RESUMEN – TRABAJO DE GRADO

AUTORES	**Erika Tatiana Quintero Quintero** **Sandra Liliana Ascanio Suarez** **Yuraima Karina Cardenas Estupiñan**
FACULTAD	**Ingenierías**
PLAN DE ESTUDIOS	**Especialización en Auditoria de Sistemas.**
DIRECTOR	**Lorencita Rodríguez Galezo**
TÍTULO DE LA TESIS	**Guía de Gestión de Riesgos para el Departamento de Sistemas de La Empresa Apuestas Cúcuta 75.**

RESUMEN
(70 palabras aproximadamente)

LA PRESENTE INVESTIGACIÓN PROPONE UNA GUIA PARA LA GESTIÓN DE RIESGOS PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA APUESTAS CUCUTA 75; SE SUSTENTA EN EL MARCO DE TRABAJO DE LAS NORMAS AS/NZS 4360:1999, NTC-ISO 31000:2011 Y LA GUIA GTC 137, TENIENDO EN CUENTA, QUE LA PRESENTE PROPUESTA ESTABLECE LOS ELEMENTOS Y EL MARCO GENERAL DE ACTUACIÓN PARA LA GESTIÓN INTEGRAL DE LOS RIESGOS DE TODA NATURALEZA A LOS QUE SE ENFRENTA EL ÁREA DE SISTEMAS.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:
133	0	0	1

GUÍA DE GESTIÓN DE RIESGOS PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA APUESTAS CÚCUTA 75

SANDRA LILIANA ASCANIO SANCHEZ
YURAIMA KARINA CARDENAS ESTUPIÑAN
ERIKA TATIANA QUINTERO QUINTERO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2015

GUÍA DE GESTIÓN DE RIESGOS PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA APUESTAS CÚCUTA 75

SANDRA LILIANA ASCANIO SANCHEZ
YURAIMA KARINA CARDENAS ESTUPIÑAN
ERIKA TATIANA QUINTERO QUINTERO

Proyecto presentado como requisito para opta al título de
Especialista en Auditoria de Sistemas

Director
LORENCITA RODRIGUEZ GALEZO
MSC(C) Ingeniería de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2015

AGRADECIMIENTOS

Primero que todo a Dios, por su infinita sabiduría y hacer posible este logro.

A la directora del proyecto MSC. Lorencita Rodríguez Galezo por su motivación, dedicación, esfuerzo y buenas recomendaciones en el desarrollo del proyecto.

A todos los docentes por su aporte a nuestra formación profesional durante el proceso de la especialización.

CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

Los riesgos son un tema de importante análisis, actualmente en las empresas o corporaciones poseen un gran impacto, especialmente sobre objetivos organizacionales. Por esta razón, es vital establecer la gestión de riesgos ya que permite identificar posibles acontecimientos, cuya materialización afecta el logro de los objetivos y la aplicación de medidas reducirá la probabilidad o el impacto de estas eventualidades.

El objetivo de este proyecto es diseñar una guía para gestionar los riesgos de cualquier nivel o ámbito de aplicación (estratégico, tecnológico, operativo, financiero o de cumplimiento) del departamento de sistemas de la empresa Apuestas Cúcuta 75, pudiéndose aplicar también a un rango de actividades incluyendo estrategias, decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

El enfoque de este documento se desarrolló mediante una investigación previa y basada en el estándar ISO 31000:2011, Gestión del Riesgo – Principios y directrices, el estándar Australiano AS/NZS 4360:1999 y la guía GTC 137, la cual suministra las definiciones de términos genéricos relacionados con la gestión del riesgo.

Basados en estos estándares de administración y/o gestión del riesgo se realizaron investigaciones sobre metodologías para gestionar los principios que proponen estas normas, para posteriormente estructurar la guía de gestión para el departamento de sistemas de Apuestas Cúcuta 75, que tiene como finalidad establecer los elementos y el marco general de actuación para la gestión integral de los riesgos de toda naturaleza a los que se enfrenta el área de sistemas.

La norma ISO 31000:2011, el estándar Australiano AS/NZS 4360:1999 y la guía GTC 137 proporcionan las directrices para gestionar riesgos permitiendo a las organizaciones lograr sus objetivos y reducir costos y riesgos. La ISO 31000:2011 establece cinco procesos para la gestión del riesgo: comunicación y consulta, establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, monitoreo y revisión; la AS/NZS 4360:1999 involucra el establecimiento del contexto, y a diferencia de la ISO 31001:2011 subdivide el proceso de valoración en: identificación, análisis y evaluación, también incluye el tratamiento, y por ultimo efectúa el proceso de comunicación y el monitoreo de los riesgos. Por último la GTC 137 suministra las definiciones de términos con el objetivo de fomentar un entendimiento mutuo y el uso de terminología de gestión de riesgo uniforme.

1. TITULO

Guía de gestión de riesgos para el departamento de sistemas de la empresa apuestas Cúcuta 75.

1.1 PLANTEAMIENTO DEL PROBLEMA

Apuestas Cúcuta 75 es una empresa que se dedica a la comercialización de apuestas permanentes chance en el departamento de Norte de Santander, que tras casi cuarenta años de historia ha mostrado no solo ser una de las organizaciones que más genera empleo en la región, sino ser pionera en avances tecnológicos y comerciales. La relación de esta organización con los sistemas y las tecnologías, presenta una serie de riesgos que comprometen la continuidad de las operaciones, afectando sus objetivos e imagen.

El departamento de sistemas de Apuestas Cúcuta 75 representa la operatividad del negocio, pues tiene la capacidad de innovar ante cualquier requerimiento, proponiendo soluciones tecnológicas que aportan a la transformación de la compañía y al manejo de la información. Dentro del departamento, existen posibles riesgos como el robo, pérdida o alteración de datos, fallas en dispositivos, copias de seguridad desactualizadas, accesos no autorizados, sabotajes, entre otros posibles eventos. Problemática que puede generar un alto impacto económico en la organización, así como su imagen ante los clientes y partes interesadas, además que podría incumplir con las leyes que buscan la protección de la información de los clientes.

El departamento de sistemas está permanentemente expuesto a riesgos que pueden afectar el cumplimiento de los objetivos misionales y comprometer la continuidad de sus operaciones. En este aspecto, se refleja la ausencia de un documento oficial donde se detallen las estrategias de mitigación implementadas o de aplicación para gestionar los riesgos, impidiendo visualizar con claridad la labor de seguridad que efectúa el departamento de sistemas en beneficio de Apuestas Cúcuta 75.

1.2 FORMULACIÓN DEL PROBLEMA

¿Una guía de gestión de riesgos permitirá al departamento de sistemas de apuestas Cúcuta 75 la identificación, valoración y tratamiento de riesgos de manera efectiva y eficiente?

1.3 OBJETIVOS

1.3.1 Objetivo general. Diseñar una guía de gestión de riesgos para el departamento de sistemas de la empresa Apuestas Cúcuta 75.

1.3.2 Objetivos específicos. Realizar un diagnóstico del departamento de sistemas de la empresa Apuestas Cúcuta 75, para establecer el contexto e identificar, valorar y tratar los riesgos.

Identificar los estándares para el diseño de una guía de gestión y/o administración de riesgos para el departamento de sistemas de la empresa Apuestas Cúcuta 75, para minimizar las posibles amenazas.

Elaborar un documento que guie la gestión del riesgo, según la información recolectada en el departamento de sistemas de la empresa Apuestas Cúcuta 75.

Socializar la guía de gestión de riesgos al personal del departamento de sistemas de la empresa Apuestas Cúcuta 75.

1.4 JUSTIFICACIÓN

La gestión del riesgo como parte integral de las buenas prácticas es un proceso interactivo que consta de varios elementos, cuyo objetivo es permitir que la organización minimice pérdidas y maximice oportunidades, estableciendo mecanismos que permitan identificar, analizar, evaluar y dar tratamiento a los riesgos a los que se encuentran expuestos, para así alcanzar la eficiencia y eficacia organizacional. Según Alter Wriston (Ex presidente de Citicorp) "todo en la vida es la administración del riesgo, no su eliminación".

Las empresas actualmente enfrentan una creciente exposición a los riesgos informáticos y diversos estudios declaran que cada segundo son creados tres virus en el mundo y que Latinoamérica es una de las zonas más afectadas, pues los ataques cibernéticos quedan impunes, dejando claro que esta clase de riesgos generan pérdidas mayores a los costos de la implementación de controles de prevención o reducción de su impacto.

Por lo tanto, es importante establecer la gestión de riesgos como una herramienta fundamental en las organizaciones, pues permite que sus áreas de tecnologías eviten, mitiguen, transfieran o acepten los riesgos que se presenten. La evaluación involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo

establecidos previamente. (…) Si los riesgos resultantes caen dentro de las categorías de bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables[1].

A nivel empresarial, la gestión de riesgos brinda seguridad en términos de prevención, conocimiento de activos, medios de protección y reducción de costos; en Apuestas Cúcuta 75 esta gestión permitirá detectar fallas con anterioridad, logrando así fortalecer estrategias de trabajo, rendimiento laboral y mayores ventajas competitivas.

1.5 HIPÓTESIS

El diseño de una guía de gestión de riesgos, proporcionará resultados eficientes para el departamento de sistemas de la empresa apuestas Cúcuta 75, permitiendo minimizar la probabilidad de ocurrencia y el impacto económico.

1.6 ALCANCE Y DELIMITACIONES

1.6.1 Alcance. La guía de gestión de riesgos se enfocará en el departamento de sistemas de la empresa Apuestas Cúcuta 75.

Esta se desarrollará apoyada en estándares de riesgos como la AS/NZS 4360:1999, la NTC-ISO 31000 y la guía GTC 137; el proceso para la gestión de riesgos, se fundamenta en los pasos a seguir para la identificación, análisis, evaluación y tratamiento de los riesgos, las probabilidades de ocurrencia, impactos y la definición de estrategias de mitigación para la gestión de los mismos.

Se realizará una guía para la gestión, que sirva de orientación para una mejor administración de los riesgos.

[1] BANCO CENTRAL DE URUGUAY. Estándar australiano administración de riesgos. AS/NZS 4360:1999. Montevideo: BCU, 1999. p. 15.

1.6.2 Limitación y delimitaciones

1.6.2.1 Geográficas. Este proyecto se desarrollará en el departamento de sistemas de la empresa Apuestas Cúcuta 75, ubicada en la Av. 6 No.10-54 de la Ciudad de Cúcuta, Norte de Santander.

1.6.2.2 Temporales. El proyecto de investigación se llevará a cabo en un lapso de 12 semanas desarrollando cada objetivo propuesto, a partir de la aprobación del Anteproyecto.

1.6.2.3 Conceptuales. Los conceptos que abarcará esta investigación se fundamentan en las normativas y estándares para la gestión y administración de riesgos.

AS/NZS 4360:1999. Estándar Australiano. Administración de Riesgos.

NTC ISO 31000. Gestión del Riesgo. Principios y Directrices. 2011.

GTC 137. Gestión del Riesgo. Vocabulario.

1.6.2.4 Operativa. El desarrollo del proyecto desde el punto de vista operativo, se soporta en los procesos principales del departamento de sistemas de la empresa Apuestas Cúcuta 75.

Al realizar el diagnóstico del departamento de sistemas se puede presentar inconvenientes con el acceso o veracidad de la información.

Al momento de recolectar la información para definir el diagnóstico del departamento de sistemas, se pueden presentar retrasos al no ser entendida las preguntas definidas en la herramienta (entrevista) de recolección de la información.

Durante el desarrollo del proyecto se pueden presentar retrasos en el cronograma de actividades establecido.

Al determinar los estándares de gestión y/o administración de riesgos para el diseño de la guía, se puede seleccionar solo algunos de los definidos para el desarrollo del proyecto.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

Para la elaboración de este documento se tomaron como referencia algunos proyectos de investigación con temas afines y relacionables, realizados por otros estudiantes de diferentes universidades a nivel regional, nacional e internacional:

OSORIO RIVERO, Yenis Piedad y PÉREZ PÉREZ, Yesica Maria. Diseño de una política de gestión de riesgos de la información para la dependencia de admisiones registro y control de Universidad Francisco de Paula Santander Ocaña. Trabajo de Grado. Especialista en Auditoria de Sistemas. Ocaña: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Especialización en Auditoría de Sistemas, 2014.

La presente investigación propone una política de gestión de riesgos de la información para la oficina de admisiones registro y control de la universidad Francisco de Paula Santander Ocaña; se sustenta en el marco de trabajo de ISO/IEC 31000/ 2009 y en la metodología de análisis y gestión de riesgos de los sistemas de información magerit.

Teniendo en cuenta, que la presente propuesta está enfocada en la gestión de riesgos de la información, también se involucran conceptos relacionados con seguridad de la información que consisten en la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

ACOSTA PORTILLO, Dinael; CAMARGO BARBOSA, Jorge Alberto y NÚÑEZ ASCANIO, Karen Lorena. Diseño de un modelo de gestión del riesgo de tecnologías de información para la unidad de contabilidad de la Universidad Francisco de Paula Santander. Trabajo de Grado. Ingeniero de Sistemas. San José de Cúcuta: Universidad Francisco de Paula Santander. Facultad de Ingenierías. Departamento de Ingeniería de Sistemas, 2013.

El modelo diseñado en gestión de riesgos de TI surge para mejorar la calidad y seguridad de la información garantizando su disponibilidad, integridad y confidencialidad. Su desarrollo se basa en el ciclo PHVA y el triángulo organizacional fundamentándose en las buenas prácticas de gobernabilidad de TI, seguridad de la Información y administración de proyectos contempladas en NTC/ISO 27001, NTC/ISO 27002, NTC/ISO 27005, NTC/ISO 31000, NTC 5254, COBIT y PMBOK.

RAMÍREZ CASTRO, Alexandra y ORTIZ BAYONA, Zulima. Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.

Trabajo de Grado. Ingeniero de Sistemas. Bogotá: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería. Departamento de Ingeniería de Sistemas, 2011.

Este documento presenta una metodología para gestionar riesgos tecnológicos cuya base son los estándares ISO (International Organization for Standardization) 31000 e ISO/IEC (International Electrotechnical Commission) 27005, teniendo en cuenta que estos indican 'qué' se requiere para la gestión de riesgos más no indican 'cómo' se puede realizar esta gestión. Además incluye recomendaciones y buenas prácticas de otros estándares y guías internacionales para manejo de riesgos, seguridad y gestión de servicios.

La metodología se desarrolla para riesgo tecnológico dado que el aumento en el uso de tecnologías de la información puede posibilitar puntos de quiebre o fisuras en aspectos de seguridad con respecto a su utilización, por ello se presenta una forma de aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva tecnológica. Como segunda parte se presenta una forma de integración de la metodología a la gestión de continuidad de negocios, como sustento al análisis de impacto sobre negocios y el desarrollo de estrategias en lo que respecta a procesos de base tecnológica.

PALACIOS VARGAS, Andrea. Sistema de gestión del riesgo: compras y comercio exterior, bajo ISO 31000. Empresa Cosmoagro S. A., Santiago de Cali. Trabajo de Grado. Contador Público. Cali: Universidad de San Buenaventura Colombia. Facultad de Ciencias Económicas. Departamento de Contaduría Pública, 2013.

Este proyecto recopila de forma clara y sustancial el proceso de compras y de comercio exterior de la empresa Cosmoagro, explica cómo funciona el proceso de suministro a las áreas de la compañía tanto de lo referente al material productivo como de los elementos de apoyo administrativo que son necesarios para apoyar su labor. Una vez terminado este manual servirá como apoyo a la labor de compra con proveedores del exterior mediante la contratación de los servicios de comercio exterior prestados por parte de proveedores y terceros autorizados, logrando de esta manera que se cumpla de manera eficiente con los acuerdos establecidos en la negociación, Garantizando la eficacia y oportunidad del pago de las obligaciones a los proveedores contratados, mejorando de esta manera las ventajas de la negociación de la compañía y la relación mutua con nuestros afiliados en el suministro de bienes/servicios y desarrollar la actividad de pagos bajo una planificación que favorezca un sano balance en el flujo de caja de la compañía. Es importante hacer las cosas bien, también es importante que las organizaciones se organicen y estructuren una serie de indicadores que permitan realizar evaluaciones periódicas sobre el funcionamiento de cada proceso dentro de una organización.

