización de este proyecto estuvo asesorada y contó con acompañamiento y evaluación por parte del personal interesado dentro de la empresa CORPLAS, desde sus etapas iniciales hasta las finales.

6.4.1. Corporación Plástica S.A.S – CORPLAS

CORPLAS, Es una empresa solida con 36 años de experiencia en la producción y comercialización de envases, tapas y piezas plásticas, entre otras cosas, reconoce que su recurso humano es el factor principal para alcanzar las metas propuestas.

6.4.1.1. MISION

Fabricar piezas plásticas con tecnologías de punta para clientes del sector industrial, brindándoles la mejor solución para la conservación e identidad de sus productos

6.4.1.2. VISION

Seremos el proveedor más confiable de piezas plásticas para nuestros clientes

6.4.1.3. CONTEXTO INICIAL DE LA IMPLEMENTACIÓN DEL PROYECTO EN EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN

El departamento de tecnologías de la información en esta empresa es reciente, desde sus inicios se había encargado únicamente del desarrollo de software y el soporte técnico en general, y se encontraba inmerso en el área administrativa, por lo que carecía de independencia. En vista de esto se optó por conformar un equipo de trabajo organizado más adelante como un departamento.

Luego de una auditoría realizada al interior de la organización, se encontró que una parte considerable de los riesgos e irregularidades presentados en la empresa pudieron haberse controlado desde el departamento de TI, por ello se pensó en implementar un modelo de riesgo tecnológicos, usando normas actuales y vigentes, razón por la cual se seleccionó la norma ISO 31000.

Al iniciar el desarrollo del proyecto se encontró el siguiente inconveniente:
Dado que el departamento de TI es reciente existía poca documentación de los procesos, lo cual es fundamental para aplicar un modelo de gestión de riesgos fundamentado en la norma ISO 31000 y debido a que el tiempo para realizar esta documentación excedería el tiempo asignado para el desarrollo de este proyecto, sólo se sentaron las bases para la ejecución del mismo, por lo que el proceso de pruebas se centró en el acompañamiento por parte del equipo de trabajo de dicho departamento al diseño e implementación del marco de referencia y la construcción de la guía propuesta.

6.4.2. CONSTRUCCIÓN Y SOCIALIZACION DEL MARCO DE REFERENCIA

Inicialmente, antes de la construcción de la guía se planteó un modelo para el marco de referencia a utilizar, este se construyó con base en la norma y metodología establecidas (ISO 31000 y PHVA, respectivamente), y fue propuesto y socializado al equipo de trabajo del departamento de tecnologías de la información de la empresa, luego se sugirió el diseño de una cadena de valor, con los procesos fundamentales en lo correspondiente a evaluación de riesgos de TI, en esa reunión de socialización se realizaron algunas sugerencias para la construcción de la guía (Ver Anexo No. 2), dichas sugerencias fueron atendidas completamente.

- Incluir tablas de entradas y salidas que faciliten la comprensión y ejecución de los procesos descritos.
- Incluir en la guía diagramas de flujos convencionales para indicar el orden de flujo de las actividades a ejecutar en cada proceso de gestión.
- Anexar conjunto de planillas para ilustrar los procesos.
- Añadir a las tablas de zona de riesgo y gestión del mismo, colores tradicionales para dar a entender con mayor facilidad el estado actual de los riesgos.

Finalmente la cadena de valor planteada para el desarrollo de la guía quedó de la siguiente manera:

CADENA DE VALOR MODELO DE GESTIÓN

MACROPROCESO	PROCESOS	PROCESOS DE GESTIÓN
GESTION DE RIESGOS DE TECNOLOGÍAS DE INFORMACION	Diseño de Marco de referencia para la gestión de riesgos	Establecimiento de mecanismos de comunicación y consulta
		Establecimiento del contexto
	Implementación del Marco de referencia	Identificación de riesgos
		Análisis de riesgos
		Evaluación de riesgos
	Monitorización y revisión del Marco de referencia	Tratamiento de riesgos
		Análisis del plan de gestión de riesgos
	Mejora continua del Marco de referencia	Análisis de mejoras del marco de referencia
		Aplicación de mejoras al marco de referencia

Figura 45. Cadena de valor de la guía

6.4.3. CONSTRUCCIÓN Y SOCIALIZACIÓN DE LA GUIA

La etapa de construcción de la guía, fue asesorada y acompañada en todo momento por el departamento de tecnología de la información de la empresa antes mencionada, específicamente por quien figura como asesorar de este proyecto, es a saber el Ingeniero Camilo Velásquez, quien estuvo en todo momento enriqueciendo el proceso de construcción de esta guía.

El acompañamiento se realizó de la siguiente manera:

Inicialmente, a petición del equipo de trabajo del departamento de TI, se desarrolló una caracterización de cada uno de los procesos, esto para facilitar su comprensión y posterior implementación. Luego se socializaron y se plasmaron en la guía.

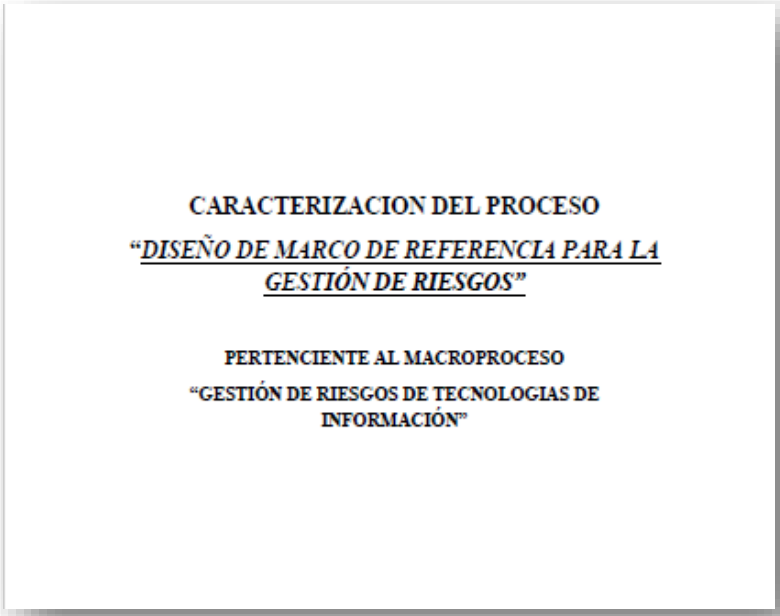


Figura 46. Portada de la caracterización del proceso "Diseño del marco de referencia para la gestión de riesgos"

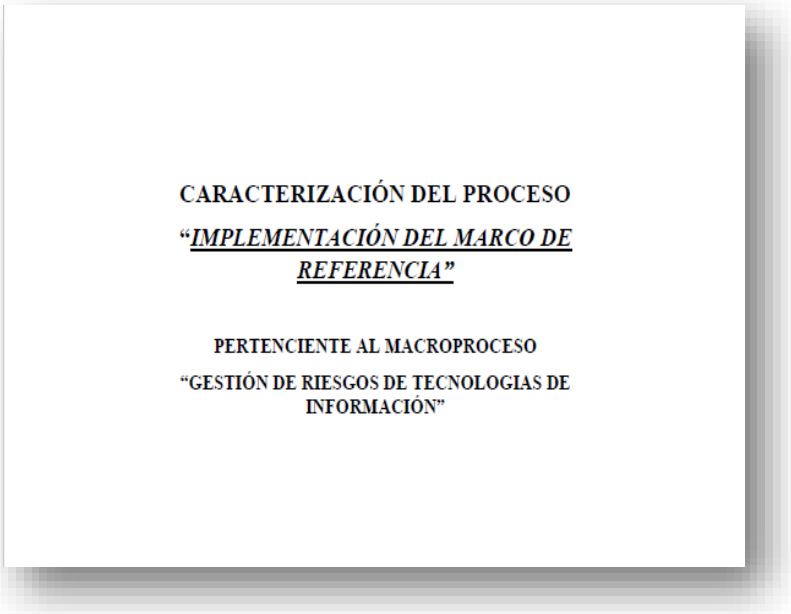


Figura 47. Portada de la caracterización del proceso "Implementación del maco de referencia"

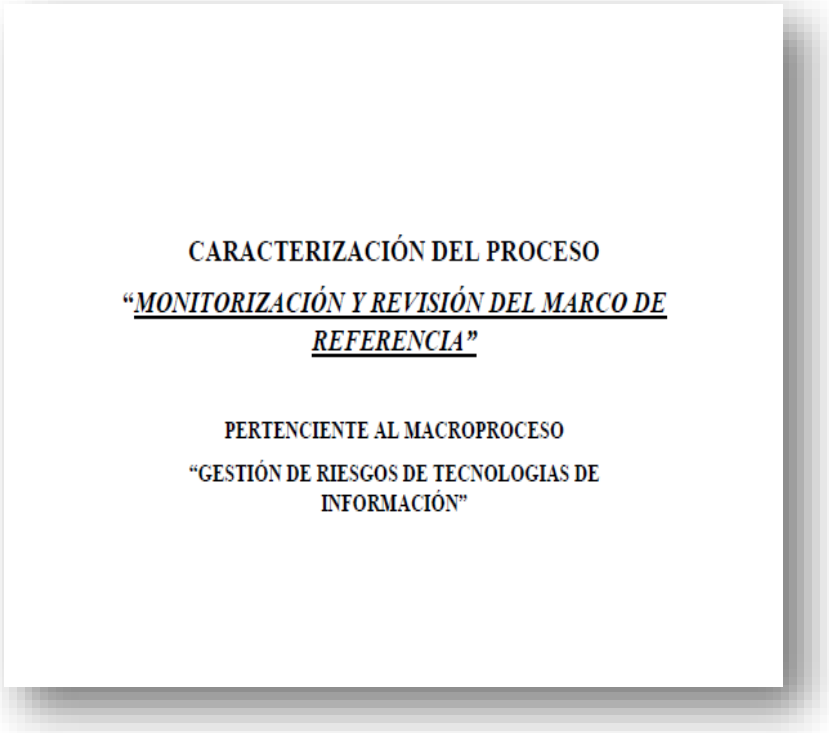


Figura 48. Portada de la caracterización del proceso "Monitorización y revisión del marco de referencia"

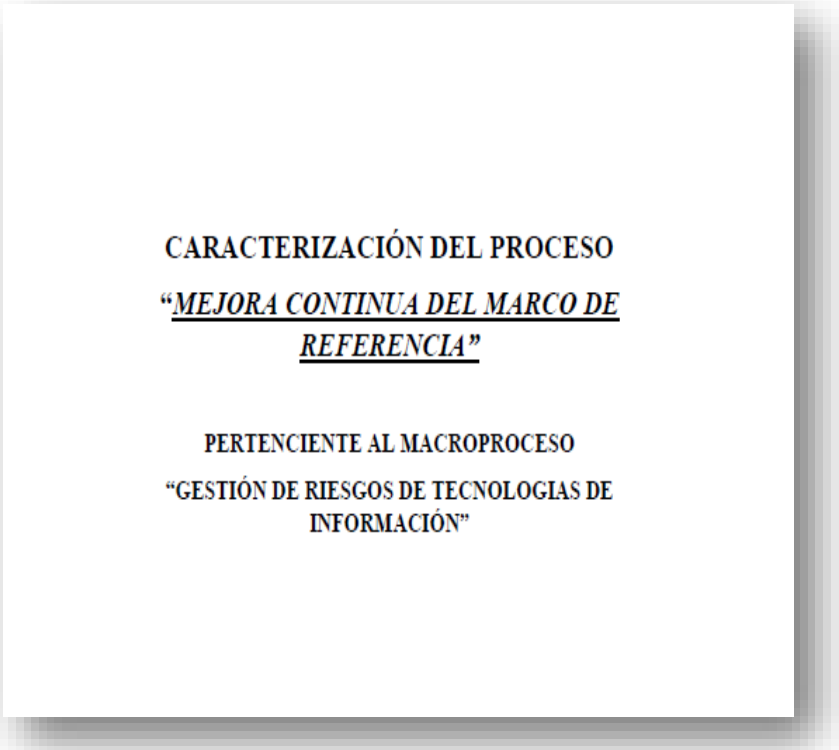


Figura 49. Portada de la caracterización del proceso "Mejora continua del marco de referencia"

Por último, se realizó un “diseño detallado” de cada uno de los proceso de gestión a implementar en la empresa CORPLAS, luego, esto se socializó con el equipo de trabajo del departamento de tecnologías de información, quienes finalmente avalaron la guía desarrollada (Ver Anexo No.3).

A continuación se muestran las respectivas portadas de los diseños detallados de los distintos procesos de gestión:


DISEÑO DETALLADO DEL PROCESO DE GESTIÓN

“ESTABLECIMIENTO DE MECANISMOS DE COMUNICACIÓN Y CONSULTA”

MACROPROCESO GESTIÓN DE RIESGOS DE TECNOLOGIAS DE INFORMACIÓN Y PROCESO

“Diseño de Marco de Referencia para la Gestión de Riesgos”

Figura 50. Portada del proceso de gestión "Establecimiento de mecanismos de comunicación y consultas"

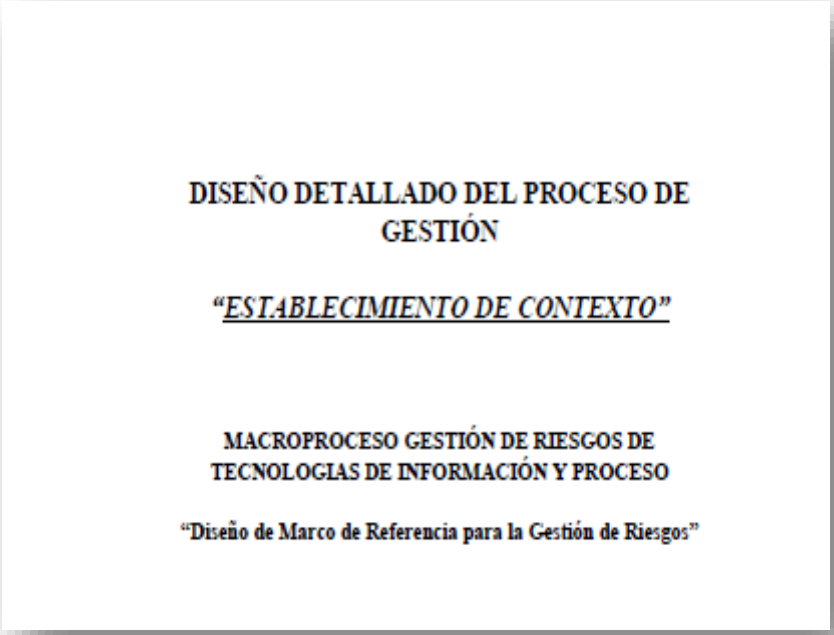


Figura 51. Portada del proceso de gestión "Establecimiento del contexto"

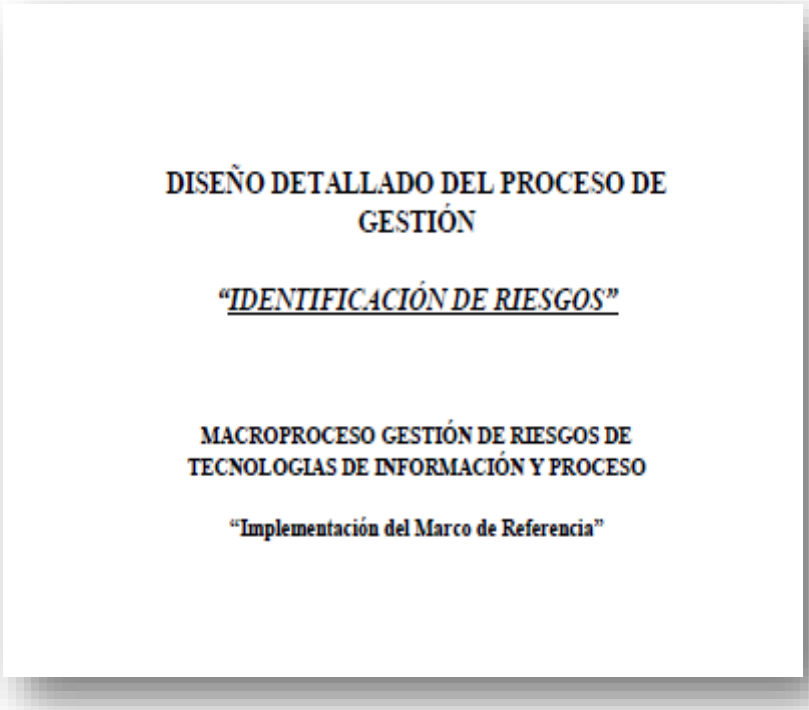


Figura 52. Portada del proceso de gestión "Identificación de riesgos"