GAONA VÁSQUEZ, Karina del Rocío. Aplicación de la metodología magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito S.A. en la ciudad de Machala, Cuenca, Ecuador. Trabajo de Grado. Ingeniero de Sistemas. Cuenca: Universidad Politécnica Salesiana sede Cuenca. Facultad de Ingeniería. Departamento de Ingeniería de Sistemas, 2013.

El presente proyecto de se trata de la seguridad de la información en cada uno de los activos que conforman la empresa "Pesquera e Industrial Bravito S.A.", para ello nos basamos en la Metodología Magerit versión 3 y con la herramienta PILAR 5.2.9 las cuales ayudan a medir el riesgo del estado actual de la empresa y como mitigarlo.

RODRÍGUEZ OCAMPO, Jair Alejandro. Definición de una metodología para la identificación, análisis, evaluación y tratamiento de riesgos en la unidad estratégica colombiana NTC ISO 31000:2009. Trabajo de Grado. Ingeniero Industrial. Bucaramanga: Universidad Pontificia Bolivariana Seccional Bucaramanga. Facultad de Ingeniería Industrial. Departamento de Ingeniería Industrial, 2014.

El proyecto comprende la consolidación de una metodología para gestionar riesgos de procesos en la Fundación Cardiovascular de Colombia, específicamente en la Unidad Estratégica de Negocios (UEN) Bioingeniería. Durante los 6 meses de práctica empresarial en la institución, la UEN Bioingeniería tuvo la iniciativa de gestionar riesgos con el fin de dar cumplimiento a lineamientos propuestos por la norma ISO 13485:2003, Dispositivos Médicos – Sistemas de Gestión de Calidad, en la cual fueron certificados el pasado 29 de Agosto de 2011. El resultado obtenido fue una metodología y un instrumento para gestionan los riesgos de los procesos de la organización, fundamentados en la norma ISO 31000:2009, Gestión del Riesgo – Principios y Directrices. Durante los 3 primeros meses de práctica en la FCV, se realizó un trabajo profundo de interpretación de la norma e investigación sobre conceptos y diferentes métodos de gestión sobre los lineamientos que propone la norma (identificación, análisis, evaluación, tratamiento y retroalimentación, de riesgos de procesos) consolidando estos conceptos se logró la definición de la metodología y el instrumento para gestionar riesgos de procesos y estratégicos, posterior a este proceso de investigación y definición, se realizó una socialización de estos conceptos, metodología y lineamientos sobre gestión de riesgos con los líderes de los 5 procesos que comprenden la UEN FCV Bioingeniería, dicha socialización sirvió de insumo a los líderes de procesos para iniciar la gestión de riesgos en sus respectivas áreas, este segundo paso tuvo lugar en los siguientes 3 meses de práctica, donde además se socializaron los avances de la gestión y se detectaron aspectos por mejorar a la metodología y al instrumento dando lugar a la fase de comunicación y consulta que propone la norma.

ESTÉVEZ AGUILAR, Diana Piedad. Estudio para el desarrollo de un modelo de gestión de riesgos y seguridad de la información para instituciones militares. Trabajo de Grado.

Maestría en Ingeniería de Sistemas. Quito: Escuela Politécnica Nacional. Facultad de Ingeniería. Departamento de Ingeniería de Sistemas, 2013.

Esta tesis propone un modelo de gestión de riesgos y seguridad de la información para instituciones militares. Para elaborar el marco de trabajo del modelo propuesto se partió de la norma ISO: 31000, con la fusión de los mejores elementos de dos metodologías de gestión de riesgos, MAGERIT v.3 y OCTAVE v.1, conformando las seis fases siguientes: Contexto Organizacional, Identificación de los Riesgos, Evaluación de los Riesgos, Tratamiento de los Riesgos, Comunicación, y Monitoreo y Revisión. Estas fases guiaran el análisis y administración de los riesgos en los siguientes ámbitos: evaluación de activos informáticos sujetos a riesgos, evaluación de servicios de seguridad o controles existentes, evaluación de vulnerabilidades ante amenazas identificadas, evaluación de amenazas o causas de riesgos, determinación y valoración del daño causado, estimación del nivel del riesgo y determinación de controles. Finalmente se evalúa el modelo de gestión de riesgos y seguridad de la información para instituciones militares en un caso de estudio.

2.2 MARCO CONCEPTUAL

La gestión de riesgos implica conocer algunas definiciones que amplíen los conocimientos sobre el tema. A continuación se definen de manera clara y sencilla los términos relacionados con la gestión del riesgo[2].

Riesgo. Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos organizacionales.

Gestión del riesgo. Es la capacidad que tiene la organización para emprender las acciones necesarias que le permitan el manejo de eventos que puedan afectar negativamente el logro de los objetivos organizacionales y protegerla de los efectos ocasionados por su ocurrencia.

Proceso para la gestión del riesgo. Aplicación sistemática de las políticas, procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.

Partes involucradas. Son las organizaciones y las personas que puedan afectar, ser afectadas por una decisión o actividad (clientes, proveedores, empleados).

[2] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Compendio Sistema de Gestión de Seguridad de la Información –SGSI. Bogotá: Kimpress, 2010.

Establecimiento contexto. La definición de los parámetros internos y externos que deben tenerse en cuenta en la gestión de riesgos, y la determinación del alcance y los criterios de riesgo para la política de gestión de riesgo.

Contexto Externo. Entorno externo en el que la organización busca alcanzar sus objetivos.

Contexto Interno. Ambiente interno en el que la organización busca alcanzar sus objetivos.

Valoración del riesgo. Elemento de control que determina el nivel o grado de exposición de la organización al impacto del riesgo, permitiendo estimar prioridades para su tratamiento mediante la aplicación de acciones tendientes a evitar, reducir, compartir o asumir el riesgo residual.

Identificación del riesgo. Elemento de control que posibilita conocer los eventos potenciales que ponen en riesgo el logro de los objetivos, estableciendo su descripción, agentes generadoras, causas y los efectos de su ocurrencia.

Fuente de riesgo. Constituyen los objetos o sujetos que tienen la capacidad de generar u originar un riesgo.

Consecuencias. Constituyen los efectos de la ocurrencia del riesgo sobre los objetivos de la empresa. Generalmente se dan sobre las personas o bienes con efectos muy importantes como daños físicos, fallecimientos, sanciones, pérdidas económicas, perdida de información, interrupción del servicio, daño ambiental, pérdida de imagen, pérdida de credibilidad y confianza.

Evento. Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Probabilidad. Es la posibilidad de que ocurra un evento específico o resultado, medido por la frecuencia y factibilidad de ocurrencia del riesgo, es expresado de manera cualitativa y cuantitativa.

Análisis del riesgo. Es el uso sistemático de información disponible para determinar con qué frecuencia un determinado evento puede ocurrir y la magnitud de sus consecuencias.

Criterio del riesgo. Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Nivel de riesgo. Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad.

Evaluación del riesgo. Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Tratamiento de riesgos. Selección e implementación de opciones apropiadas para tratar el riesgo.

Control. Son las políticas, procesos, prácticas u otras acciones que actúan para eliminar o minimizar los riesgos o maximizar oportunidades.

Riesgo residual. Se refiere al margen o residuo del riesgo que puede darse a pesar de las medidas de tratamiento tomadas para la gestión del riesgo.

Monitoreo. Comprobar, supervisar, observar cítricamente o registrar el progreso de una actividad, acción en forma sistemática para identificar cambios.

Mitigación. Planificación y ejecución de medidas dirigidas a reducir o minimizar los riesgos.

Transferir riesgos. Cambiar la responsabilidad o carga por las pérdidas a una tercera parte mediante legislación, contrato, seguro u otros medios. También se puede referir a cambiar un riesgo físico o parte del mismo a otro sitio.

2.3 MARCO CONTEXTUAL

2.3.1 La organización. El chance que según crónicas llegó de Cuba, operó como juego clandestino algunos años.

En el año de 1974 varios empresarios de todo Colombia deciden iniciar con su explotación, siendo el señor JUAN JOSE PITA MARTINEZ (Q.E.P.D.) y SAMUEL SANCHEZ

TORRES (Q.E.P.D) pioneros en el Departamento de Norte de Santander, quienes al año siguiente deciden crear la sociedad J.J. PITA Y CIA LTDA, mediante Escritura Pública 218 de la Notaría 3 de Cúcuta, conocida popularmente como Apuestas Cúcuta 75. Luego en 1976 se abrieron las agencias: Apuestas La Frontera, Santander, El Trébol, El Motilón cerrando algunas de ellas más tarde. En 1982 el gobierno a través de la ley 1 de ese año legaliza el juego de chance o Apuestas Permanentes y se localizan las siguientes empresas:

J.J PITA Y CIA LTDA, comercialmente Apuestas Cúcuta 75.

- Apuestas Santander.
- Apuestas La Frontera.
- Rojo y Negro.
- La 86.
- La Herradura.
- Las Vegas, entre otras.

Es así como se otorgó la primera licencia en el país para la explotación de apuestas permanentes siendo beneficiario de la misma la empresa J.J. PITA & CIA LTDA, la cual era dirigida por el señor JUAN JOSE PITA MARTINEZ.

En 1998 dicha sociedad se transformó en J.J. Pita Y CIA. S.A. mediante Escritura Pública 1255 suscrita en la notaría 2 de Cúcuta.

Hoy en día J.J. PITA Y CIA S.A. es una empresa 100% Norte santandereana que cuenta con aproximadamente 1006 empleados, incluidos 46 auxiliares del Sena bajo modalidad de contrato de aprendizaje, producto de la transformación de su estructura e implementación de estrategias.

J.J. PITA Y CIA S.A. no solo se ha caracterizado por ser en la actualidad la empresa del sector privado más grande del Departamento, su gestión va más allá del punto de vista económico, siendo pioneros y reconocidos a nivel nacional en RESPONSABILIDAD

SOCIAL EMPRESARIAL y fue así como en convenio suscrito con ICBF se creó en el año 2002 el primer Hogar Comunitario Empresarial del Departamento, que en la actualidad alberga aproximadamente 80 niños entre 0 y 7 años, en su mayoría hijos de madres solteras cabeza de familia que se dedican a comercializar apuestas permanentes, a través de la FUNDACION SOCIAL JJ PITA, creada en el mismo año.

JJ PITA Y CIA S.A. dirigida por el señor REINALDO ROJAS CASTELLANOS es una empresa líder en la región, dedicada al manejo de las apuestas permanentes, que se expande en todo el departamento fortaleciendo la imagen de la empresa y estableciendo la más avanzada tecnología digital para estar acorde con las exigencias del juego de las apuestas.

2.3.2 Dependencia de la Organización. La dependencia de sistemas tiene como objetivos aumentar la eficacia de los sistemas de información y tecnología para la óptima prestación del servicio y adoptar la gestión de riesgos como una actividad continua en cada uno de los procesos de la empresa.

La empresa APUESTAS CÚCUTA 75 (J.J. PITA Y CIA S.A.) vincula los objetivos de la dependencia de sistemas, directamente con la misión y visión de la empresa.

Misión. Comercializar juegos de suerte y azar, generando recursos a la salud en el departamento de Norte de Santander, recaudo y pago de servicios. Contribuyendo al progreso de la empresa y la comunidad; teniendo como principios la inversión en responsabilidad social empresarial, la eficiencia, seguridad, transparencia, cumplimiento, innovación y calidad humana; apoyados en infraestructura tecnológica propia y un sistema de gestión integral que permite un mejoramiento continuo.

Visión. Ser reconocidos en el 2018 como empresa generadora de nuevos productos, servicios y como aliados estratégicos en el aprovechamiento de nuestra infraestructura tecnológica, con personal altamente calificado para superar las expectativas de los clientes a nivel nacional. Manteniendo el liderazgo en la comercialización de juegos de suerte y azar.

2.4 MARCO TEÓRICO

Debido a que la definición del riesgo cubre una gama muy amplia de sucesos de diferente naturaleza, se han desarrollado diferentes modelos de gestión, algunos son propios por sector de actividad y otros se especializan en el tratamiento de algún tipo de riesgo.

Todas las definiciones de riesgo llevan a pensar que en una situación riesgosa existen muchos elementos que es necesario analizar para poder llegar a controlarlo (objetivos, probabilidad, incertidumbre, efectos), y si bien los riesgos pueden traer consecuencias negativas, no tomarlos en algunas ocasiones puede ser un riesgo en sí mismo, pues se pueden perder oportunidades que podrían traer mayores beneficios.

Es importante diferenciar entre riesgo e incertidumbre. La incertidumbre existe siempre que no se sabe con seguridad qué ocurrirá en el futuro; el riesgo es la incertidumbre que afecta negativamente el bienestar de la gente.

La administración de riesgos debe estar incorporada dentro de la organización a través de los procesos de estrategia y presupuesto.

Una buena Administración de Riesgos se centra en la identificación y el tratamiento de esos riesgos para aumentar la probabilidad de éxito y reducir tanto la probabilidad de fracaso como la incertidumbre de lograr los objetivos y metas generales de la organización.

2.4.1 AS/NZS 4360:1999 – Administración de Riesgos. En el Estándar Australiano AS/NZS 4360:1999, La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones[3].

Administración de riesgos es el término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. Administración de riesgos es tanto identificar oportunidades como evitar o mitigar pérdidas.

A continuación se describen los elementos principales del proceso de administración de riesgo.

1. Establecer contexto: identificación de los diferentes tipos de contexto, ya sea estratégico, organizacional o administración de riesgos, en el cual se tendrá lugar el proceso a controlar. Donde se debería establecer criterios que evalúen los riesgos y definan la estructura del análisis.

[3] BANCO CENTRAL DE URUGUAY. Op. cit., p. 23.

2. Identificar riesgos: Identificar el qué, el por qué y cómo pueden surgir las cosas como base para análisis posterior; en esta etapa se deberían incluir todos los riesgos, estén o no bajo control de la organización.

3. Analizar riesgos: Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de consecuencias potenciales y la probabilidad que ocurran estas mismas. Las consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.

4. Evaluar riesgos: Comparar niveles estimados de riesgos contra los criterios preestablecidos. Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración. Si los niveles de riesgo establecidos son bajos, los riesgos podrían caer en una categoría aceptable y no se requeriría un tratamiento.

5. Tratar riesgos: Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.

6. Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.

7. Comunicar y consultar con partes interesadas internas y externas según corresponda en cada etapa del proceso de administración de riesgo y concerniendo al proceso como un todo. La administración de riesgos se puede aplicar en una organización a muchos niveles. Se lo puede aplicar a proyectos específicos, para asistir con decisiones específicas o para administrar áreas específicas reconocidas de riesgo[4].

2.4.2 ISO 31000:2011 Gestión de Riesgos – Principios y Directrices. El enfoque genérico descrito en la Norma NTC-ISO 31000:2011 establece los principios y directrices para la gestión de cualquier forma de riesgo de una manera sistemática, transparente, creíble para cualquier ámbito y contexto.

Una característica clave de la NTC-ISO 31000:2011 es la inclusión del "Establecimiento del Contexto" como una actividad al inicio de la gestión del riesgo, al establecer el contexto se capturaran los objetivos de la organización, el entorno en el cual ella persigue sus

[4] Ibid., p. 25.

objetivos, las partes interesadas y la diversidad de criterios de riesgo con lo cual todo en conjunto ayudará a revelar y evaluar la naturaleza y complejidad de sus riesgos[5].

Cuando la gestión del riesgo se implementa y se mantiene de acuerdo con la Norma NTC – ISO 31000:2011, le permite a una institución, por ejemplo:

- Aumentar la probabilidad de lograr los objetivos.