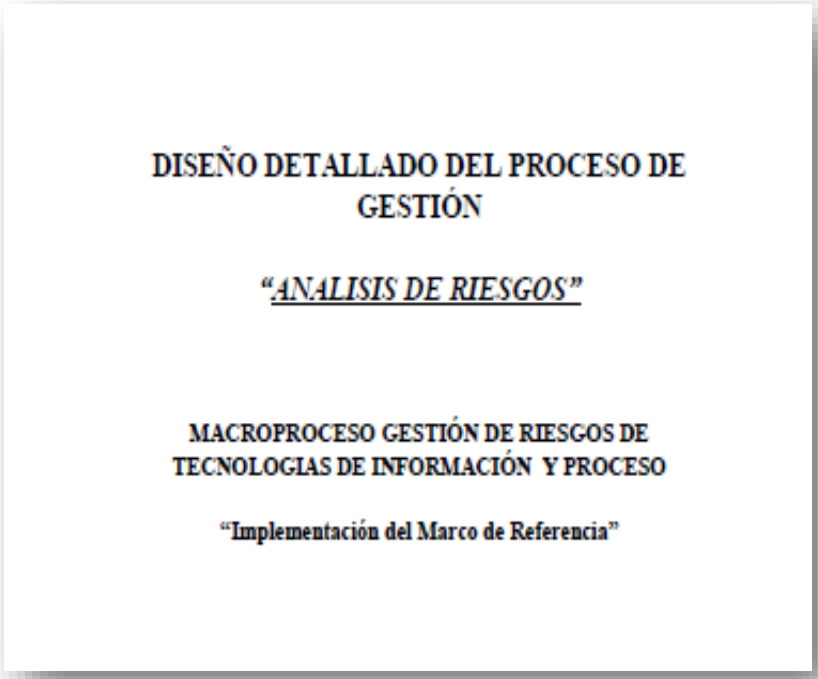


Figura 53. Portada del proceso de gestión "Análisis de riesgos"

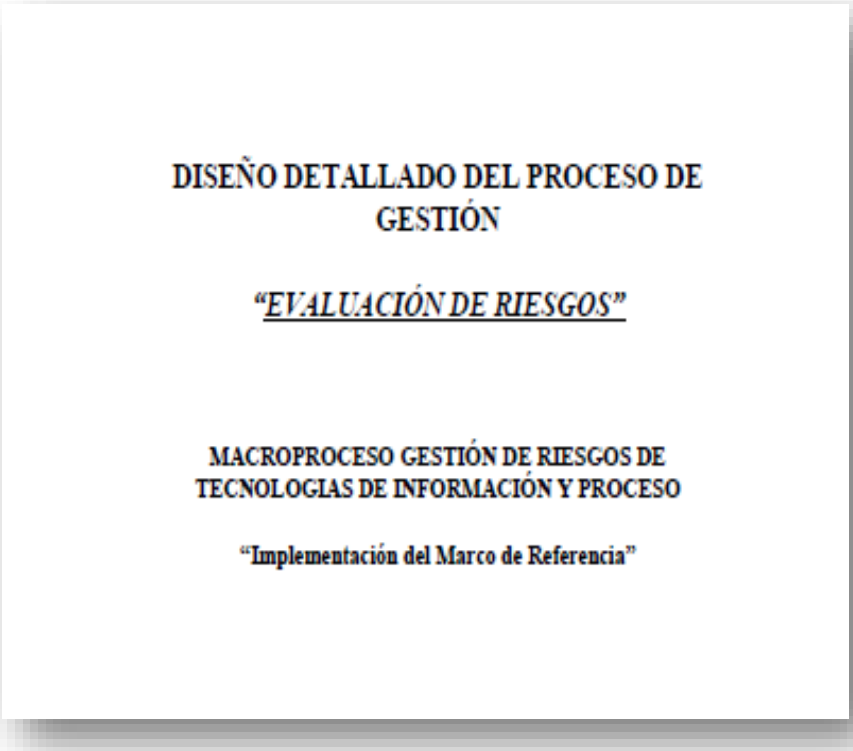


Figura 54. Portada del proceso de gestión "Evaluación de riesgos"

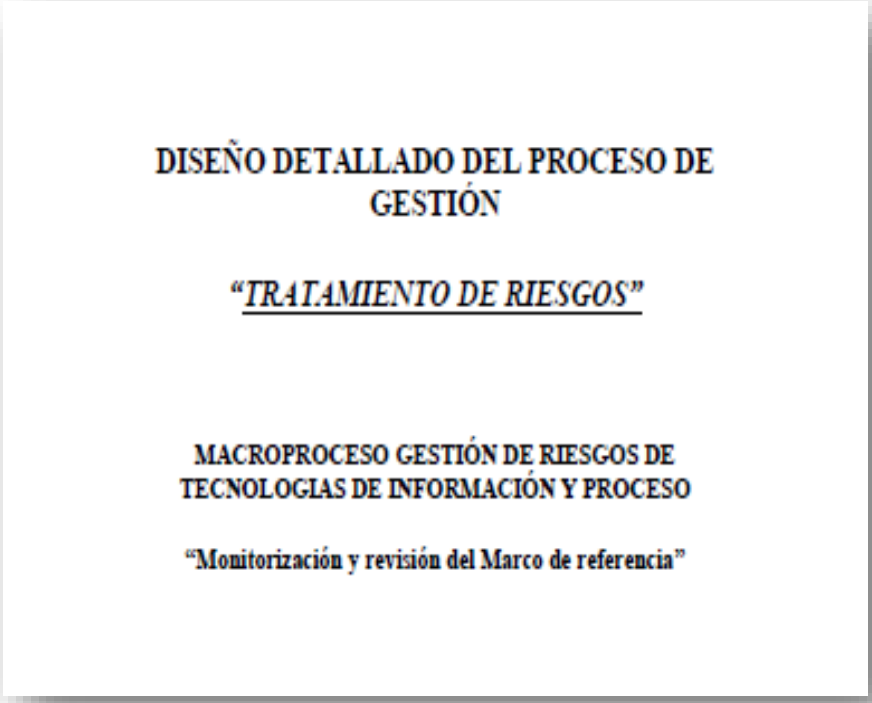


Figura 55. Portada del proceso de gestión " Tratamiento de riesgos"

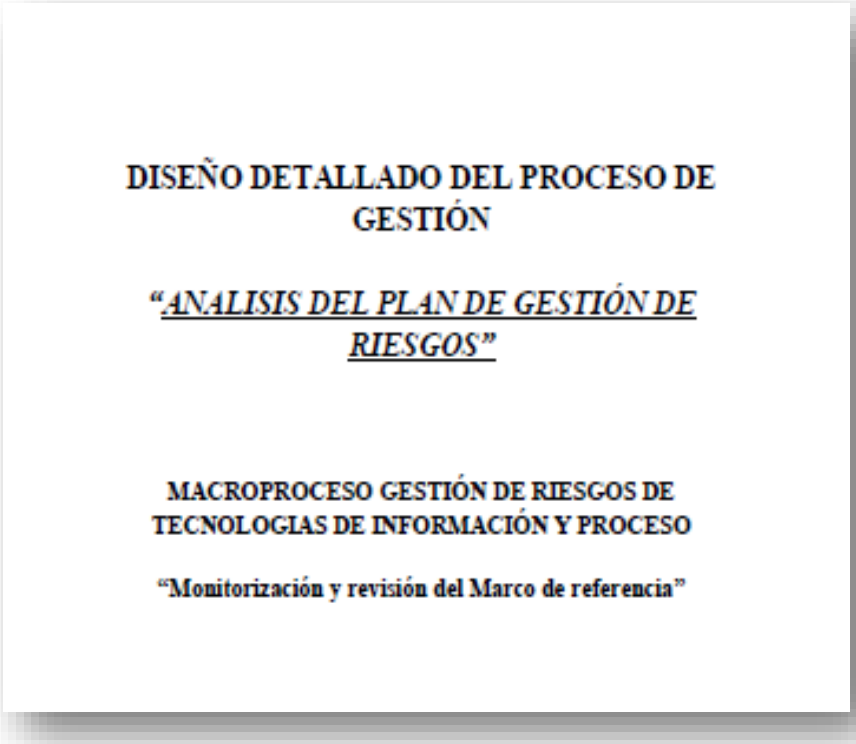


Figura 56. Portada del proceso de gestión "Análisis del plan gestión de riesgos"