- Fomentar una gestión proactiva.

- Se genera la conciencia de la necesidad para identificar y tratar los riesgos en toda la organización.

- Mejorar la identificación de las oportunidades y amenazas.

- Cumplir con las exigencias legales, reglamentarias y las normas internacionales.

- Mejorar la presentación de información obligatoria y voluntaria.

- Mejorar el nivel de confianza de las partes interesadas.

Establecer una base confiable para la toma de decisiones y la planificación.

- Mejorar los controles.

- Asignar y utilizar eficazmente los recursos para el tratamiento del riesgo.

- Mejorar la eficacia y la eficiencia operacional.

- Mejorar el desempeño de la salud y de seguridad, así como la protección del medio ambiente.

[5] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo, principios y directrices. NTC-ISO 31000. Bogotá: ICONTEC, 2011. p. 10.

- Mejorar la prevención de pérdidas y gestión de incidentes.

- Minimizar las pérdidas.

- Mejorar el aprendizaje de la organización[6].

La NTC–ISO 31000:2011 está destinada a satisfacer las necesidades de una amplia gama de partes interesadas, incluyendo:

- Los responsables de la formulación de políticas de gestión del riesgo dentro de la organización.

- Los responsables de asegurar que el riesgo se gestiona eficazmente dentro de la organización como un todo dentro de

- un área específica, un proyecto o actividad.

- Los que evalúan la eficacia de una organización basado en la gestión del riesgo.

- Los desarrolladores de los estándares, guías, procedimientos y códigos de prácticas que parcial o totalmente, establecen el modo de gestionar el riesgo dentro del contexto específico de estos documentos.

Principios de la Gestión del Riesgo:

- La gestión del riesgo crea y protege el valor. La gestión del riesgo contribuye al logro demostrable de los objetivos y a la mejora del desempeño, por ejemplo: la salud y la seguridad humana, la conformidad legal y reglamentaria, la seguridad, la aceptación pública, la protección del medio ambiente, la calidad del producto, la gestión de proyectos, la eficiencia en las operaciones y la reputación.

- La gestión del riesgo es una parte integral de todos los procesos de la organización. La gestión del riesgo no es una actividad independiente que se separa de las actividades y los procesos principales de la organización.

[6] Ibid., p. 10.

- La gestión del riesgo es parte de las responsabilidades de la dirección y una parte integral de todos los procesos de la organización, incluyendo la planeación estratégica y todos los procesos de gestión de proyectos y de cambio.

- La gestión del riesgo es parte de la toma de decisiones.

- La gestión del riesgo ayuda a quienes toman las decisiones a hacer elecciones informadas, priorizar acciones y distinguir entre cursos de acción alternativos.

- La gestión del riesgo aborda explícitamente la incertidumbre. La gestión del riesgo toma en consideración explícitamente a la incertidumbre, su naturaleza y la forma en que se puede tratar.

- La gestión del riesgo es sistemática, estructurada y oportuna. Un enfoque sistemático, oportuno y estructurado para la gestión del riesgo contribuye a la eficiencia y a resultados consistentes, comparables y confiables.

- La gestión del riesgo se basa en la mejor información disponible. Las entradas para el proceso de gestión del riesgo se basan en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes interesadas, observación, previsiones y examen de expertos. Sin embargo, quienes toman las decisiones deberían informarse y tomar en consideración todas las limitaciones de los datos o de los modelos utilizados o la posibilidad de divergencia entre los expertos.

- La gestión del riesgo está adaptada. La gestión del riesgo se alinea del contexto externo e interno y del perfil de riesgo de la organización.

- La gestión del riesgo toma en consideración los factores humanos y culturales. La gestión del riesgo reconoce las capacidades, percepciones e intenciones de individuos externos e internos, los cuales pueden facilitar o dificultar el logro de los objetivos de la organización.

- La gestión del riesgo es transparente e inclusiva. La correcta y oportuna intervención de las partes interesadas y en particular de aquellos que toman las decisiones en todos los niveles de la organización, garantiza que la gestión del riesgo siga siendo pertinente y se actualice. Esta intervención también permite a las partes interesadas estar correctamente representadas y hacer que sus puntos de vista se tomen en consideración al determinar los criterios del riesgo.

- La gestión del riesgo es dinámica, reiterativa y receptiva al cambio. La gestión del riesgo siente y responde continuamente al cambio. A medida que se presentan los eventos externos e internos, el contexto y el conocimiento cambian, tienen lugar el monitoreo y la revisión de los riesgos, emergen riesgos nuevos, algunos cambian y otros desaparecen.

- La gestión del riesgo facilita la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar la madurez de su gestión de riesgo junto con todos los otros aspectos de su organización[7].

2.4.3 Guía GTC 137 Gestión de Riesgos – Vocabulario. Esta norma suministra las definiciones de términos genéricos relacionados con la gestión del riesgo. El objetivo es fomentar un entendimiento mutuo y consistente de la descripción de las actividades relacionadas con esta gestión, así como un enfoque coherente de ésta, así el uso de terminología de gestión de riesgo uniforme en los procesos y los marcos de referencia relacionados con la gestión del riesgo.

Esta guía está destinada para el uso por parte de:

- Aquellos involucrados en la gestión de riesgos.

- Aquellos involucrados en actividades de ISO, IEC, y

- Aquellos a cargo de desarrollar normas, guías, procedimientos y códigos de práctica nacionales o específicos del sector relacionados con la gestión del riesgo[8].

2.5 MARCO LEGAL

En Colombia desde la expedición de la Ley 87 de 1993, se gesta el concepto de riesgos, al establecer como uno de los objetivos del control interno en el artículo 2 literal a) "proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan". También el literal f) expresa: "definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos".

[7] Ibid., p. 12.
[8] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo, Vocabulario. GTC 137:2011. Bogotá: ICONTEC, 2011.

Los lineamientos del marco legal relacionados con la gestión del riesgo tienen como base un conjunto de leyes, decretos, resoluciones y normativas que definen y orientan su estudio y aplicación. El riesgo y su gestión se fundamentan en el siguiente marco legal.

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso de Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En el Capítulo II, Principios Básicos, se dice:

Artículo 6. Gestión de la seguridad basada en los riesgos.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

El mismo Real Decreto 3/2010, en el Capítulo III, Requisitos Mínimos, se dice:

Artículo 13. Análisis y gestión de los riesgos.

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) dice así:

El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2.5.1 Decreto 4485 de 2009. Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) "establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

2.5.2 Ley 1474 de 2011. Estatuto Anticorrupción. Artículo 73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.

2.5.3 Norma Técnica Colombiana. Norma para la "Gestión de Riesgo" NTC 5254 de 2006.

Norma para la "Gestión de Riesgo" NTC 31000 de 2011.

Guía "Gestión del Riesgo - Vocabulario" GTC 137.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Esta es una investigación según el propósito de tipo descriptiva aplicada, cuyo producto responde a las necesidades de la organización en cuanto a la gestión y/o administración de riesgos a través del diseño de una guía para la gestión de riesgos, permitiendo así el logro de los objetivos misionales.

Este tipo de estudio es una investigación basada en el uso de fuentes externas, para apoyar el punto de vista y argumentos de un trabajo como son los estándares AS/NZS 4360:1999, la NTC-ISO 31000, GTC 137, implicando a menudo una parte de la conceptualización, el uso y la evaluación de dichas normas.

3.2 POBLACIÓN

La población para la realización de la investigación está conformada por trece (13) integrantes del departamento de sistemas de la empresa Apuestas Cúcuta 75, director de sistemas, programadores, administradores de la red y personal de mantenimiento de hardware.

3.3 MUESTRA

Debido a que el departamento de sistemas de la empresa Apuestas Cúcuta 75 está integrado por un limitado grupo de personas, se tomará como muestra la totalidad del personal.

3.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Las fuentes de información que se tienen en cuenta para la realización del proyecto se pueden catalogar en:

3.4.1 Fuentes de información primaria. La recolección de la información se realizara a través del trabajo con el personal de sistemas, mediante una entrevista al director del departamento de sistemas, documentación de los procesos establecidos en el departamento de sistemas, además de observar las instalaciones del departamento y el desarrollo de las tareas.

Las actividades a desarrollar para el cumplimiento de este proyecto se enmarcan en:

- Recolección de información mediante una entrevista al director del departamento de sistemas.

- Observación directa, esta será una herramienta de trabajo en donde se evaluarán las instalaciones y el funcionamiento del departamento de sistemas.

- Observación de la realización de las tareas del personal de sistemas.

- Documentación de los procesos establecidos en el departamento de sistemas.

- Durante todo este proceso se realizará el asesoramiento de la directora del proyecto de grado.

3.4.2 Fuentes de información secundaria. Las fuentes de la investigación fueron las normas AS/NZS 4360:1999, la NTC-ISO 31000:2011 y la guía GTC 137, normas relacionadas con la gestión de riesgos.

Artículos científicos relacionados con la gestión de riesgos.

4. PRESENTACIÓN DE RESULTADOS

Para el logro de los objetivos propuestos se implementaron una serie de actividades para el diseño de la guía de gestión de riesgos del departamento de sistemas. Se explica con el siguiente cuadro la estructura de desarrollo del proyecto:

Cuadro 1. Presentación de resultados

Objetivos Específicos	Actividades	Resultado/Entregable
Realizar un diagnóstico del departamento de sistemas de la empresa Apuestas Cúcuta 75, para establecer el contexto e identificar, valorar y tratar los riesgos	• Recolección de información como: misión, visión, metas, objetivos, estrategias, entre otros. • Realizar el análisis interno y externo para establecer el contexto del departamento de sistemas de la empresa Apuestas Cúcuta 75.	Análisis y evaluación de la información obtenida donde se definirá el contexto del departamento de sistemas, la cual se estructurará bajo un formato utilizando la técnica PESTA.
Identificar los estándares para el diseño de una guía de gestión y/o administración de riesgos para el departamento de sistemas de la empresa Apuestas Cúcuta 75, para minimizar las posibles amenazas.	• Analizar los estándares de gestión y/o administración de riesgos. • Determinar el estándar de gestión y/o administración de riesgos a utilizar para el diseño de la guía.	Análisis y elaboración de Cuadro comparativo de estándares para la gestión y/o administración de riesgos (AS/NZS 4360:1999, NTC ISO 31000, GTC 137).
Elaborar un documento que guie la gestión del riesgo, según la información recolectada en el departamento de sistemas de la empresa Apuestas Cúcuta 75.	• Proyectar la guía de gestión de riesgos. • Aplicar el proceso de comunicación y consulta, valoración, tratamiento, monitoreo y revisión, a dos riesgos relevantes del departamento de sistemas.	Documento: "Diseño de la guía para la gestión de Riesgos del departamento de sistemas de Apuestas Cúcuta 75". Ejemplos aplicados a la guía diseñada.
Socializar la guía de gestión de riesgos al personal del departamento de sistemas de la empresa Apuestas Cúcuta 75.	• Reunir al personal de sistemas y socializar la guía para la gestión de riesgos.	Presentación de diapositivas con el resumen de la Guía a socializar al personal, incluyendo ejemplos aplicados. Listado del personal asistente a la socialización. Evaluación de la socialización por parte de los asistentes.

Fuente: Autores del proyecto.

4.1 DIAGNOSTICO EMPRESARIAL BASADO EN VALORACIÓN DE RIESGOS.

Objetivo: Realizar un diagnóstico del departamento de sistemas de la empresa Apuestas Cúcuta 75, para establecer el contexto e identificar, valorar y tratar los riesgos.

Para lograr este objetivo se plantearon las siguientes actividades, las cuales se desarrollaron en el siguiente orden.

- Actividad 1: Recolectar información como: misión, visión, metas, objetivos, estrategias, entre otros.

- Actividad 2: Realizar el análisis interno y externo para establecer el contexto del departamento de sistemas de la empresa Apuestas Cúcuta 75.

Desarrollo del objetivo:

Actividad 1: Recolectar información como: misión, visión, metas, objetivos, estrategias, entre otros.

La recolección de la información se realizó a través de la aplicación de una entrevista al director del departamento de sistemas (ANEXO A) con la que se determinó el contexto establecido en el departamento. Además, se obtuvo información tanto a nivel organizacional (misión, visión, objetivos), como de la dependencia de sistemas (procesos, subprocesos y objetivos), información obtenida a partir de la documentación establecida en área.

A continuación se relaciona la información suministrada por la dependencia de sistemas, para posteriormente establecer el contexto en el que se desarrolla:

4.1.1 Reconocimiento del Departamento de Sistemas de la Empresa Apuestas Cúcuta 75. En el reconocimiento realizado al departamento de sistemas de la empresa Apuesta Cúcuta 75, se obtuvo información, que brindo soporte fundamental para el desarrollo del objetivo de la presente propuesta.

El departamento de sistemas, está permanentemente expuesto a riesgos que pueden comprometer los objetivos misionales, con el fin de apoyar la gestión de riesgos se propone diseñar una guía, la cual tiene como finalidad establecer los elementos y el marco general de actuación para la gestión integral de los riesgos de toda naturaleza a los que se enfrenta el área de sistemas, de forma tal que se garantice el cumplimiento de los objetivos organizacionales.

4.1.1.1 Misión y Visión del Departamento de Sistemas. APUESTAS CÚCUTA 75 (J.J. PITA Y CIA S.A.) vincula los objetivos de la dependencia de sistemas, directamente con la misión y visión de la empresa.

Misión. Comercializar juegos de suerte y azar, generando recursos a la salud en el departamento de Norte de Santander, recaudo y pago de servicios. Contribuyendo al progreso de la empresa y la comunidad; teniendo como principios la inversión en responsabilidad social empresarial, la eficiencia, seguridad, transparencia, cumplimiento, innovación y calidad humana; apoyados en infraestructura tecnológica propia y un sistema de gestión integral que nos permita un mejoramiento continuo.

Visión. Ser reconocidos en el 2018 como empresa generadora de nuevos productos, servicios y como aliados estratégicos en el aprovechamiento de nuestra infraestructura tecnológica, con personal altamente calificado para superar las expectativas de los clientes a nivel nacional. Manteniendo el liderazgo en la comercialización de juegos de suerte y azar.

4.1.1.2 Objetivos del departamento de Sistemas. Objetivos:

- Satisfacer los requerimientos de los clientes internos.

- Asegurar la continuidad de los servicios de TI según lo requerido y en caso de falla minimizar el impacto sobre el funcionamiento del sistema.

- Mantener la disponibilidad, integridad y confidencialidad de los sistemas de información, mediante la implementación de controles de seguridad.

- Capacitar al usuario en el uso de la tecnología, los riesgos y las responsabilidades involucradas.

Objetivo Integral:

- Adoptar la gestión de riesgos como una actividad continua en cada uno de los procesos de la empresa.

- Aumentar la eficacia de los sistemas de información y tecnología para la óptima prestación del servicio.

4.1.1.3 Diagrama de Procesos del Departamento de Sistemas de Apuestas Cúcuta 75. Para realizar los diagramas de procesos se consultó la documentación de la dependencia de sistemas de la empresa APUESTAS CÚCUTA 75 (J.J. PITA Y CIA S.A.), en el cual se definen los procesos principales del departamento.

APUESTAS CÚCUTA 75 (J.J. PIT AY CIA S.A.), realiza sus productos, brinda servicios y llega a sus usuarios utilizando diferentes procesos diseñados por el departamento de sistemas.

Figura 1. Diagrama de Procesos del Departamento de Sistemas de Apuestas Cúcuta 75

Fuente: Autores del proyecto.

Este proceso se encuentra compuesto por tres procesos, que permiten cumplir con las exigencias del departamento de sistemas de la empresa APUESTAS CÚCUTA 75 (J.J. PITA Y CIA S.A.), con el fin de dar cumplimiento y evaluación de la documentación respectiva. Estos procesos son:

- Proceso Gestión De Desarrollo De Software.

- Proceso Gestión de Comunicaciones.

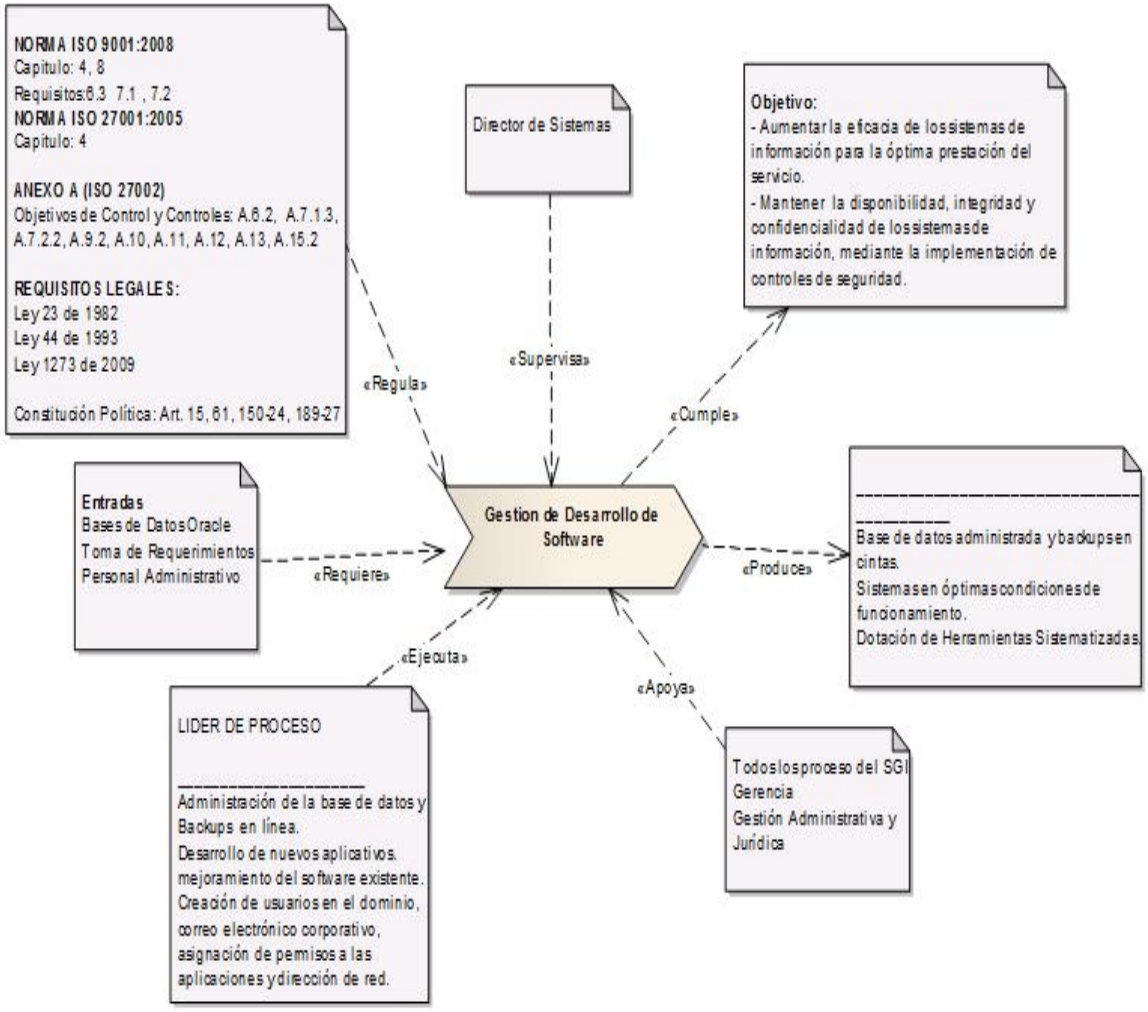
- Proceso Gestión de Soporte de Hardware.

La descripción de cada uno de estos procesos se presenta en el Diagrama de Descripción de Procesos de manera jerárquica.

- **Diagrama de Descripción de Procesos**

- **Diagrama de Proceso Gestión de Desarrollo de Software.** El proceso de Gestión de Desarrollo de Software tiene como objetivo asegurar el correcto funcionamiento del software logrando la eficacia y el buen funcionamiento de todo el sistema operacional y organizacional, pasando por la administración de la base de datos, desarrollos de nuevos aplicativos, mejoramiento del software existente, creación de usuarios y asignación de permisos e implementación de controles de seguridad.

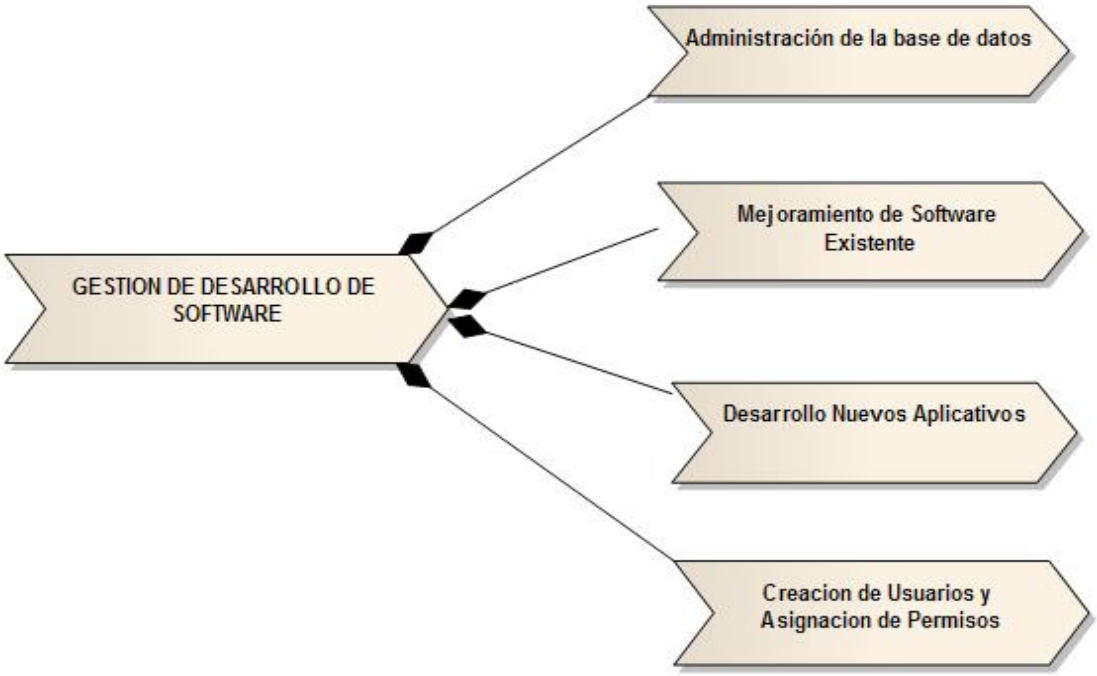
Figura 2. Diagrama de Proceso Gestión de Desarrollo de Software



Fuente: Autores del proyecto.

- **Diagrama Gestión de Desarrollo de Software y sus Subprocesos**

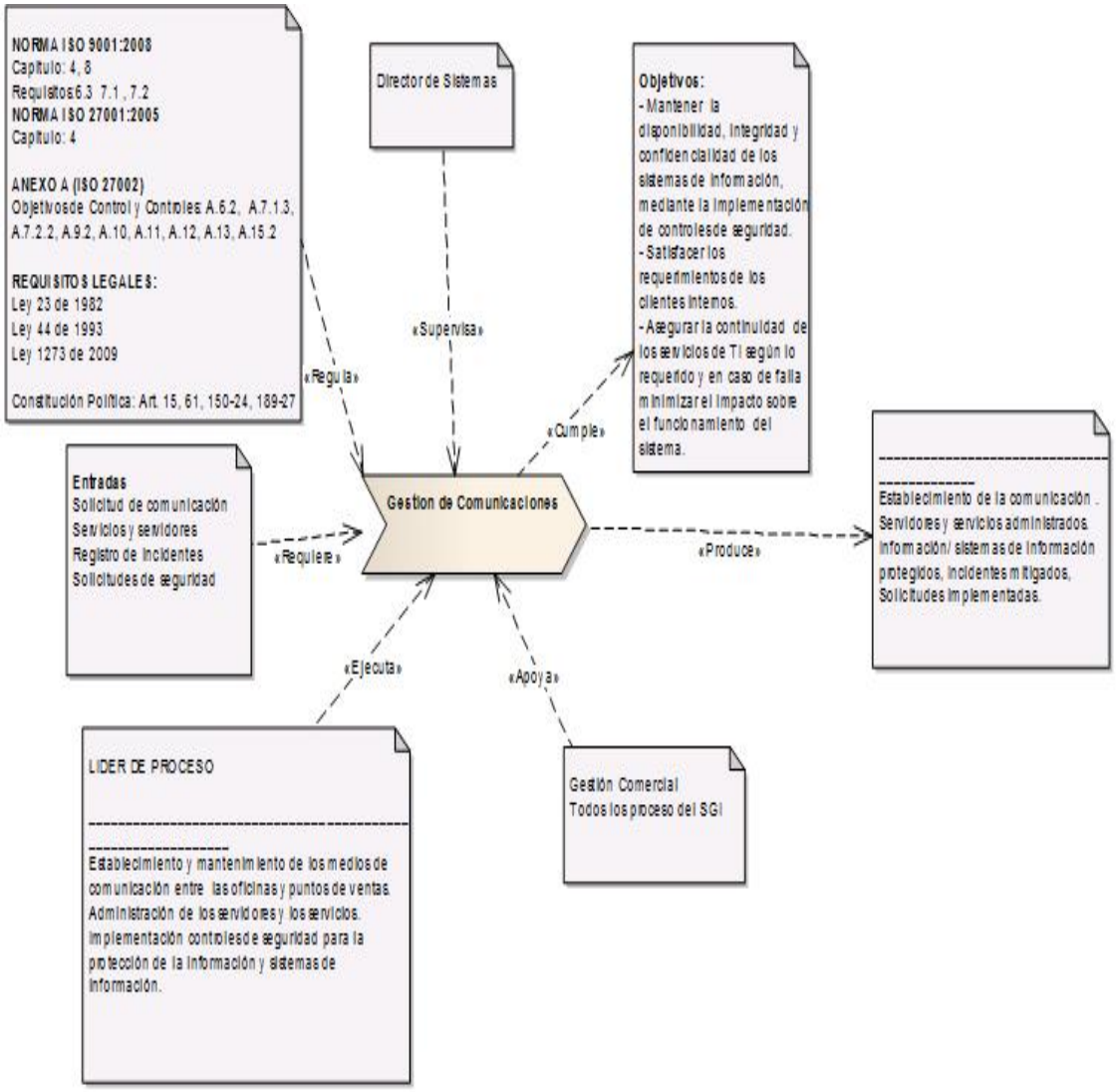
Figura 3. Diagrama Gestión de Desarrollo de Software y sus Subprocesos



Fuente: Autores del proyecto.

- **Diagrama de Proceso Gestión de Comunicaciones.** El proceso de Gestión de Desarrollo de Comunicaciones tiene como objetivo Asegurar el correcto funcionamiento de las Comunicaciones logrando la eficacia y el buen funcionamiento de todo el sistema operacional y organizacional, pasando por el Establecimiento y mantenimiento de los medios de comunicación, Administración de los servidores y los servicios.

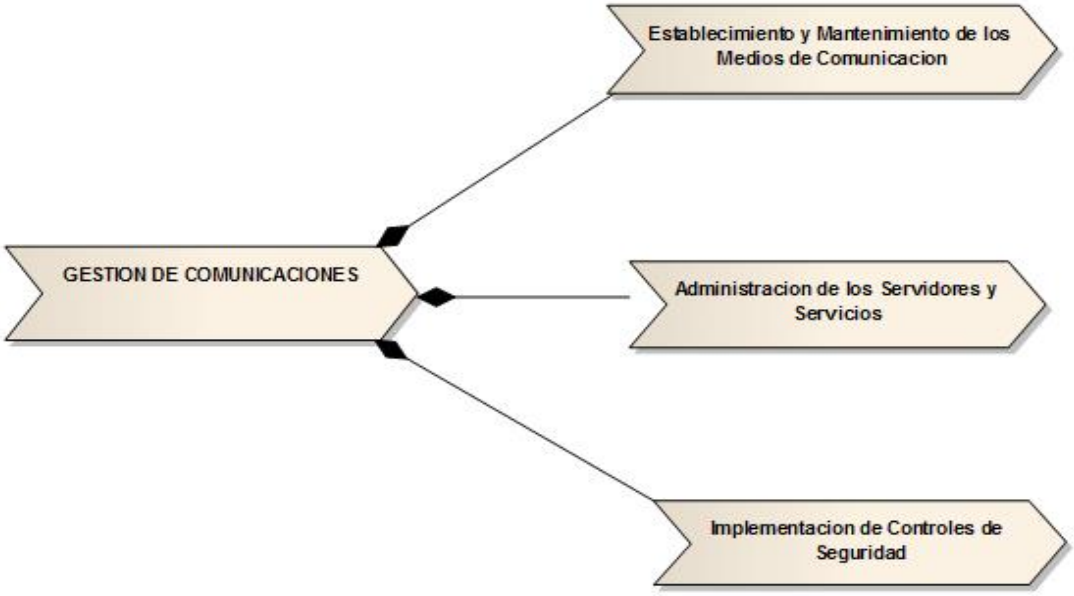
Figura 4. Diagrama de Proceso Gestión de Comunicaciones



Fuente: Autores del proyecto.

- **Diagrama de Proceso Gestión de Comunicaciones y sus Subprocesos**

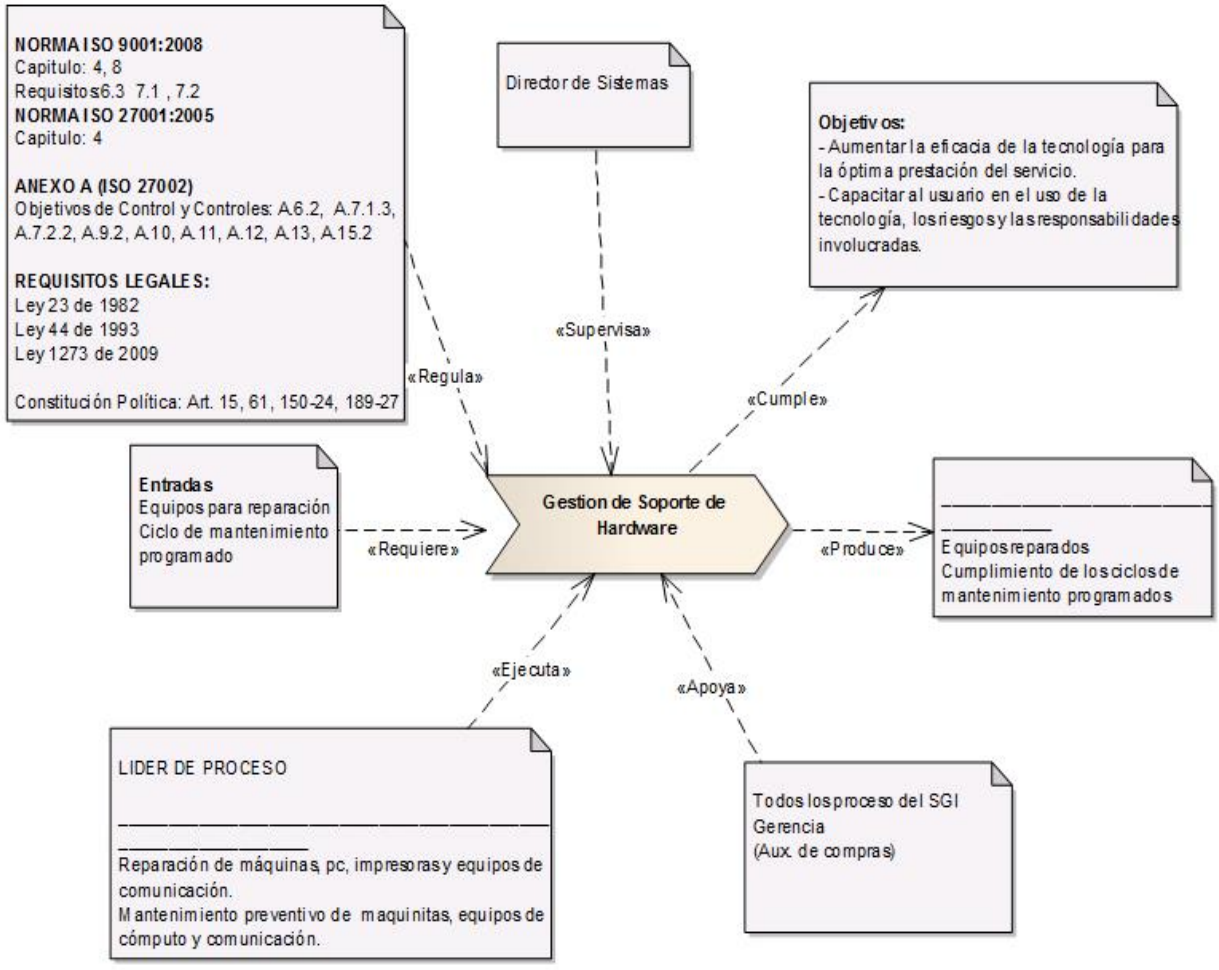
Figura 5. Diagrama de Proceso Gestión de Comunicaciones y sus Subprocesos



Fuente: Autores del proyecto.