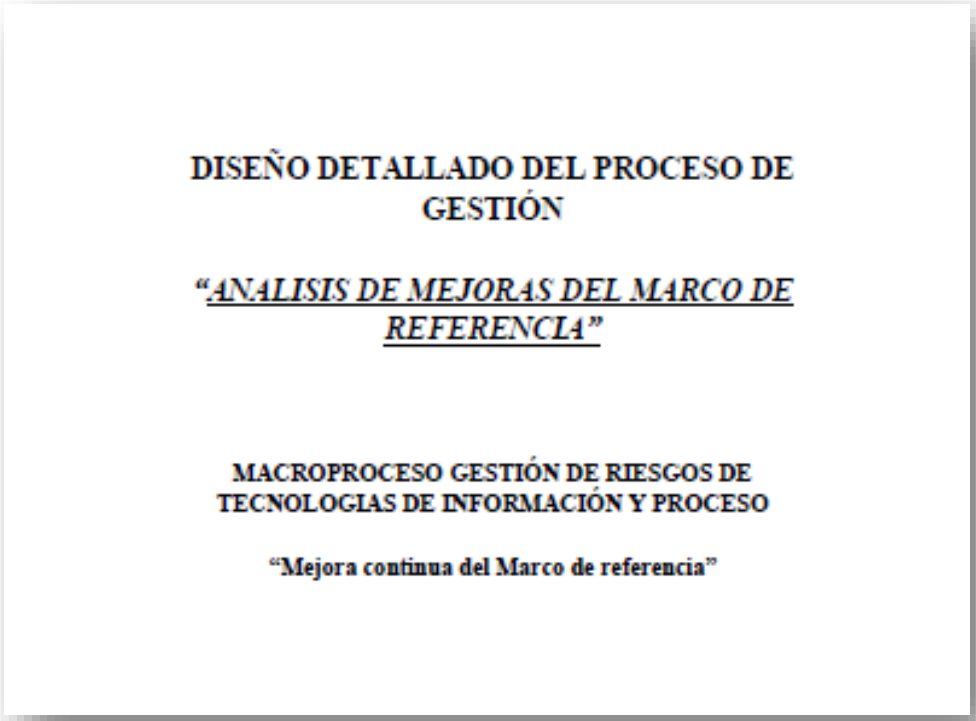


Figura 57. Portada del proceso de gestión "Análisis de mejoras del marco de referencia"

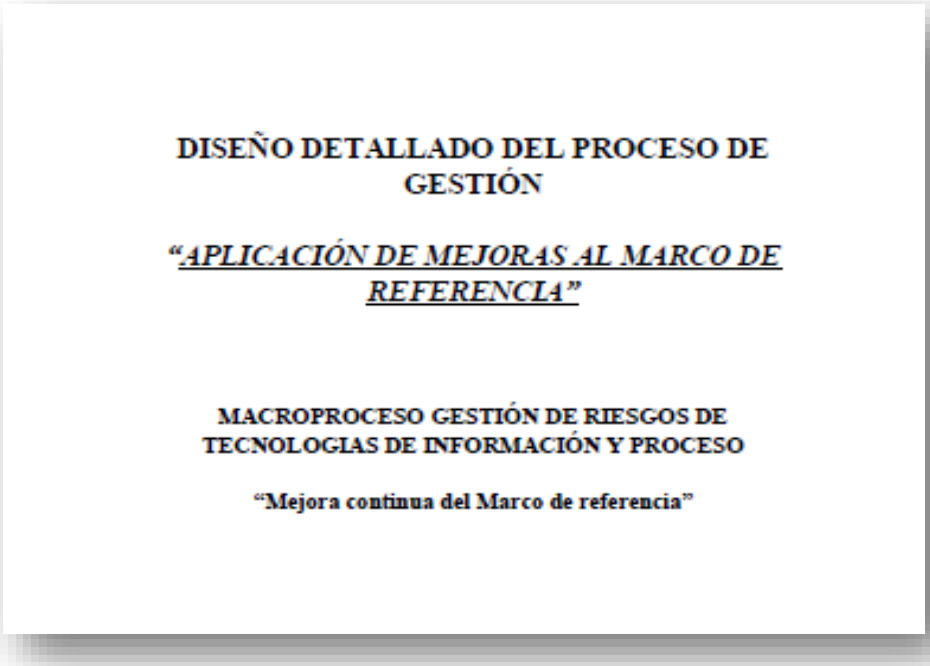


Figura 58. Portada del proceso de gestión "Aplicación de mejoras al marco de referencia"

6.4.4. APLICACIÓN DE PRUEBA A LA GUIA

La aplicación de pruebas estuvo encaminada ‘l acompañamiento de la construcción de la guía, como fue mencionado anteriormente, fue necesario realizar un nuevo trabajo, enfocado en la documentación de los procesos relacionados con el departamento de tecnologías de la información. En vista del tiempo de ejecución del proyecto, se pensó en seleccionar una línea de trabajo de dicho departamento para aplicar las pruebas, por ello se seleccionó la línea de trabajo “CONTINUIDAD DEL NEGOCIO” cuyo objetivo principal es: *“Garantizar el respaldo lógico y físico, periódico de los archivos y código fuente necesarios para el funcionamiento de sistemas críticos.”,* para iniciar la identificación de los procesos correspondientes se analizó la única documentación existente, esta consistía una tabla correspondiente a la línea de trabajo o área de gestión, donde se describían el objetivo principal y las responsabilidades fundamentales ejecutadas y vigiladas por dicha área.

ÁREA CLAVE DE GESTIÓN: CONTINUIDAD DE NEGOCIO	
OBJETIVO	RESPONSABILDAD
Garantizar el respaldo lógico y físico, periódico de los archivos y código fuente necesarios para el funcionamiento de sistemas críticos.	✓ **Realizar un plan de respaldo.** ✓ **Garantizar el resguardo y copia diario del código fuente y sus cambios.** ✓ **Garantizar el resguardo y copia histórica de código fuente de aplicaciones de misión crítica.** ✓ **Realizar prueba aleatorias de verificación de copias de respaldo.** ✓ **Informar y documentar el log de sucesos en el respaldo de la información.**

Tabla 13. Tabla de especificación de área clave de gestión "Continuidad de negocio"

Tratando de definir los procesos, se pensó en nombrarlos de una forma generalizada, de tal modo que permitiera omitir aspectos que para este nivel (definición de procesos) son

irrelevantes tales como el ¿cuándo?, ¿Dónde? Y ¿Por qué? de los procesos, pero que si serían descritos con detalle más adelante para labores de documentación del departamento.

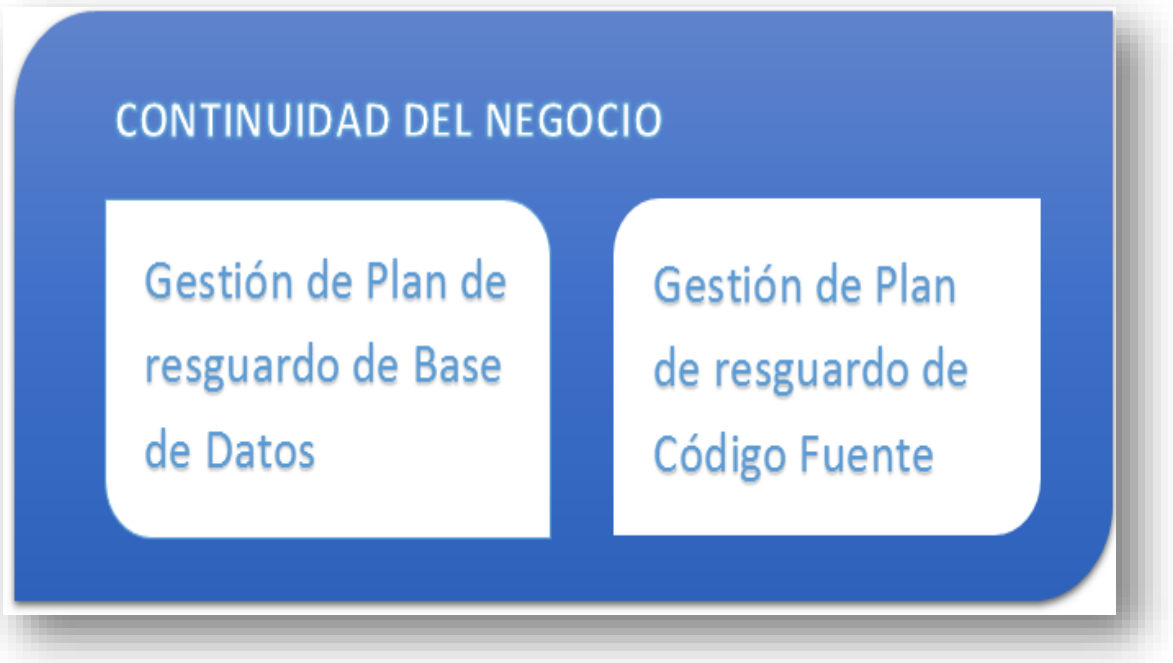


Figura 59. Procesos identificados y documentados del área de gestión "Continuidad de Negocio"

Descripción de Procesos:

1. **Gestionar plan de resguardo de Base de datos**: Bajo la ejecución de este proceso se haría y describiría todo lo relacionado con la continuidad del negocio desde la perspectiva de las bases de datos, es decir, todo lo requerido para que en caso que se presente un evento fortuito toda la información organizacional necesaria para una óptima ejecución de labores pueda ser retomada.

2. **Gestionar plan de resguardo del código fuente:** Bajo la ejecución de este proceso se haría y describiría todo lo relacionado con la continuidad del negocio desde la perspectiva del código fuente desarrollado y mantenido en la empresa, es decir, todo lo requerido para que en caso que se presente un evento fortuito todo lo requerido, necesario para una óptima ejecución de labores pueda ser retomado.

6.4.4.1. PLAN DE ACCIÓN

A pesar de las dificultades en la aplicación de la guía, ocasionadas por la falta de documentación pertinente, se diseñó un plan de acción a seguir, en el que se resaltas las principales actividades comprendidas por la guía, dicho plan será implementado en conjunto con la guía y sus respectivas planillas. Este plan incluye la ejecución de los procesos señalados como principales para la ejecución de este proyecto en el alcance del mismo:

PROCESO: Diseño del Marco de referencia

1. Establecimiento de mecanismos de consulta

1.1. Asignar el Personal a trabajar (Planilla de Asignación)

2. Establecimiento del contexto

2.1. Identificar procesos relacionados con TI (planilla de contexto Interno)

2.2. Describir procesos de contexto interno (Planilla – descripción de proceso)

PROCESO: Implementación del marco de referencia

1. Identificación de riesgos

1.1. Identificar los activos involucradas en los procesos (Planilla procesos-activos)

1.2. Realizar inventario de activos

1.3. Analizar los proceso, identificando sus riesgos (Planilla identificación riesgos-causas)

2. Análisis de riesgos

2.1. Calcular la probabilidad de ocurrencia (Tabla de probabilidad y Planilla de probabilidad)

2.2. Determinar el impacto en caso de ocurrencia (Tabla de impacto y Planilla de impacto)

2.3. Clasificar los riesgos (Planilla de Análisis de riesgos y Tabla de Zona de riesgo)

3. Evaluación de riesgos

3.1. Indexar los riesgos analizados (Planilla de categorización, llenando específicamente los campos correspondientes al “índice” y “descripción”.)

3.2. Categorizar los riesgos (Planilla de categorización, llenando específicamente el campo correspondiente “categoría”.)

3.3. Calcular la severidad de los riesgos absolutos (Planilla de severidad de riesgos absolutos).

7. RESULTADOS

A partir de los objetivos planteados al inicio de la ejecución del proyecto, se obtuvieron los siguientes resultados:

✓ La recopilación de un estado del arte con respecto a la temática que fue objeto de estudio en este proyecto, el cual estuvo conformado por:

- Estudio de antecedentes históricos que evidencian las graves consecuencias que acarrea la ausencia de modelos de gestión de riesgos tecnológicos en múltiples organizaciones.
- Compendio de Soluciones propuestas históricamente, para tratar con la gestión de riesgos tecnológicos, además, un conjunto de casos de estudios enmarcados en esta misma temática

✓ También se logró la construcción de un marco teórico que facilitó la comprensión de esta temática, en la que se destacaron normas y estándares ampliamente utilizados actualmente, estableció las bases teóricas y conceptuales para la ejecución de este proyecto, que en su mayoría son los conceptos emitidos por la norma ISO 31000, utilizada como el principal fundamento de este trabajo. Además, se describió las características principales de las herramientas utilizadas durante esta implementación, resaltando así sus principales atractivos.

✓ La definición de los procesos correspondientes a la gestión de riesgos de TI. Para ello se diseñó una cadena de valor en la que se destacan los procesos fundamentales, alineados directamente con las cuatro fases de la metodología PHVA, como son PLANEAR, HACER, VERIFICAR Y ACTUAR, seguido a esto, fueron definidos los procesos de gestión que se desprenden de los procesos principales, toda la definición de estos fue hecha con base en los conceptos y principios sugeridos por la norma ISO 31000, cumpliendo así con uno de los objetivos propuestos, como era la definición de procesos principales en el marco de la gestión de riesgos.

✓ Luego de definir los procesos correspondientes, se procedió a organizarlos y definirlos en orden secuencial, esto se hizo mediante la construcción de una guía metodológica, dando de este modo cumplimiento a los objetivos planteados previamente, para facilitar la comprensión e implementación de esta, se diseñaron diagramas de flujo

y planillas de trabajo, los diagramas de flujo fueron realizados únicamente para los proceso determinados como objeto de estudio en el alcance de este proyecto (*se hicieron otros, correspondientes a procesos relacionados directamente con estos* "sección 6.3"), que son los siguientes:

- Identificación de Riegos
- Análisis y Clasificación de Riesgos
- Evaluación de Riesgos

Y se diseñaron las siguientes planillas de trabajo, con el objetivo de ser apoyo a la ejecución de los procesos descritos en la guía:

- Planilla de asistencia
- Planilla de descripción de procesos
- Planilla de asignación de personal
- Planilla de contexto interno
- Planilla de identificación de activos en los procesos
- Planilla para identificación de causas de riesgos
- Planilla de probabilidad de ocurrencia de riesgos
- Planilla de Impacto de los riesgos
- Planilla de análisis de riesgos
- Planilla de categorización
- Planilla de Cálculo de Severidad de riesgos absolutos
- Tabla de Categorías
- Tabla de impactos
- Tabla de probabilidades
- Tabla de zona de riesgos
- Planilla de establecimiento de controles
- Planilla – Constancia de aplicación de controles
- Planilla de cálculo de severidad de riesgos controlados
- Planilla de verificación de mejora
- Planilla de solicitudes PQRS
- Planilla de indexación de solicitud PQRS
- Planilla de atención a solicitudes PQRS

✓ Finalmente como se tenía previsto, se socializó el modelo de la guía de evaluación de riesgos desarrollada, en la empresa local Corporación Plástica S.A.S – CORPLAS, logrando así enriquecer la información proporcionada a los usuarios en esta guía, a través de los comentarios y sugerencias del equipo de trabajo del departamento de tecnologías de la información de dicha empresa, quienes estuvieron involucrados en el desarrollo de este proyecto, gracias a este apoyo se logró realizar un mejor trabajo, cumpliendo de esta manera el objetivo general planteado.

8. CONCLUSIONES Y RECOMENDACIONES

8.1. CONCLUSIONES

A partir del crecimiento de estas tecnologías se ha hecho evidente una serie de causas de riesgos y amenazas que colocan en peligro la infraestructura de TI utilizada y por ende exponen a riesgos y problemas a quien las utilice, en este caso específico las organizaciones. Algunos de los riesgos que traen consigo las TI no se pueden evitar, ignorarlos o descuidarlos puede causar graves daños y/o pérdidas dentro de las organizaciones, debido a que estas tecnologías suelen soportar procesos de mucha importancia, que podrían salir gravemente afectados si ocurre algún fallo. Después del estudio de algunos antecedentes históricos en este campo, se notó lo grave que suelen ser las consecuencias, de la materialización de los riesgos a los que se encuentran expuestos las organizaciones en la actualidad, por ende se puede llegar a afirmar que es imprescindible para las organizaciones hacer una correcta y pertinente evaluación de todo tipo de riesgos, que le facilite controlar, asegurar sus activos informáticos, por ello es necesario plantear y desarrollar unos controles, que permitan tener todos estos riesgos vigilados y en constante monitoreo, esto puede ser corroborado con la siguiente idea: *"La gestión de los riesgos tecnológicos es importante dado que las organizaciones al usar tecnología en su actividad diaria y como parte de sus procesos de negocio se encuentran expuestas a este tipo de riesgos; por ello pueden afectar la actividad propia de las mismas y ser fuentes de pérdidas y daños considerables"*. (Ramírez & Ortiz, 2011)

También es notorio que existe una actitud hacia los riesgos sumamente reactiva, es decir, predomina en el medio un accionar defensivo. Se cree que el campo de acción de esta rama inicia cuando se ha descubierto un error o en el peor de los casos un desastre dentro de la organización, en este momento es cuando se intenta desplegar una lista de mecanismos para solventar las fallas y devolver la estabilidad organizacional, en algunos casos estos mecanismos cumplirán con su objetivo, sacrificando recursos valiosos, como tiempo y dinero, y entre otras cosas, afectará factores de calidad como la fiabilidad de la organización aun cuando ya se haya solucionado el inconveniente. A través de la presente investigación, se identificó que las distintas etapas de un buen modelo de gestión de riesgos, constituyen un ciclo estructurado, que se enfoca más en evitar que se materialicen

los riesgos que en corregir las consecuencias que estos acarrean, por esta razón, con la realización de este proyecto se demuestra que es posible tratar los riesgos, entendiéndose por esto, la identificación, análisis, evaluación y la creación de políticas para mitigarlos.