- **Diagrama de Proceso Gestión de Soporte de Hardware.** El proceso de Gestión de Soporte de Hardware tiene como objetivo asegurar el correcto funcionamiento del hardware logrando la eficacia y el buen funcionamiento de todo el sistema operacional y organizacional, pasando por la reparación y mantenimiento de equipos de comunicación e Información.

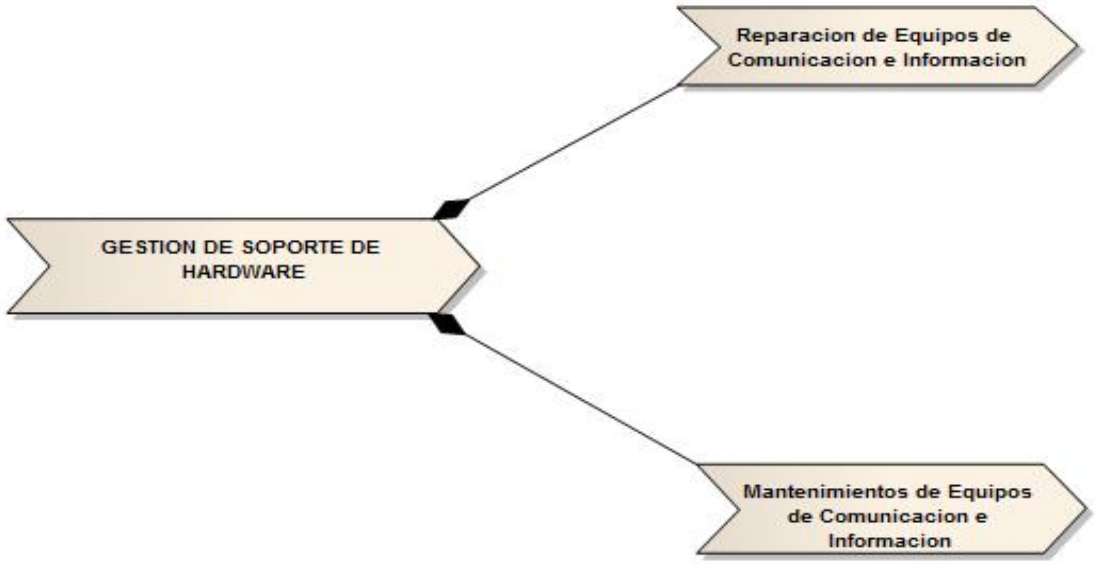
Figura 6. Diagrama de Proceso Gestión de Soporte de Hardware



Fuente: Autores del proyecto.

- **Diagrama de Proceso Gestión de Soporte de Hardware y sus Subprocesos**

Figura 7. Diagrama de Proceso Gestión de Soporte de Hardware y sus Subprocesos



Fuente: Autores del proyecto.

Actividad 2: Realizar el análisis interno y externo para establecer el contexto del departamento de sistemas de la empresa Apuestas Cúcuta 75.

Una vez recolectada la información del departamento de sistemas, se realizó el análisis de factores internos y externos, donde se establece el contexto en el que se desarrolla el departamento.

4.1.2 Establecimiento del contexto del departamento de sistemas. Para establecer el contexto en el departamento de sistemas se realizó el análisis interno y externo, estableciéndose dentro del alcance y los criterios en los cuales se evaluarán y analizarán los riesgos posteriormente.

El contexto (interno y externo) del departamento de sistemas se efectuó utilizando la técnica PESTA, la cual se estructuró de acuerdo al siguiente cuadro:

Cuadro 2. Establecimiento del contexto

ESTABLECIMIENTO DEL CONTEXTO	Código:	F- GR- 02
	Versión:	01
	Elaborado:	12-01-2015
	Página:	1 de 3

ESTABLECIMIENTO DEL CONTEXTO
Empresa o Dependencia: Sistemas
Proceso: Gestión de Sistemas
Objetivo: Adoptar la gestión de riesgos como una actividad continúa en el proceso de gestión de sistemas
Alcance: Comprende los lineamientos para la gestión de riesgos en el proceso de sistemas.
Responsable: Director de Sistemas
Recursos: Aplicaciones para la detección de vulnerabilidades, recurso humano
Relación: Recursos Humanos, Gerencia

DIAGNÓSTICO DEL CONTEXTO EXTERNO (FACTORES DE RIESGO) – AMENAZAS	
POLÍTICO/LEGAL	**ECONÓMICOS**
1. Inclusión o modificación de normativas (leyes, acuerdos o resoluciones) que comprometan al sector de juegos de suerte y azar "acuerdo 097de 2014". 2. Implementación por parte del máximo órgano de la empresa de nuevas políticas internas o cambios en las existentes, que afecten la dependencia de sistemas.	1. Situación económica del Departamento Norte de Santander. 2. Disminución en la asignación de recursos para la dependencia de sistemas.

Cuadro 2. (Continuación)

ESTABLECIMIENTO DEL CONTEXTO	Código:	F- GR- 02
	Versión:	01
	Elaborado:	12-01-2015
	Página:	2 de 3

POLÍTICO/LEGAL	**ECONÓMICOS**
1. Alteraciones del orden público. 2. Incremento de nuevos grupos delictivos y criminales.	1. Vulnerabilidad en los sistemas de seguridad de la información. 2. La proliferación de delitos informáticos.
AMBIENTALES	
1. Fenómenos naturales. 2. Los factores climáticos que afectan el desarrollo de las actividades fuera de las instalaciones y la eficiencia de los equipos externos de comunicación.	

DIAGNÓSTICO DEL CONTEXTO INTERNO (FACTORES DE RIESGO) – DEBILIDADES	
POLÍTICO/LEGAL	**ECONÓMICOS**
1. Incumplimiento de los procedimientos establecidos en la dependencia de sistemas 2. Incumplimiento en la normatividad y procedimientos de derechos de autor.	1. Ausencia de un plan estratégico de TI. 2. Deficiencia en la administración de los recursos asignados a la dependencia.
POLÍTICO/LEGAL	**ECONÓMICOS**
1. Multiplicidad de funciones a un mismo cargo. 2. Personal con baja formación ética y moral que debilita el trabajo en equipo.	1. Ausencia de estudios de seguridad de la información e informáticos. 2. No aplicación de actualizaciones (parches de seguridad).

Cuadro 2. (Continuación)

ESTABLECIMIENTO DEL CONTEXTO	Código:	F- GR- 02
	Versión:	01
	Elaborado:	12-01-2015
	Página:	3 de 3

AMBIENTALES
1. Ausencia de un procedimiento sobre la eliminación de equipos informativos obsoletos en pro del medio ambiente. **2.** Eliminación inadecuada de los equipos informáticos obsoletos (no se aplican prácticas de reciclaje).

Elaborado Por: Director de Sistemas	Fecha: 14-01-2015
Revisado Por: Gestor de Riesgos	Fecha: 14-01-2015
Aprobado Por: Comité de Riesgos	Fecha: 14-01-2015

Fuente: Autores del proyecto.

Con la información recolectada se identificó el contexto del departamento de sistemas, para ello se diseñó un formato en el cual se establece el nombre de la empresa o dependencia dependiendo del ámbito de aplicación, el proceso, objetivo(s), el alcance, los responsables, los recursos, las relaciones (con otras dependencias), contiene además el diagnóstico y análisis de los factores de riesgo tanto interno (debilidades) como externo (amenazas) establecidos a nivel político, económico, social, tecnológico y ambiental.

De acuerdo al análisis del contexto se diagnostica que el departamento de sistemas no cuenta con una visión y misión propia, así como los objetivos del área ya que se encuentran vinculados directamente con la misión y visión de la empresa. Además presenta una serie de amenazas y debilidades en los diferentes niveles: políticos, económico, social, tecnológico y ambiental, lo que indica que se hace necesario la gestión de riesgos dentro del departamento de sistemas de la empresa apuestas Cúcuta 75, para eliminar o reducir la probabilidad o impacto de estos eventos que pueden comprometer los objetivos del departamento y la organización.

Este tipo de valoración permite conocer profundamente todos los aspectos y acciones del departamento, teniendo a la mano la situación empresarial y exactamente la del área de sistemas, sus objetivos, impedimentos y alcances. A través de este proceso se reconocen múltiples responsabilidades en las que existen probabilidades de riesgo, dando la oportunidad de considerar su gestión como una herramienta necesaria.

Al tomar la información necesaria sobre el proceso, se evidencian acciones en torno a las actividades de desarrollo de software, administración de la red, mantenimiento de hardware y oportunidad de riesgo como perdidas de servicios e información, sabotajes, alteración de datos, entre otros que deben ser atendidos de manera oportuna.

4.2 IDENTIFICACIÓN DE ESTÁNDARES PARA LA GESTIÓN Y/O ADMINISTRACIÓN DE RIESGOS

Objetivo: Identificar los estándares para el diseño de una guía de gestión y/o administración de riesgos para el departamento de sistemas de la empresa Apuestas Cúcuta 75, para minimizar las posibles amenazas.

Para lograr este objetivo se plantearon y desarrollaron las siguientes actividades.

- Actividad 1: Analizar los estándares de gestión y/o administración de riesgos.

- Actividad 2: Determinar el estándar de gestión y/o administración de riesgos a utilizar para el diseño de la guía.

Desarrollo del objetivo:

Actividad 1: Analizar los estándares de gestión y/o administración de riesgos.

4.2.1 Análisis de estándares de gestión y/o administración de riesgos. Existen una serie de estándares y normas que orientan como se deben administrar o gestionar los riesgos en una organización, para el desarrollo de este proyecto se analizaron y compararon los estándares y normativos más utilizados. Para ello se presenta un comparativo donde se resaltan los lineamientos establecidos en cada uno de ellos:

Cuadro 3. Comparativo estándares y normas de gestión de riesgos

COMPARATIVO ESTANDARES Y NORMAS DE GESTIÓN DE RIESGOS		
NTC-ISO 31000	**AS/NZS 4360:1999**	**GUIA GTC 137**
Esta norma proporciona las directrices en la gestión de riesgos permitiendo a las organizaciones lograr sus objetivos, tener una línea base para la planificación y toma de decisiones, mejorar la gestión de incidentes y la reducción de costos y riesgos.	Este Estándar provee una guía genérica para el establecimiento e implementación del proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.	Esta guía suministra las definiciones de términos genéricos relacionados con la gestión del riesgo. El objetivo es fomentar un entendimiento mutuo y consistente de la descripción de las actividades relacionadas con esta gestión, así como un enfoque coherente y el uso de terminología de gestión de riesgo uniforme en los procesos y los marcos de referencia relacionados con la gestión del riesgo.
Esta norma establece cinco procesos para la gestión del riesgo: Comunicación y consulta. Establecimiento del contexto. Valoración del riesgo. Tratamiento del riesgo. Monitoreo y revisión.	Establece unos elementos principales dentro del proceso de administración de riesgos: Establecer el contexto. Identificar riesgos. Analizar riesgos. Evaluar riesgos. Tratar riesgos. Monitorear y revisar. Comunicar y consultar.	
Establece un marco de referencia para la gestión, el cual brinda las bases y disposiciones que se introducirán en todos los niveles de la organización. El marco garantiza que la información acerca del riesgo derivada del proceso para la gestión del riesgo se reporte de manera adecuada y se utilice como base para la toma de decisiones.		

Cuadro 3. (Continuación)

COMPARATIVO ESTANDARES Y NORMAS DE GESTIÓN DE RIESGOS		
NTC-ISO 31000	**AS/NZS 4360:1999**	**GUIA GTC 137**
Al establecer el contexto la organización articula sus objetivos, define los parámetros internos y externos, y establece los criterios del riesgo para el resto del proceso.	Establecer el contexto estratégico, organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso.	
Identificar las fuentes de riesgo, las áreas de impacto, los eventos, sus causas y consecuencias potenciales.	Identificar qué, por qué y cómo pueden surgir las cosas como base para un análisis posterior.	
Facilita la toma de decisiones basado en los resultados del análisis de riesgos obtenido. Implica la comparación del nivel de riesgo observado durante el análisis y de los criterios de riesgo establecidos al considerar el contexto.	Compara los niveles estimados de riesgos contra los criterios preestablecidos.	
El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones.	Aceptar y monitorear los riesgos de baja prioridad. Para desarrollar otros riesgos e implementar un plan de administración especifico.	
El monitoreo y revisión son parte integral del proceso para la gestión del riesgo.	Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.	

Fuente: Autores del proyecto.

Actividad 2: Determinar el estándar de gestión y/o administración de riesgos a utilizar para el diseño de la guía.

4.2.2 Determinación del estándar de gestión de riesgos para el diseño de la guía. Para determinar el estándar a utilizar para el diseño de la guía de gestión de riesgos, se analizó el comparativo anterior y se determinaron las normas AS/NZ4360, ISO 31000 y la guía GTC 37, las cuales se señalan a continuación:

El estándar ISO 31000 acoge prácticamente todo el AS/NZ4360; adicionalmente, incorpora once (11) principios claves, enunciados a continuación:

Principio I: Crear valor.

Principio II: Es parte integral de los procesos de la organización.

Principio III: Es parte de la toma de decisiones.

Principio IV: Aborda explícitamente la incertidumbre.

Principio V: Es sistemática, estructurada y oportuna.

Principio VI: Se basa en la mejor información disponible.

Principio VII: Esta adaptada.

Principio VIII: Toma en consideración a los factores humanos y culturales.

Principio IX: Es transparente e inclusiva.

Principio X: Es dinámica, reiterativa y receptiva al cambio.

Principio XI: Facilita el mejoramiento continuo de la organización

Lo anterior, brinda a la gestión de riesgos un soporte firme para desarrollar un modelo de gestión operacional más amplio y con la capacidad de abarcar todos los objetivos que soporte la estrategia del negocio.

Respecto al marco general de trabajo, el cual permite incorporar la práctica basada en el estándar en todos los niveles de la organización, se desarrollaron unas guías de importante valor que orientan con detalle las acciones a ejecutar, agrupadas en el siguiente ciclo continuo:

- Diseño del marco de referencia para la gestión de riesgos.

- Implementación de la gestión de riesgos.