En otras ocasiones dichos riesgos no son tratados de forma correcta, a causa del desconocimiento que predomina en la forma de implementar la información que existe concerniente al tema, y esto conlleva a una gestión deficiente de los riesgos, lo cual puede afectar directamente sobre las metas y objetivos organizacionales, debido a la estrecha relación que existe entre las TI y los procesos de negocio organizacionales; además, los posibles fallos también pueden afectar la buena imagen y reputación de la organización (Ramírez & Ortiz, 2011), con base en esta situación, el presente proyecto, obtuvo como resultado un conjunto de procesos y actividades que sugieren un orden especifico de estas y que facilitan la gestión de riesgos, demostrando así, que el orden de los procesos y actividades en los tiempos adecuados garantizan no solo una buena gestión de riesgos, sino que impulsan el buen clima organizacional, puesto que la metodología propuesta involucra de forma general todos los departamentos inmersos en una organización.

A pesar de que existe abundante información relacionada con estándares nacionales e internacionales, normas y metodologías, que si bien es cierto, es de buena calidad, no existía una guía que no solo ofreciera buenos conceptos y buenas prácticas para implementar, sino que mostrara la senda, paso a paso, para lograr una correcta gestión de riesgos, y de esta forma colaborar con las empresas. Con la ejecución de este proyecto, no solo se logró construir dicha guía, sino que se logró afirmar la idea de que, gestionar los riesgos no es tarea de la gerencia, o de uno pocos, es más bien una labor que exige compromiso de todos y de ser ejecutada con responsabilidad traerá los resultados esperados.

En este sentido, la construcción de esta guía metodológica propuesta como solución en el presente proyecto, estuvo marcada por investigaciones amplias que además de confirmar la importancia de la gestión de riesgos tecnológicos, mostró en su estado del arte las graves consecuencias afrontadas por algunos antes de prestar la atención necesaria a estos tipos de procesos.

El trabajo realizado fue una experiencia realmente enriquecedora, no sólo a nivel académico sino personal; los miembros del equipo se integraron para realizar tareas de recolección de información, análisis de la misma, comprensión y aplicación de teorías correspondientes a la gestión de riesgos, especialmente la ofrecida por la norma ISO 31000, entre otros, que permitieron el intercambio de conocimientos, destrezas y valores humanos, además del fortalecimiento del nivel intelectual, al entrar en contacto con empresas, para las que trabajos como este, son realmente importante y útiles.

El producto final conseguido constituye una guía metodológica que describe procesos y actividades a ejecutar en la gestión de riesgos de tecnologías de la información. Acompañada de los conceptos ofrecidos por la norma base, y las demás herramientas desarrolladas (diagramas de flujos, planillas, tablas, etc.) para facilitar su aplicación.

Para concluir, *"La gestión del riesgo se puede aplicar a toda la organización, en todas sus áreas y niveles, en cualquier momento, así como a funciones, proyectos y actividades específicos."*.

8.2 RECOMENDACIONES

Tomando como precedente los resultados planteados, se recomienda seguir trabajando en la definición completa del Macroproceso GESTION DE RIESGOS DE TI, Lo que implica realizar una descripción más concreta de los proceso MONITORIZACIÓN Y REVISION DEL MARCO DE REFERENCIA y MEJORA CONTINUA DEL MARCO DE REFERENCIA y sus respectivos procesos de gestión, dado que esta investigación se centró principalmente en los proceso de DISEÑO DE MARCO DE REFERENCIA PARA LA GESTION DE RIESGOS e IMPLEMENTACIÓN DEL MARCO DE REFERENCIA, tal como se expresó en el alcance. Las bases teóricas adelantadas en el proyecto, pueden agilizar su implementación.

Igualmente, se recomienda el estudio cabal de la norma internacional ISO 31000 y la metodología PHVA, puesto que en algún momento, de acuerdo al contexto de aplicación

de esta guía, el marco de referencia o cualquier otro aspecto requiera un cambio o una mejora.

La utilización e implementación de la guía desarrollada requieren tiempo y dedicación, por lo que se sugiere asignar a una persona con conocimientos en principios básicos de auditoria y tecnología de la información para que figure como líder de dicha implementación.

Como se mencionó anteriormente, la guía diseñada contiene herramientas básicas como tablas, planillas etc., que no fueron diseñadas para forzar su uso a quien implemente la metodología que expone la guía, sino para efectos de ilustración, es decir, que el uso de estas, será a criterio del usuario.

REFERENCIAS BIBLIOGRÁFICAS

(REFERENCIA DE REVISTA PERSPECTIVAS MICROSOFT NO. 13, 2004 recuperado de: http://www.microsoft.com/spain/enterprise/perspectivas/numero_13/estrategia.mspx

AXWLOA. (2011). ITIL, continual service improvement. Norwich, UK: TSO

CASTRO, M. (s.f). El Nuevo Estándar ISO para la Gestión del Riesgo.

CERT (Software Engineering Institute, Carnegie Mellon University). (2008). Octave. Retrieved from http://www.cert.org/octave/

DISTERER, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management.

FERNÁNDEZ, M. A. (2003). *Nuevo Marco COSO de gestión de riesgos.* En: Boletín de la comisión de normas y asuntos profesionales del instituto de auditores internos de argentina. No. 9

FREITAS, V. D. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Caracas, Venezuela

GAITÁN, R. E. (2006). *Administración de riesgos ERM y la auditoría interna*. Ecoe Ediciones.

GALLO MACHADO, G. (17 de febrero de 2011). Volvió a fallar la red Bancolombia. *El Colombiano*.

GUERRERO, J. M. L., & GÓMEZ, F. L. C. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información.

ISACA Issues COBIT 5 Governance Framework (2012) recuperado de: *http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Issues-COBIT-5-Governance-Framework.aspx*

ISACA (2013). The RISK IT Framework [online]. recuperado de: http://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/TheRisk-IT-Framework.aspx

ISO (International Standard Organization). (2005). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Estándar de Seguridad ISO/IEC 27001

ISO (International Standard Organization). (2011). Gestión del riesgo – Principios directrices. Estándar de Seguridad ISO 31000.

ISO (International Organization forStandardization) .,& International Electrotechnical Commission [IEC]. (2011a). ISO/IEC 27005: gestión de riesgos de seguridad de la Información. Geneve, Swizerland: ISO

ISO (International Organization forStandardization) .,& International Electrotechnical Commission [IEC].. (2011b). Risk management — Risk assessment techniques [IEC/FDIS 31010]. Retrieved from http://www.previ.be/pdf/31010_FDIS. Pdf

ITU. (2012). *La UIT publica las cifras más recientes sobre desarrollo de tecnologías a escala mundial*. 2012, de Unión Internacional de Telecomunicaciones: http://www.itu.int/net/pressoffice/press_releases/2012/70-es.aspx#.VNrIzvmG-R.

LAVELL, A. (2001). Sobre la gestión del riesgo: apuntes hacia una definición. *Scripta Nova–Revista*.

LEITCH, M.(2010). ISO 31000: 2009—The new international standard on risk management. *Risk Analysis*, 30(6), 887-892.

MAXITANA, C. J. D., & NARANJO, S. B. A. (2005). Administración de riesgos de tecnología de información de una empresa del sector informático.

MEDINA, L. C. F., GIRALDO, O. L., & HERRERA, A. (2010). Guía de buenas prácticas en gestión de riesgos de TI en el sector bancario colombiano.

MHAP (Ministerio de Hacienda y Administraciones Públicas). (2012). MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de

MINTIC. (2013). *Gestión TI: Nacional*. 2015, de Ministerio de TIC: http://estrategiaticolombia.co/estadisticas/stats.php?s=7

POSADA, E. (2004, Diciembre). *Ciencia, Tecnología y Desarrollo*. Revista De La Información Básica.

PURDY, G. (2010). ISO 31000: 2009—setting a new standard for risk management. Risk analysis, 30(6), 881-886.

QUINTERO, F. J. E (2011). Gestión de riesgos de TI: Factor Clave para el logro de los objetivos del negocio.

RAMÍREZ, A., ORTIZ, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. En: Ingeniería, Vol. 16, No. 2, pág. 56-66.

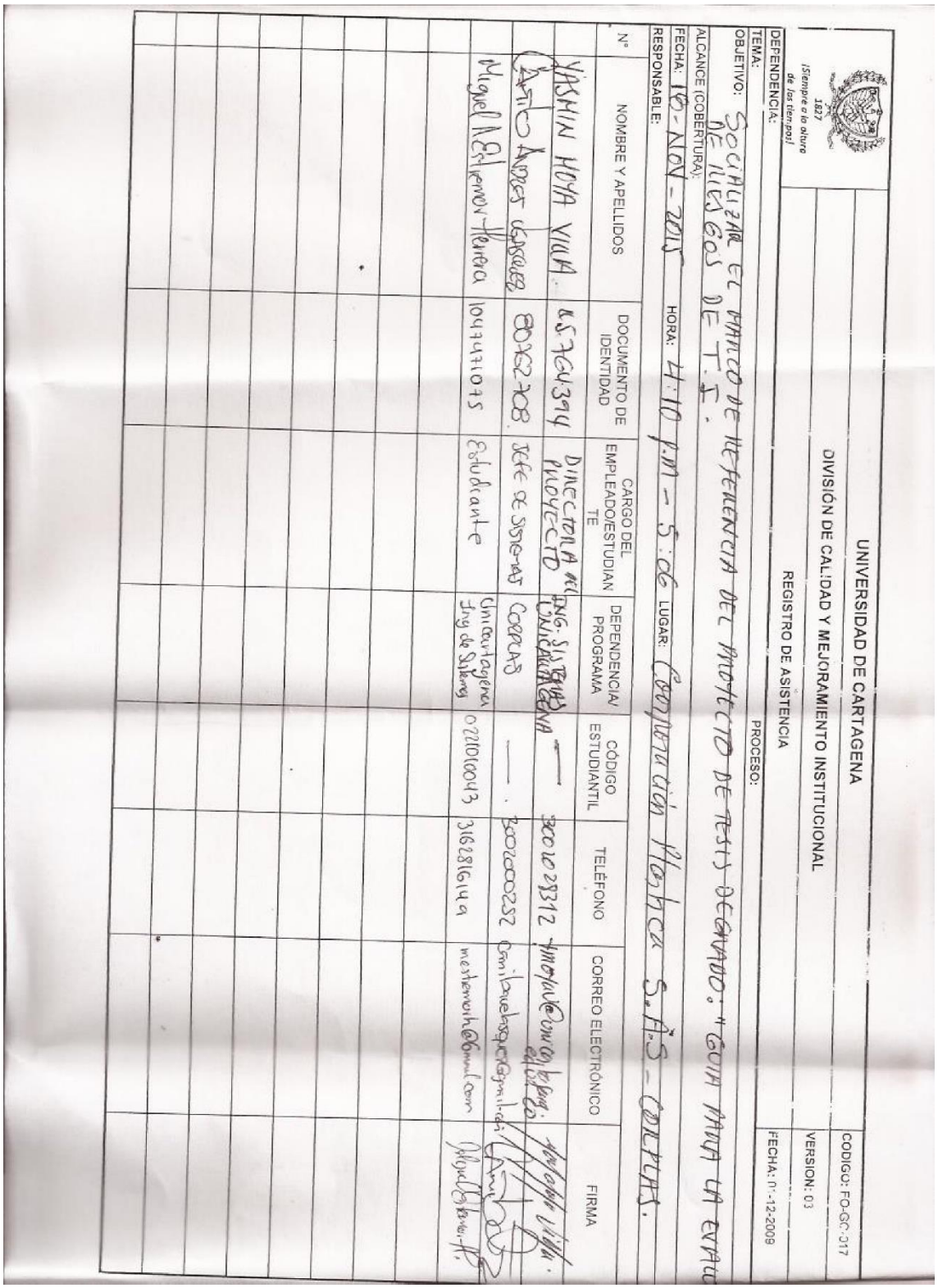
SLOSSE, C. A. (2013). Auditoría. Editorial de la Universidad Nacional de La Plata (EDULP).

WESTERMAN, G., & HUNTER, R. (2007). IT risk: turning business threats into competitive advantage. Cambridge: Harvard Business School Press.

ANEXOS

ANEXOS No. 1.

Registros de Asistencias de Entrevistas realizada en la empresa Corporación Plástica S.A.S – CORPLAS.



UNIVERSIDAD DE CARTAGENA
DIVISIÓN DE CALIDAD Y MEJORAMIENTO INSTITUCIONAL
REGISTRO DE ASISTENCIA
CODIGO: FO-GC-017
VERSION: 03
FECHA: 01-12-2009
DEPENDENCIA:
PROCESO:
TEMA:
OBJETIVO: Socializar el marco de referencia del proyecto de tesis de grado: "Guía para un estudio de ilusiones de T.I."
ALCANCE (COBERTURA):
FECHA: 10-NOV-2015 HORA: 4:10 p.m - 5:00 LUGAR: Corporación Plástica S.A.S - CORPLAS.
RESPONSABLE:

N°	NOMBRE Y APELLIDOS	DOCUMENTO DE IDENTIDAD	CARGO DEL EMPLEADO/ESTUDIANTE	DEPENDENCIA/ PROGRAMA	CÓDIGO ESTUDIANTIL	TELÉFONO	CORREO ELECTRÓNICO	FIRMA
	YASMIN HOYA VILLA	45764394	DIRECTORA DE PROYECTO	ING. SISTEMAS UNICARTAGENA	—	3001283112	yhoyav@unicartagena.edu.co	
	Carlos Andres Gonzalez	80062708	Jefe de Sistemas	Corplas	—	3003000252	carlosandresgonzalez@hotmail.com	
	Miguel Melendez Herrera	1047431045	Estudiante	Unicartagena Ing de Sistemas	0221010043	3162816149	miguelmelendez@gmail.com	

	UNIVERSIDAD DE CARTAGENA	CODIGO: FO-GC-017
1827 ¡Siempre a la altura de los tiempos!	DIVISIÓN DE CALIDAD Y MEJORAMIENTO INSTITUCIONAL	VERSION: 03
	REGISTRO DE ASISTENCIA	FECHA: 0[illegible]-12-2009

DEPENDENCIA:

TEMA: PROCESO:

OBJETIVO: Conocer la percepción de riesgos tecnológicos del departamento de TI.

ALCANCE (COBERTURA):

FECHA: 04/03/2016 HORA: 10:00 - 11:30 AM LUGAR: Corporación plastica S.A.S - Corplas

RESPONSABLE:

N°	NOMBRE Y APELLIDOS	DOCUMENTO DE IDENTIDAD	CARGO DEL EMPLEADO/ESTUDIANTE	DEPENDENCIA/ PROGRAMA	CÓDIGO ESTUDIANTIL	TELÉFONO	CORREO ELECTRÓNICO	FIRMA
	Miguel Angel Estremor	1047471075	Estudiante	UDC	0211010043	3162816149	mestremorh@gmail.com	
	Carlos Andres Vasquez	80762708	JEFE DE SISTEMAS	CORPLAS	X	3002000252	carlosvasquez@gmail.com	

	UNIVERSIDAD DE CARTAGENA	CODIGO: FO-GC-017
1827 ¡Siempre a la altura de los tiempos!	DIVISIÓN DE CALIDAD Y MEJORAMIENTO INSTITUCIONAL	VERSION: 03
	REGISTRO DE ASISTENCIA	FECHA: 01-12-2009

DEPENDENCIA: PROCESO:

TEMA:

OBJETIVO: Socializar Contexto actual del departamento de TI, en materia de documentación interna.

ALCANCE (COBERTURA):

FECHA: 22/04/16 HORA: 04:00 - 5:45 PM LUGAR: Corporación platica SAS - Corplas

RESPONSABLE:

N°	NOMBRE Y APELLIDOS	DOCUMENTO DE IDENTIDAD	CARGO DEL EMPLEADO/ESTUDIANTE	DEPENDENCIA/ PROGRAMA	CÓDIGO ESTUDIANTIL	TELÉFONO	CORREO ELECTRÓNICO	FIRMA
	Carlos Andres Casseres	80752708	JEFE DE SISTEMAS	CORPLAS	—	3002000252	carlosandrescasseres@gmail.com	
	Miguel Angel Estevez H	1047471075	Estudiante	U de C	0221010043	3162816149	meithaven@gmail.com	

ANEXO No. 2.

Constancia expedida por la empresa Corporación Plástica S.A.S – CORPLAS, como garante de la socialización del marco de referencia propuesto.