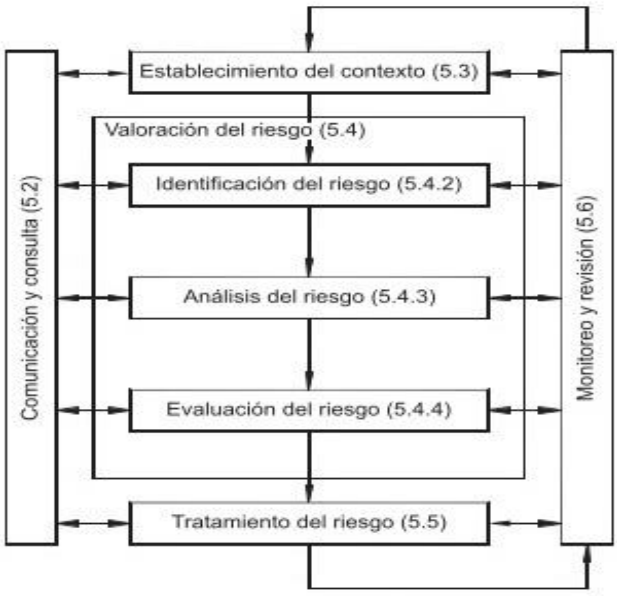
- Monitorización y revisión del marco de riesgos.

- Mejoramiento continúo del marco de referencia.

Un aspecto relevante del ISO 31000; y que nos agrada saber; es que, en el centro del marco de gestión de riesgos, está el proceso de evaluación (risk assessment), el cual se mantiene casi idéntico al apreciado y efectivo AS/NZ4360.

Proceso. El proceso para la gestión de riesgos debería ser parte integral de la gestión, estar incluido en la cultura y las prácticas y estar adaptado a los procesos de negocio de la organización.

Figura 8. Proceso para la gestión del riesgo



Fuente: INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo, principios y directrices. NTC-ISO 31000. Bogotá: ICONTEC, 2011.

Comunicación y consulta. Un enfoque de equipo consultor puede:

- Ayudar a establecer correctamente el contexto.
- Garantizar que se entienden y se toman en consideración los intereses de las partes involucradas.
- Ayudar a garantizar que los riesgos estén correctamente identificados.
- Reunir diferentes áreas de experticia para analizar los riesgos.
- Garantizar que los diversos puntos de vista se toman en consideración adecuadamente al definir los criterios y al evaluar los riesgos.
- Asegurar la aprobación y el soporte para el plan de tratamiento.
- Fomentar la gestión adecuada del cambio durante el proceso para la gestión del riesgo y desarrollar un plan adecuado de comunicación y consulta externo e interno.

Establecimiento del contexto. La organización articula sus objetivos, define los parámetros externos e internos que se va a considerar al gestionar el riesgo y establecer el alcance y los criterios del riesgo para el resto del proceso.

- Establecer el contexto externo.
- Establecer el contexto interno.
- Establecer el contexto del proceso para la gestión del riesgo.
- Definir los criterios del riesgo.

Valoración del riesgo. La valoración del riesgo es el proceso total de identificación, análisis y evaluación del riesgo.

Tratamiento del riesgo. El tratamiento del riesgo involucra una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.

Monitoreo y revisión. Debe ser una parte planificada del proceso para la gestión del riesgo e incluir verificación o vigilancia regular.

El análisis de riesgos considera los siguientes elementos:

- Activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización.

- Amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la organización.

- Salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

- El impacto: lo que podría pasar.

- El riesgo: lo que probablemente pase.

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión[9].

La guía GTC 137 suministra las definiciones de términos genéricos relacionados con la gestión del riesgo. El objetivo es fomentar un entendimiento mutuo y consistente de la descripción de las actividades relacionadas con esta gestión, así como un enfoque coherente

[9] (Dirección General de Modernización Administrativa pág. 127)

de ésta, así el uso de terminología de gestión de riesgo uniforme en los procesos y los marcos de referencia relacionados con la gestión del riesgo.

4.3 DISEÑO DE LA GUÍA DE GESTIÓN DE RIESGOS PARA EL DEPARTAMENTO DE SISTEMAS.

Objetivo: Elaborar un documento que guie la gestión del riesgo, según la información recolectada en el departamento de sistemas de la empresa Apuestas Cúcuta 75.

Para el logro de este objetivo se plantearon y desarrollaron las siguientes actividades.

- Actividad 1: Proyectar la guía de gestión de riesgos.

- Actividad 2: Aplicar el proceso de comunicación y consulta, valoración, tratamiento, monitoreo y revisión, a dos riesgos relevantes del departamento de sistemas.

Desarrollo del objetivo:

Actividad 1: Proyectar la guía de gestión de riesgos.

La guía se diseñó con base en los estándares ISO 31000, ANZ 4360 y la guía GTC 137, comprende el marco normativo y conceptual, los pasos a seguir para la gestión de riesgos, el mapa de riesgos, la política de gestión de riesgos y el glosario de términos utilizados, pudiéndose aplicar a un rango de actividades, incluyendo estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos (Véase el Anexo D).

Actividad 2: Aplicar el proceso de comunicación y consulta, valoración, tratamiento, monitoreo y revisión, a un riesgo relevante del departamento de sistemas.

El proceso de comunicación y consulta, valoración, tratamiento, monitoreo y revisión, se aplicó a un riesgo relevante del departamento de sistemas, el cual se muestra a continuación:

Comunicación y consulta. El proceso de comunicación y consulta es parte integral de la gestión de riesgos, para llevarlo a cabo a lo largo del proceso se diseñó un formato, el cual

contiene información del riesgo, como descripción, causas y consecuencias, así como información relevante de las partes involucradas.

A continuación se anexa el formato diseñado, junto con el ejemplo aplicado:

Cuadro 4. Comunicación y consulta de riesgos

COMUNICACIÓN Y CONSULTA DE RIESGOS	Código:	F- GR- 01
	Versión:	01
	Elaborado:	12-01-2015
	Página:	1 de 3

COMUNICACIÓN Y COSULTA DE RIESGOS		
COMUNICANTE	**Fecha:** 13-01-2015	**Empresa o Dependencia:** Sistemas
	Nombre: Carlos Parra	**Cargo:** Director de Sistemas

COMUNICADO	**Riesgo:** Bajo rendimiento de la base de datos por una administración inadecuada
	Causas: 1. Administración deficiente de la Base de Datos. 2. No se tiene establecido un procedimiento de monitoreo y mantenimiento de la Base de Datos.
	Consecuencias: 1. Interrupción en la prestación del servicio al cliente. 2. Aumento de los tiempos de respuesta del sistema de información.

Cuadro 4. (Continuación)

COMUNICACIÓN Y CONSULTA DE RIESGOS	Código:	F- GR- 01
	Versión:	01
	Elaborado:	12-01-2015
	Página:	2 de 3

Valoración Riesgo

(I) Impacto

1	2	3	**4**	5

(P) Probabilidad

1	2	3	4	**5**

(N) Nivel Riesgo

1	2	3	**4**

Opción Tratamiento

1	2	3	4

ACCIONES/DECISIONES	**FECHA**	**RESPONSABLE(S)**
Evaluar e implementar técnicas para mejorar el rendimiento de base de datos.	14-01-2015	Administrador de la base de datos (DBA).
Redefinir las funciones del administrador de base de datos para una correcta administración de la misma.	14-01-2015	Director de sistemas.

Conclusiones: El riesgo de clasificación tecnológica es de gran impacto lo cual puede ocasionar la interrupción de las operaciones, por esta razón se debe tratar de manera inmediata.

Cuadro 4. (Continuación)

COMUNICACIÓN Y CONSULTA DE RIESGOS	Código:	F- GR- 01
	Versión:	01
	Elaborado:	12-01-2015
	Página:	3 de 3

Recomendaciones: Se requiere la implementación las acciones de manera inmediata para bajar el nivel del riesgo.

(I) Impacto	**(P) Probabilidad**	**(N) Nivel Riesgo**	**Opción Tratamiento**
1 Insignificante	1 Raro	1 Bajo	1 Mitigar
2 Menor	2 Improbable	2 Medio	2 Evitar
3 Moderado	3 Posible	3 Alto	3 Transferir
4 Mayor	4 Probable	4 Extremo	4 Aceptar
5 Catastrófico	5 Casi certeza		

Fuente: Autores del proyecto.

Valoración del riesgo. La valoración del riesgo comprende a su vez: la identificación, análisis y evaluación del riesgo.

Identificación de riesgo. Una vez realizado el establecimiento del contexto (factores internos o externos) del departamento de sistemas, se buscan identificar los riesgos a gestionar, el objetivo de esta etapa es desarrollar una lista amplia de las fuentes de riesgos y eventos que tendrían impacto en el logro de cada uno de los objetivos identificados en el contexto. Como en el siguiente ejemplo:

Cuadro 5. Valoración y tratamiento de riesgos

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	1 de 7

Empresa o Dependencia:	Sistemas					
Responsable:	Directos de Sistemas					
IDENTIFICACIÓN DE RIESGOS						
Clasificación	**Riesgo**	**Fuente de Riesgo**	**Área de Impacto**	**Evento**	**Causas**	**Consecuencias**
TECNOLÓGICOS	Caída de la comunicación por fallas del enlace principal	*Eventos naturales *Aspectos tecnológicos y técnicos	*Comportamiento organizacional *Costo *Imagen	Presencia fallas en las comunicaciones (redes) de la empresa generado alteración en el desarrollo de las operaciones	1. Falta de disponibilidad del servicio por parte del proveedor.	1. Perdida de la imagen de la empresa ante el público.
					2. Ausencia de un enlace de contingencia con otro proveedor.	2. Alteración de la operación.
					3. Vida útil de los equipos de comunicaciones.	3. Aumento de los tiempos de respuesta del sistema de información.

Cuadro 5. (Continuación)

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	2 de 7

IDENTIFICACIÓN DE RIESGOS						
Clasificación	**Riesgo**	**Fuente de Riesgo**	**Área de Impacto**	**Evento**	**Causas**	**Consecuencias**
TECNOLÓGICOS	Bajo rendimiento de la base de datos por una administración inadecuada.	*Comportamiento humano *Aspectos tecnológicos y técnicos	*Comportamiento organizacional *Costo *Imagen *Desempeño	Disminución del rendimiento del sistema por fallas en la base de datos.	1. Administración deficiente de la Base de Datos.	1. Interrupción en la prestación del servicio al cliente.
					2. No se tiene establecido un procedimiento de monitoreo y mantenimiento de la Base de Datos.	2. Aumento de los tiempos de respuesta del sistema de información.

Análisis y evaluación del riesgo. Una vez identificados los riesgos, se pretende analizar y evaluarlos de acuerdo a unos criterios preestablecidos, priorizando de esta manera los riesgos para posteriormente darles tratamiento. A continuación se plantea un ejemplo aplicando el análisis y evaluación de riesgos:

Cuadro 5. (Continuación)

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	3 de 7

ANÁLISIS Y EVALUACIÓN DE RIESGOS										
Controles Existentes	**Está Documentado**		**Se Aplica el Control**		**Minimiza el Riesgo**		**Calificación del Control**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**
	Si	**No**	**Si**	**No**	**Si**	**No**				
1. Se cuenta con cronogramas de mantenimiento preventivos de equipos de comunicación.	x		x		X		1	**MODERADO**	**PROBABLE**	**ALTO**
2. Se cuenta con máquinas móviles para la continuidad de la actividad comercial.	x		x		X		1			
3. Se cuenta con una consola de monitoreo de la red.	x		x		X		1			

Cuadro 5. (Continuación)

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	4 de 7

ANÁLISIS Y EVALUACIÓN DE RIESGOS										
Controles Existentes	**Está Documentado**		**Se Aplica el Control**		**Minimiza el Riesgo**		**Calificación del Control**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**
	Si	**No**	**Si**	**No**	**Si**	**No**				
1. Se cuenta con un administrador de la base de datos (DBA).	x		x			x	3	**MAYOR**	**CASI CERTEZA**	**EXTREMO**
2. Se cuenta con una consola para el monitoreo de la base de datos que genera notificaciones mediante correo electrónico sobre: incremento de sesiones activas, caída del servicio o bloqueos.	x		x			x	3			

Tratamiento del riesgo. Una vez valorados los riesgos, se identifican opciones para tratar los riesgos, se evalúan y se preparan planes para darles tratamiento y se implementan. A continuación se plantea un ejemplo aplicando el tratamiento de riesgos:

Cuadro 5. (Continuación)

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	5 de 7

TRATAMIENTO DE RIESGOS					
Opción de Tratamiento	**Acciones Propuestas**	**Responsable**	**Recursos y/o Requisitos**	**Tiempo o Fecha de Ejecución**	**Periodicidad del Monitoreo**
MITIGAR	1. Realizar revisiones periódicas del enlace principal de comunicación y de las redes de comunicación.	Administrador de la Red.	*Redes comunicación. *Enlace comunicación. * Recurso Humano.	22-01-2015	Mensual
	2. Diseñar, documentar e implementar un procedimiento de mantenimiento preventivo de los equipos de comunicación y redes de comunicación.	Administrador de la Red.	*Equipos de comunicación. *Redes comunicación. *Recurso Humano.	22-01-2015	Semestral
	3. Realizar un estudio de viabilidad para evaluar la adquisición e implementación de un enlace de comunicación adicional.	Director de sistemas.	*Recurso Humano. *Recurso económico.	22-01-2015	N/A

Cuadro 5. (Continuación)

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	6 de 7

TRATAMIENTO DE RIESGOS					
Opción de Tratamiento	**Acciones Propuestas**	**Responsable**	**Recursos y/o Requisitos**	**Tiempo o Fecha de Ejecución**	**Periodicidad del Monitoreo**
MITIGAR	1. Evaluar e implementar técnicas para mejorar el rendimiento de base de datos.	Administrador de la base de datos (DBA).	*Recurso Humano. * Recurso tecnológico.	22-01-2015	Semestral
	2. Redefinir las funciones del administrador de base de datos para una correcta administración de la misma.	Director de sistemas.	*Recurso Humano.	22-01-2015	Semestral

Cuadro 5. (Continuación)

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	7 de 7

SEGUIMIENTO RIESGO RESIDUAL												
Fecha de seguimiento	**Está Documentado**		**Se Aplica el Control**		**Minimiza el Riesgo**		**Calificación del Control**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**	**Opción de Tratamiento**	**Observaciones**
	Si	**No**	**Si**	**No**	**Si**	**No**						
26-01-2015	X		x		x		1	**MENOR**	**IMPROBABLE**	**BAJO**	**ACEPTAR**	Se acepta el riesgo
26-01-2015	X		x		x		1	**MENOR**	**POSIBLE**	**MEDIO**	**ACEPTAR**	Se acepta el riesgo

Elaborado Por: Director de Sistemas	Fecha: 14-01-2015
Revisado Por: Gestor de Riesgos	Fecha: 14-01-2015
Aprobado Por: Comité de Riesgos	Fecha: 14-01-2015

Fuente: Autores del proyecto.

Monitoreo y revisión. Una vez diseñado y validado el plan para gestionar los riesgos, es necesario monitorearlo teniendo en cuenta que no dejan de ser una amenaza para la organización. El monitoreo y la revisión debe ser una parte integral del proceso para la gestión del riesgo e incluir verificaciones continuamente. A continuación se plantea un ejemplo aplicando el monitoreo y revisión de los riesgos:

Cuadro 6. Monitoreo y Revisión de riesgos

MONITOREO Y REVISIÓN DE RIESGOS	Código:	F- GR- 04
	Versión:	1
	Elaborado:	12/01/2015
	Página:	1 de 1

MONITOREO Y REVISIÓN DE RIESGOS								
Riesgo	**Fecha**	**Logros**	**Justificación**	**Indicador**	**Reportado A**	**Existe Riesgo Emergente**		**Observaciones**
						Si	**No**	
Caída de la comunicación por fallas del enlace principal	27-01-2015	Se logra bajar el nivel del riesgo de alto a bajo	Actualmente se cuentan con el estudio de viabilidad, el procedimiento de mantenimiento y evidencias de las revisiones.	Indicador = Horas de suspensión del servicio/ Total horas de servicio * 100%	Gerente		X	Se efectuó el monitoreo de los riesgos
Bajo rendimiento de la base de datos por una administración inadecuada.	27-01-2015	Se logra bajar el nivel del riesgo de extremo a medio	Las funciones del DBA fueron redefinías y se implementaron técnicas que mejoraron el rendimiento de la BD.	Indicador = Horas de suspensión del servicio/ Total horas de servicio * 100%	Gerente		x	Se efectuó el monitoreo de los riesgos

Elaborado Por: Director de Sistemas	Fecha: 27-01-2015
Revisado Por: Gestor de Riesgos	Fecha: 27-01-2015
Aprobado Por: Comité de Riesgos	Fecha: 27-01-2015

Fuente: Autores del proyecto.