Corplas

Cartagena de Indias D.T. y C. 18 de noviembre de 2015

Señores:
COMITE DE INVESTIGACIÓN Y PROYECTOS DE GRADO
Programa de Ingeniería de sistemas
UNIVERSIDAD DE CARTAGENA

Ref. Constancia de Socialización

Por medio de la presente, se hace constar que se llevó a cabo la socialización del marco de referencia diseñado para el desarrollo del proyecto de investigación denominado: **GUIA PARA LA EJECUCIÓN DE PROCESOS DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS EN TECNOLOGIAS DE INFORMACION USANDO LA NORMA ISO 31000**, desarrollado por el estudiante: Miguel Ángel Estremor Herrera y dirigido por la ingeniera Yasmin Moya Villa.

Como resultado de dicha socialización, se hicieron las siguientes sugerencias, para el diseño y construcción de la guía:

- Incluir tablas de entradas y salidas que faciliten la comprensión y ejecución de los procesos descritos.
- Incluir en la guía diagramas de flujos convencionales para indicar el orden de flujo de las actividades a ejecutar en cada proceso de gestión.
- Anexar conjuntos de planillas para ilustrar los procesos.
- Añadir a las tablas de zona de riesgo y gestión del mismo, colores tradicionales para dar a entender con mayor facilidad el estado actual de los riesgos.

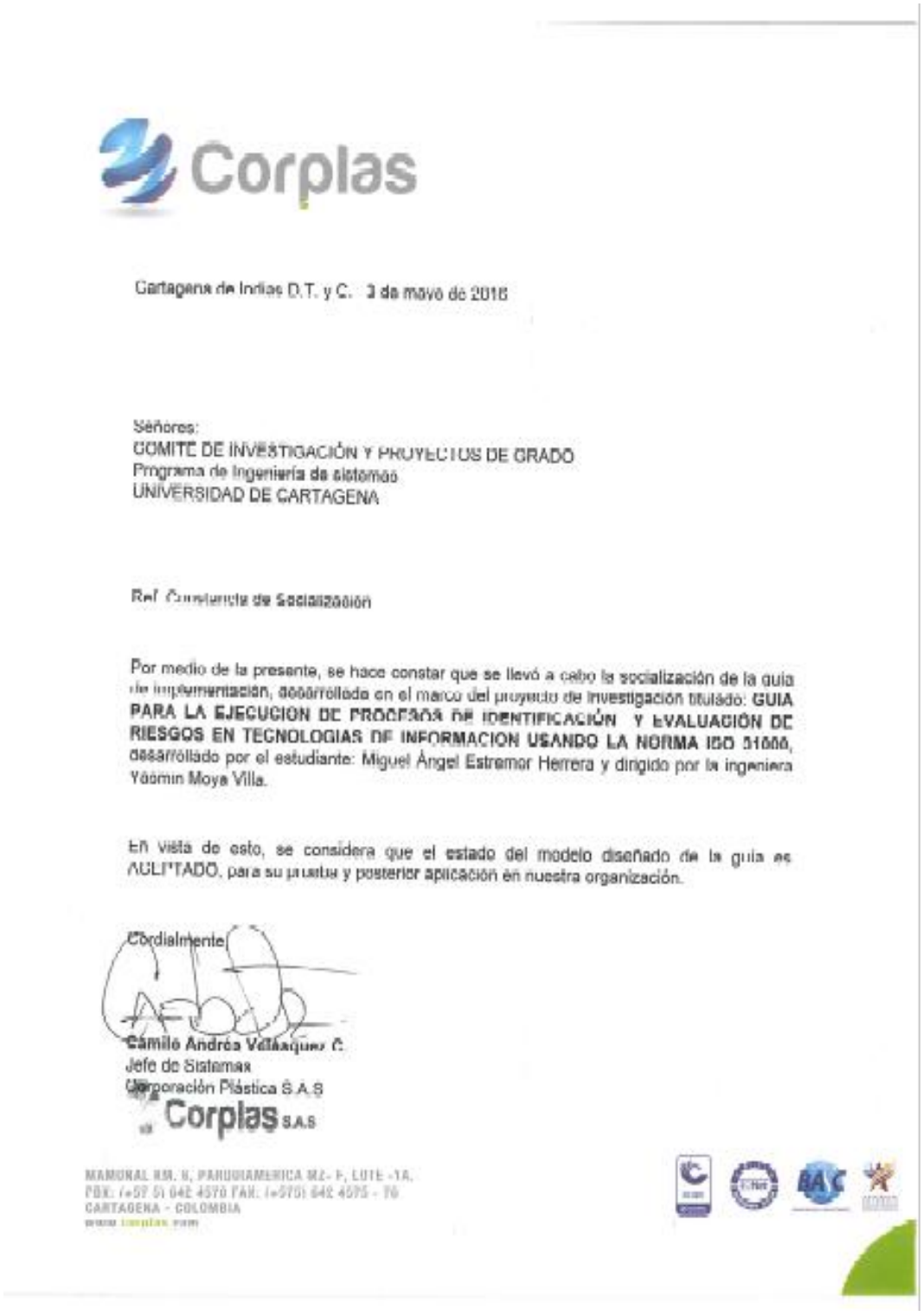
Cordialmente,

Camilo Andrés Velásquez G.
Jefe de Sistemas
Corporación Plástica S.A.S

MAMONAL KM. 6, PARQUEMERICA MZ- P, LOTE -18.
PBX: (+57 5) 642 1670 FAX: (+575) 642 1676 - 78
CARTAGENA - COLOMBIA
www.corplas.com

ANEXO No. 3.

Constancia expedida por la empresa Corporación Plástica S.A.S – CORPLAS, como garante de la socialización de la guía desarrollada.



Corplas

Cartagena de Indias D.T. y C. 3 de mayo de 2016

Señores:
COMITE DE INVESTIGACIÓN Y PROYECTOS DE GRADO
Programa de Ingeniería de sistemas
UNIVERSIDAD DE CARTAGENA

Ref Constancia de Socialización

Por medio de la presente, se hace constar que se llevó a cabo la socialización de la guía de implementación, desarrollada en el marco del proyecto de investigación titulado: **GUIA PARA LA EJECUCION DE PROCESOS DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS EN TECNOLOGIAS DE INFORMACION USANDO LA NORMA ISO 31000**, desarrollado por el estudiante: Miguel Ángel Estramor Herrera y dirigido por la ingeniera Yasmin Moya Villa.

En vista de esto, se considera que el estado del modelo diseñado de la guía es ACEPTADO, para su prueba y posterior aplicación en nuestra organización.

Cordialmente,

Camilo Andrés Velásquez C.
Jefe de Sistemas
Corporación Plástica S.A.S
Corplas S.A.S

MANUAL KM. 8, PARQUIAMERICA MZ- F, LOTE -1A,
PBX: (+57 5) 642 4570 FAX: (+575) 642 4575 - 76
CARTAGENA - COLOMBIA
www.corplas.com

ANEXO No. 4.

Constancia expedida por la empresa Corporación Plástica S.A.S – CORPLAS, como garante de la realización de pruebas y trabajo en conjunto con la empresa.

Corplas

Señores:
COMITÉ DE INVESTIGACIÓN Y PROYECTOS DE GRADO
Programa de Ingeniería de sistemas
UNIVERSIDAD DE CARTAGENA

Ref. Constancia de Realización de Pruebas en el marco del proyecto de investigación titulado: **GUIA PARA LA EJECUCION DE PROCESOS DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS EN TECNOLOGIAS DE INFORMACION USANDO LA NORMA ISO 31000.**

Por medio de la presente, se hace constar que se llevó a cabo el proceso de aplicación de la **GUIA PARA LA EJECUCION DE PROCESOS DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS EN TECNOLOGIAS DE INFORMACION USANDO LA NORMA ISO 31000.**

Las pruebas a la Guía fueron realizadas en el Departamento de "Tecnologías de Información" de nuestra empresa, en la línea de "Continuidad del Negocio". Como resultado de la aplicación de la Guía, se realizó la definición de los procesos correspondientes a dicho departamento

Cabe resaltar la importancia del desarrollo de este tipo de proyectos, los cuales fortalecen las relaciones de la Universidad con el sector productivo y acercan al estudiante y futuro profesional a la realidad del campo laboral.

Camilo Andrés Velásquez C.
Jefe de Sistemas
Corporación Plástica S.A.S
Corplas S.A.S

MAMONAL KM. 6, PARQUEAMERICA MZ- P, LOTE -1A.
PBX: (+57 5) 642 4670 FAX: (+575) 642 4675 76
CARTAGENA - COLOMBIA
www.corplas.com