4.4 PRESENTACIÓN Y SOCIALIZACIÓN DE LA GUÍA DE GESTIÓN DE RIESGOS.

Objetivo: Socializar la guía de gestión de riesgos al personal del departamento de sistemas de la empresa Apuestas Cúcuta 75.

Para alcanzar este objetivo se planteó la siguiente actividad.

- Actividad 1: Reunir al personal de sistemas y socializar la guía para la gestión de riesgos.

Socializar la guía al personal del área de sistemas, radica en la importancia de su ejecución y constante aplicación en los diferentes procesos de la organización y especialmente del departamento de sistemas.

La presentación le otorgó al equipo la capacidad de visibilizar posibilidades de riesgo a las que no se les había proporcionado suficiente consideración; además de poner en común la importancia de gestionar esta clase de eventualidades, hechos que al ser descubiertos cobraban inconvenientes en este departamento que es reconocido como uno de los más importantes de Apuestas Cúcuta 75.

Al evaluar esta actividad (ANEXO B), no solo se está valorando el diseño de la guía, también la claridad, el entendimiento y la disposición para aplicarla en su área de trabajo y sobre todos los procesos. Los funcionarios del departamento de sistemas de apuestas Cúcuta 75 (ANEXO C) se mostraron complacidos y dispuestos a darle visibilidad a los riesgos de su área para tratarlos oportunamente, logrando así fortalecer la continuidad del negocio y la satisfacción de sus públicos objetivo.

5. CONCLUSIONES

El desarrollo del proyecto permitió la identificación de estándares, normativas y técnicas especializadas para la valoración e implementación de acciones para dar tratamiento a los riesgos.

Se consolidaron conocimientos sobre la gestión de riesgos, logrando aplicarlo a un rango de actividades, decisiones, operaciones, procesos, funciones, proyectos, productos, servicios, activos, departamentos u organizaciones.

El diseño de la guía para la gestión de riesgos permitió establecer un marco teórico práctico sobre la gestión de riesgos como mecanismo de control y mejoramiento del departamento de sistemas de la empresa Apuestas Cúcuta 75.

6. RECOMENDACIONES

Implementar la guía de gestión del riesgo en el departamento de sistemas de la empresa Apuestas Cúcuta 75.

Es necesario elaborar programas de formación, capacitación y entrenamiento sobre gestión de riesgos en pro del mejoramiento continuo.

Lograr el apoyo y respaldo por parte de los altos directivos de Apuestas Cúcuta 75 a los directores, jefes o líderes de áreas al proceso de gestión de riesgos.

Realizar evaluaciones periódicas al proceso de gestión de riesgos que permita medir la eficacia del proceso.

Socializar la guía para la gestión de riesgos con los jefes de procesos de los demás departamentos de la organización en pro del mejoramiento continuo.

Establecer coordinaciones entre las diferentes dependencias de Apuestas Cúcuta 75 para la ejecución compartida de las acciones de disminución de riesgos.

BIBLIOGRAFÍA

BANCO CENTRAL DE URUGUAY. Estándar australiano administración de riesgos. AS/NZS 4360:1999. Montevideo: BCU, 1999. 36 p.

COSTA SANTOS, Jesús. Seguridad informática. Bogotá: Ediciones de la U, 2011.

DE LARA, A. Medición y control de riesgos financieros. México: Limusa, 2005. 219 p.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Cartillas de Administración pública [en línea]. [Citado 20 octubre 2014]. Disponible en Internet en: http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=558.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la Administración del riesgo. 4 ed. Bogotá: DAFP, 2011.

DIZ, E. Teoría de riesgo. 3 ed. Bogotá: Ecoe Ediciones, 2009. 181 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Compendio Sistema de Gestión de Seguridad de la Información –SGSI. Bogotá: Kimpress, 2010.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo, principios y directrices. NTC-ISO 31000. Bogotá: ICONTEC, 2011. 34 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo, Vocabulario. GTC 137:2011. Bogotá: ICONTEC, 2011.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana de Gestión del Riesgo. NTC-5254:2006. Bogotá: ICONTEC, 2006. 33 p.

JIMENO GARCÍA, María Teresa; MÍGUEZ PÉREZ, Carlos y MATAS GARCÍA, Abel Mariano. Hacker, guía práctica. Bogotá: Anaya, 2012. 368 p.

JORION, P. Valor en riesgo. México: Editorial Limusa, 2004. 357 p.

OSORIO RIVERO, Yenis Piedad y PÉREZ PÉREZ, Yesica Maria. Diseño de una política de gestión de riesgos de la información para la dependencia de admisiones registro y control de Universidad Francisco de Paula Santander Ocaña. Trabajo de Grado. Especialista en Auditoria de Sistemas. Ocaña: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Especialización en Auditoria de Sistemas, 2014.

UNIVERSIDAD DE ANTIOQUIA. Manual institucional de gestión de riesgos. Versión 2 [en línea]. [Citado 20 octubre 2014]. Disponible en Internet en: http://www.udea.edu.co/portal/page/portal/BibliotecaPortal/GestionAcademicoAdministrativa/SGC/Viceadministrativa/ElementosDiseno/Manuales/m-5200-001.pdf.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER. Guía para la evaluación metodológica de proyectos de investigación formativa. Ocaña: UFPS, 2012. 9 p.

VELÁSQUEZ PÉREZ, Torcoroma. Módulo de inducción. Ocaña: UFPS, 2012.

ANEXOS

Anexo A. Entrevista realizada al director de sistemas de la empresa Apuestas Cúcuta 75

ANEXO A. ENTREVISTA REALIZADA AL DIRECTOR DE SISTEMAS DE LA EMPRESA APUESTAS CÚCUTA 75

Fecha: 05-11-2014

Nombre del entrevistado: CARLOS PARRA

Cargo del entrevistado: DIRECTOR DE SISTEMAS

Nombre del entrevistador: ERIKA TATIANA QUINTERO QUINTERO

El objetivo de la entrevista es conocer el nivel de gestión de Riesgos implementado en el departamento de Sistemas de la empresa Apuestas Cúcuta 75

#	Pregunta	Respuesta
1	¿Las metas y los objetivos estratégicos de Apuestas Cúcuta 75 se comunican y las entienden todo el equipo del departamento de sistemas?	Si, estas son comunicadas a todo el personal del departamento de sistemas a través de capacitaciones y programas de formación.
2	¿Apuestas Cúcuta 75 (cuenta con políticas que describen la estandarización, medición, control y mejoras continuas) en los procesos del departamento de sistemas?	Si, han sido implementadas a través de la norma ISO 27001.
3	De acuerdo con su nivel de conocimiento y experiencia, ¿cuál es el objetivo principal del departamento de sistemas de Apuestas Cúcuta 75? ¿De qué manera podría medirse el impacto de la labor del departamento?	Mantener la continuidad de los operaciones, el impacto se pueden medir a través de indicadores que midan la disponibilidad del servicio.
4	¿Cuáles considera que son los procesos misionales del departamento de Sistemas de Apuestas Cúcuta 75? ¿Cuáles son los roles (cargos) responsables de realizar estas actividades?	Proceso de Desarrollo de Software y Administración de Red, el personal encargado de desempeñar estas funciones son los Programadores y administradores de la red

5	A su juicio, ¿cuáles son los cinco principales procesos que constituyen la esencia del departamento de sistemas?	-Proceso de desarrollo de software -Proceso de comunicaciones -Proceso mantenimiento de hardware.
6	La metodología de gestión de riesgos en el departamento de sistemas de Apuestas Cúcuta 75 es:	No existe una metodología de gestión de riesgos
7	¿El departamento de sistemas utiliza técnicas de gestión del riesgo para medir y evaluar el impacto del riesgo durante la ejecución de sus operaciones?	No, ya que no existe una metodología para su gestión.
8	¿Se cuenta con un plan de tratamientos razonable, acorde a la severidad de los riesgos asociados?	No, ya que no existe una metodología para la gestión de riesgos
9	¿Cómo Director de sistemas como apoya el proceso de gestión de riesgos?	Actualmente existen unos activos establecidos pero no se lleva a cabo programa de gestión de riesgos.
10	¿Cómo se comunican y se discuten la gestión de riesgos en las reuniones?	No se efectúa un proceso de comunicación porque no se lleva a cabo un proceso de gestión de riesgos.
11	¿Qué herramientas se utilizan para la valoración de los riesgos?	No, ya que no existe una metodología para la gestión de los riesgos

12	¿Cómo contribuye en la identificación de riesgos asociados al departamento de sistemas?	No existe un proceso formal de gestión de riesgos, motivo por el cual no existe una adecuada identificación de los mismos.
13	¿Para los proyectos que se realizan se hace alguna evaluación de riesgos o se implementa cuando se identifican los riesgos? ¿Existe un proceso definido?	No existe un proceso definido para la gestión de riesgos.
14	¿Cómo se realiza el proceso de registro de riesgos detectados en el departamento de sistemas?	No existe una adecuada registro de riesgos puesto que no existe un proceso formal.
15	¿Cómo es el mecanismo empleado para la evaluación de riesgos?	No existe un mecanismo para la gestión de riesgo por lo cual no se realiza una valoración adecuada.
16	¿Cómo participa usted en el proceso de valoración de riesgos?	No se efectúa un proceso de valoración de riesgos.

Firma del Entrevistado

Anexo B. Evaluación de la socialización

EVALUACIÓN DE LA SOCIALIZACIÓN	Código:	F- GR- 06
	Versión:	01
	Elaborado:	12-01-2015
	Página:	1 de 1

CAPACITACION: INTEGRACION: OTRO: EVALUACIÓN SOCIALIZACIÓN

NOMBRE DE LA ACTIVIDAD: EVALUACIÓN SOCIALIZACIÓN FECHA: 17-01-2015

NOMBRE DEL INSTRUCTOR: ERIKA TATIANA QUINTERO, SANDRA LILIANA ASCANIO, KARINA CARDENAS ESTUPIÑAN

De acuerdo a la socialización brindada deseamos conocer su opinión, escriba al frente de cada aspecto la calificación que desea darle de 1 a 5, según la escala explicada a continuación. Realice cualquier observación, sugerencia o recomendación que considere necesaria, su opinión es muy importante para nosotros.

ESCALA DE CALIFICACIÓN

1 - Malo	2 - Regular	3 - Aceptable	4 - Bueno	5 - Excelente

No.	ASPECTO	CALIFICACIÓN
1	CONOCIMIENTOS DEL INSTRUCTOR	5
2	CAPACIDAD PARA ENSEÑAR	4
3	ACTITUD DEL INSTRUCTOR FRENTE AL GRUPO	5
4	CONTENIDO DE LA SOCIALIZACIÓN	5
5	¿LE GUSTÓ EL MÉTODO DE ENSEÑANZA?	4

	TOTAL ASPECTOS EVALUADOS	TOTAL	5
		CALIFICACIÓN PROMEDIO	4.6

Comentarios y/o sugerencias: Se recomienda la implementación de la guía para la gestión de riesgos en el departamento de sistemas para una adecuada gestión de los mismos como mecanismo preventivo.

NOMBRE DE LA PERSONA QUE DILIGENCIA LA EVALUACION: Carlos Parra
CARGO: Practica Proceso Sistemas

1. ¿EXPLIQUE CUÁL FUE EL TEMA DE LA SOCIALIZACIÓN?:
Guía para la gestión de riesgos donde se expuso los lineamientos, factores técnicos como conceptuales para la adecuada gestión de los riesgos, junto con los formatos y ejemplos aplicados durante cada una de las etapas del proceso gestión.

2. ¿DESCRIBA QUE ASPECTOS LE QUEDARON CLAROS DE LA SOCIALIZACIÓN?
- Los formatos utilizados en cada uno de los capítulos del proceso de gestión son claros, estan bien y facil su diligenciamiento.
- Proceso de gestion de riesgos

3. ¿EN QUE CONTRIBUYE EL TEMA O OBJETIVOS CON EL DESEMPEÑO DE SU TRABAJO?
- garantizar la seguridad de la información
- implementar acciones ante cualquier evento que se presente

4. ¿EN QUÉ TEMA DE LA CAPACITACIÓN NECESITA REFUERZOS?
Ninguno

SOLO PARA EL CAPACITADOR: (CALIFICAR DE 1 A 5) TOTAL DE LA EVALUACION: 4.5

Anexo C. Listado de asistencia

LISTADO DE ASISTENCIA	Código:	F- GR- 05
	Versión:	01
	Elaborado:	12-01-2015
	Página:	1 de 1

FECHA: 19-01-2015

TEMA: SOCIALIZACIÓN GUÍA PARA LA GESTIÓN DE RIESGOS

MODERADOR: ERIKA TATIANA QUINTERO QUINTERO, SANDRA LILIANA ASCANIO, YURAIMA KARINA CARDENAS ESTUPIÑAN

CAPACITACION: X

CONFERENCIA:

REUNION:

ACTIVIDAD:

NOMBRE	CARGO	FIRMA
FRANK MORALES	ING. DESARROLLADOR MASTER	
EDGAR LEÓN	ING. DESARROLLADOR MASTER	
FABIO ROJAS	ING. DESARROLLADOR JUNIOR	
CARLOS PARRA	DIRECTOR DE SISTEMAS	
RUBÉN RONQUILLO	TECNÓLOGO DE SISTEMAS	
HUMBERTO GUTIERREZ	TÉCNICO DE SISTEMAS MASTER	
FREDY CRUZ	TECNICO DE REDES JUNIOR	
MICHELT DAW	ADMINISTRADOR DE RED	MICHELT DAW
JULIO CONTRERAS	TECNICO DE REDES JUNIOR	
EDISON RIVERA	TECNICO DE REDES JUNIOR	
ERIKA ARBOLEDA	TÉCNICO DE MANTENIMIENTO	Erika Arboleda
YAMID MOLINA	TÉCNICO DE MANTENIMIENTO	Yamid Molina
LUIS EDUARDO NAVARRO	TECNICO DE REDES SENIOR	

Anexo D. Guía de riesgos

APUESTAS CÚCUTA 75
J.J.PITA & CIA. S.A.
¡Su chance legal!

GUIA PARA LA GESTIÓN DE RIESGOS

APUESTAS CÚCUTA 75

PRESENTACIÓN

La guía para la gestión de riesgos del departamento de sistemas de Apuestas Cúcuta 75, establece un marco teórico y conceptual sobre la gestión como mecanismo de control y mejoramiento de la organización, describiendo los pasos a seguir para gestionar los riesgos identificados en cualquier nivel o ámbito de aplicación (estratégico, tecnológico, operativo, financiero o de cumplimiento) que pueden afectar el logro de los objetivos organizacionales.

CONTENIDO

INTRODUCCIÓN

La gestión del riesgo cobra mayor importancia para las organizaciones de hoy, dado el dinamismo y los constantes cambios que el mundo globalizado exige. Estos cambios hacen que dichas entidades deban enfrentarse a factores internos y externos que pueden crear incertidumbre sobre el logro de sus objetivos. Así el efecto que dicha incertidumbre tiene en los objetivos de una organización se denomina "riesgo"[10].

Las tendencias globales que desarrollan modelos de sistemas de gestión de calidad y de control, han incorporado al proceso administrativo la gestión de riesgos, permitiendo que al visualizarlos y tratarlos, disminuya la incertidumbre de las acciones en el alcance de los objetivos.

La guía contiene aspectos esenciales a considerar para gestionar riesgos, cuya base son los estándares ISO 31000 y ANZ 4360. Ésta muestra el marco normativo y conceptual, los pasos a seguir para la gestión de riesgos, el mapa de riesgos, la política de gestión de riesgos y el glosario de términos utilizados; pudiéndose aplicar a un rango de actividades, incluyendo estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

[10] Norma Técnica Colombiana NTC – ISO 31000.

1. GESTIÓN DEL RIESGO

La gestión de riesgos no es un tema nuevo, pues de alguna u otra manera, las organizaciones han desarrollado planes, programas y proyectos para dar un manejo adecuado a los riesgos, con el fin de lograr de manera eficiente el cumplimiento de sus objetivos y prepararse para cualquier eventualidad.

El riesgo y su manejo o control, puede considerarse fundamental en cualquier organización, por lo tanto es necesario introducir el concepto de gestión de riesgos en la empresa Apuestas Cúcuta 75 (J.J. PITA y CIA S.A.), basándose en qué todas las organizaciones independientemente de su naturaleza y tamaño están expuestas a riesgos que pueden afectar su existencia y permanencia.

1.1 ALCANCE

El diseño de la guía de gestión de riesgos se realiza para el departamento de sistemas, teniendo en cuenta los objetivos organizacionales, además de los mecanismos para esta clase de estrategia que identificará, analizará, evaluará y brindará tratamiento a los posibles riesgos del departamento.

1.2 APLICACIÓN

La gestión del riesgo como parte integral de las buenas prácticas es un proceso interactivo que consta de varios elementos, cuyo objetivo es permitir que la organización minimice pérdidas y maximice oportunidades. Su aplicación se basa en los paramentos y lineamientos planteados en la guía del departamento de sistemas, que contará con la participación de los funcionarios, espacios donde se establecerán mecanismos para identificar, analizar, evaluar y darles tratamiento a riesgos a los que se encuentran expuestos, alcanzando así la eficiencia y eficacia organizacional.

1.3 VENTAJAS DE LA GESTIÓN DEL RIESGO SEGÚN LA NORMA ISO 31000

La implementación y mantenimiento de una gestión del riesgo le permite a las organizaciones[11]:

- Aumentar la probabilidad de alcanzar los objetivos.
- Fomentar la gestión proactiva.
- Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización.
- Cumplir con los requisitos legales y reglamentarios pertinentes y con las normas internacionales.
- Mejorar la presentación de informes obligatorios y voluntarios.
- Mejorar la confianza y honestidad de las partes involucradas.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Mejorar los controles.
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
- Mejorar la eficacia y la eficiencia operativa.
- Incrementar el desempeño de la salud y la seguridad, así como la protección ambiental.
- Mejorar la prevención de pérdidas y la gestión de incidentes.
- Minimizar las pérdidas.
- Mejorar el aprendizaje organizacional.
- Mejorar la flexibilidad organizacional.

[11] Norma Técnica Colombiana NTC-ISO 31000.

2. POLÍTICA DE GESTIÓN DEL RIESGO

La gestión de riesgo en Apuestas Cúcuta 75 J.J. (PITA y CIA S.A.) tendrá como propósito garantizar el cumplimiento de la misión, fomentar en mayor grado la cultura del autocontrol y autoevaluación como herramientas de gestión para lograr buenas prácticas, que logren resolver con calidad las necesidades de la organización y el logro de los objetivos organizacionales y misionales.

Las políticas son los controles establecidos, que identifican las opciones para tratar y manejar los riesgos con base en su valoración y permiten tomar decisiones adecuadas para evitar, reducir, compartir, transferir o asumir riesgos.

2.1 OBJETIVOS

- Mejorar la seguridad de Apuestas Cúcuta 75 (J.J. PITA y CIA S.A.) a través de la gestión del riesgo en el departamento de sistemas.

- Generar una visión integral sobre el análisis, identificación, evaluación y tratamiento del riesgo mediante el desarrollo de procesos de formación y capacitación.

- Involucrar a todos los funcionarios en la búsqueda de acciones efectivas encaminadas a prevenir y gestionar los riesgos.

2.2 RESPONSABLES

- Comité de Gestión de Riesgos, es el encargado de evaluar y aprobar las políticas, mecanismos y procedimientos de riesgos implementados, así como recomendar las medidas o ajustes a los que haya lugar.

- El Gestor de Riesgos, en representación del Comité de Riesgos, lidera el proceso de gestión del riesgo en la empresa.

- Los directores o jefes de procesos, son los encargados de realizar la gestión de riesgos en sus áreas bajo el acompañamiento del Gestor de Riesgos.

- Empleados y terceros, tienen la responsabilidad de participar activamente en el proceso de gestión de riesgos de la empresa.

2.3 SOPORTE METODOLÓGICO

La elaboración de la guía de gestión de riesgos para el departamento de sistemas de la empresa Apuestas Cúcuta 75 (J.J. PITA y CIA S.A.), se rige por los parámetros y lineamientos metodológicos para la gestión de riesgos, en concordancia con los estándares ISO 31000 y ANZ 4360.

2.4 RECURSOS

La asignación de los recursos necesarios para el desarrollo y gestión del riesgo se realizará en coordinación con los altos directivos de la organización y la dependencia financiera.

2.5 APROBACIÓN DE POLÍTICAS Y CONTROLES

Las medidas de tratamiento que generen cambios significativos dentro de la estructura organizacional serán evaluadas y aprobadas por el Comité de Gestión de Riesgos.

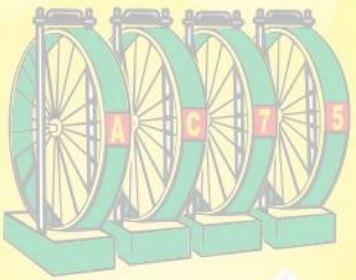
2.6 COMUNICACIÓN DE LAS POLÍTICAS Y CONTROLES

Dentro de los programas de formación y capacitación de la empresa estará incluida la gestión del riesgo, temática que será sensibilizada por el Gestor de Riesgos (políticas, procedimientos, controles, etc.).

2.7 EVALUACIÓN Y MEJORA

El Comité de Gestión de Riesgos, el Gestor de Riesgos y los directores o jefes de procesos son los responsables de realizar la verificación de la efectividad de la gestión del riesgo e identificar y aplicar acciones de mejora que optimicen el tratamiento del riesgo.

La evaluación constante del proceso de gestión de riesgos, permite la generación de acciones de mejora para aumentar la eficiencia, eficacia y efectividad de los procesos.



3. NORMATIVA

Los lineamientos del marco normativo relacionados con la gestión del riesgo tienen como base un conjunto de leyes, decretos, resoluciones y normativas que definen y orientan su estudio y aplicación. El riesgo y su gestión se fundamentan en el siguiente marco normativo.

3.1 LEY 87 DE 1993

Mediante esta Ley se desarrollan los artículos constitucionales 209 y 269. En su artículo 2 se definen los objetivos del Sistema de Control Interno y dentro de éste, los literales a) y f) que establecen: "a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten y f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos".

3.2 DECRETO 4485 DE 2009

Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) "establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

3.3 LEY 1474 DE 2011

Estatuto Anticorrupción. Artículo 73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.

3.4 NORMA TÉCNICA COLOMBIANA

Norma para la "Gestión de Riesgo" NTC 5254 de 2006.

Norma para la "Gestión de Riesgo" NTC 31000 de 2011.

Guía "Gestión del Riesgo - Vocabulario" GTC 137.

4. GLOSARIO

La gestión de riesgos implica conocer algunas definiciones que amplíen los conocimientos sobre el tema. A continuación se definen de manera clara y sencilla los términos relacionados con la gestión del riesgo los cuales fueron tomados de los estándares ISO 31000, ANZ 4360 y GTC 173.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos organizacionales.

Gestión del riesgo: Es la capacidad que tiene la organización para emprender las acciones necesarias que le permitan el manejo de eventos que puedan afectar negativamente el logro de los objetivos organizacionales y protegerla de los efectos ocasionados por su ocurrencia.

Proceso para la gestión del riesgo: Aplicación sistemática de las políticas, procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.

Partes involucradas: Son las organizaciones y las personas que puedan afectar, ser afectadas por una decisión o actividad (clientes, proveedores, empleados).

Valoración del riesgo: Elemento de control que determina el nivel o grado de exposición de la organización al impacto del riesgo, permitiendo estimar prioridades para su tratamiento mediante la aplicación de acciones tendientes a evitar, reducir, compartir o asumir el riesgo residual.

Identificación del riesgo: Elemento de control que posibilita conocer los eventos potenciales que ponen en riesgo el logro de los objetivos, estableciendo su descripción, agentes generadoras, causas y los efectos de su ocurrencia.

Fuente de riesgo: Constituyen los objetos o sujetos que tienen la capacidad de generar u originar un riesgo.

Consecuencias: Constituyen los efectos de la ocurrencia del riesgo sobre los objetivos de la empresa. Generalmente se dan sobre las personas o bienes con efectos muy importantes como daños físicos, fallecimientos, sanciones, pérdidas económicas, perdida de información, interrupción del servicio, daño ambiental, pérdida de imagen, pérdida de credibilidad y confianza.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Probabilidad: Es la posibilidad de que ocurra un evento específico o resultado, medido por la frecuencia y factibilidad de ocurrencia del riesgo, es expresado de manera cualitativa y cuantitativa.

Análisis del riesgo: Es el uso sistemático de información disponible para determinar con qué frecuencia un determinado evento puede ocurrir y la magnitud de sus consecuencias.

Criterio del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad.

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Tratamiento de riesgos: Selección e implementación de opciones apropiadas para tratar el riesgo.

Control: Son las políticas, procesos, prácticas u otras acciones que actúan para eliminar o minimizar los riesgos o maximizar oportunidades.

Riesgo residual: Se refiere al margen o residuo del riesgo que puede darse a pesar de las medidas de tratamiento tomadas para la gestión del riesgo.

Monitoreo: Comprobar, supervisar, observar cítricamente o registrar el progreso de una actividad, acción en forma sistemática para identificar cambios.

Mitigación: Planificación y ejecución de medidas dirigidas a reducir o minimizar los riesgos.

Transferir riesgos: Cambiar la responsabilidad o carga por las pérdidas a una tercera parte mediante legislación, contrato, seguro u otros medios. También se puede referir a cambiar un riesgo físico o parte del mismo a otro sitio.

5. PROCESO PARA LA GESTIÓN DEL RIESGO

En los estándares ISO 31000 y ANZ 4360 se encuentran establecidos los argumentos que soportan la necesidad de la implementación de un sistema integral de gestión de riesgos, que permitirá a la organización evaluar eventos negativos internos como externos que pueden afectar o impedir el logro de los objetivos organizacionales, así como los eventos positivos, que permitirán identificar oportunidades para un mejor cumplimiento de su misión, a través de la interrelación de los elementos de control que lo conforman.

La adecuada gestión de los riesgos favorece el desarrollo y crecimiento de la organización, para asegurar esto es importante que se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de tratamiento de los riesgos, así como su revisión, monitoreo y el proceso de comunicación, esto en desarrollo de los siguientes elementos de control:

- Comunicación y consulta.
- Establecimiento del contexto.
- Identificación del riesgo.
- Análisis del riesgo.
- Evaluación del riesgo.
- Tratamiento del riesgo.
- Monitoreo y revisión.

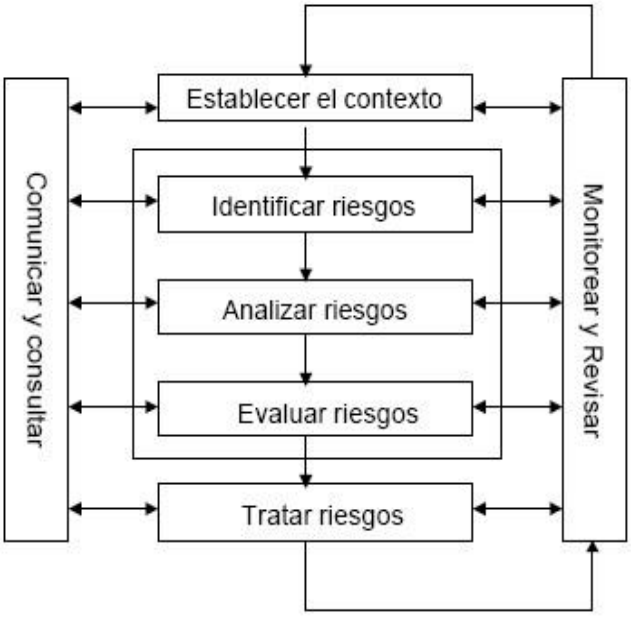


Figura 1. Proceso para la Gestión del Riesgo.

La gestión de riesgos se puede aplicar en diversos ámbitos de una organización, en los niveles estratégico, táctico y operacional, también en proyectos, tomas de decisiones específicas o para mejorar áreas reconocidas de riesgo.

5.1 COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas (internas o externas), es un proceso bidireccional que debe realizarse durante todas las etapas del proceso de gestión del riesgo. Por lo tanto, se deben desarrollar planes para la comunicación y la consulta, dado que sus puntos de vista pueden tener un impacto significativo en las decisiones que se tomen.

El plan para la comunicación y la consulta debe contener los aspectos relacionados con los riesgos, sus causas, consecuencias y tratamiento, así como los participantes, sus perspectivas y opiniones.

La comunicación y consulta podrá realizarse de manera digital a través de correo electrónico o física mediante formatos impresos.

La comunicación y la consulta son importantes porque:

- ✓ Hace la gestión explicita y relevante.
- ✓ Agrega valor a la organización.
- ✓ Integra las perspectivas.
- ✓ Desarrolla confianza.
- ✓ Mejora la determinación y el tratamiento efectivo del riesgo.

Un equipo consultor puede:

- ✓ Ayudar a establecer el contexto.
- ✓ Garantizar que se entiendan y se tomen en cuenta las decisiones de las partes involucradas.
- ✓ Ayudar a garantizar que los riesgos sean correctamente identificados.
- ✓ Reunir diferentes áreas expertas para analizar los riesgos.
- ✓ Asegurar la aprobación y el soporte para el plan de tratamiento.
- ✓ Fomentar la gestión adecuada del cambio durante el proceso de gestión del riesgo.
- ✓ Desarrollar un plan adecuado de comunicación y consulta externo e interno.

Para la realización de la comunicación y consulta ver **Anexo A. Formato de comunicación y consulta de riesgos.**

5.2 ESTABLECIMIENTO DEL CONTEXTO

El establecimiento del contexto comprende articular los objetivos de la organización, definir los parámetros internos (contexto interno) y externos (contexto externo) a considerar al gestionar el riesgo (contexto para la gestión del riesgo) y establece el alcance y los criterios (criterios del riesgo) contra los cuales se evaluarán los riesgos y se definirá la estructura del análisis.

5.2.1 Contexto Externo

Analiza los aspectos más relevantes del entorno, y busca brindar una apreciación amplia de todos los factores que pueden influir en la capacidad de la organización para lograr sus objetivos, es importante tener en cuenta que el análisis y valoración de los siguientes factores facilitará la identificación de los riesgos y brindará la información necesaria para estimar el grado de exposición de los mismos.

El contexto externo puede incluir:

- ✓ El ambiente social, cultural, político, legal, financiero, tecnológico, económico, bien sea internacional, nacional, regional o local.
- ✓ Los impulsores claves que tienen impacto en los objetivos de la organización.
- ✓ Las relaciones con las partes involucradas externas y sus percepciones.

Entender el contexto es importante con el fin de garantizar que los objetivos y las preocupaciones de las partes involucradas externas se toman en consideración al desarrollar los criterios del riesgo

5.2.2 Contexto Interno

Analiza los aspectos internos de la organización, y busca apreciar los factores que pueden influir en la organización para lograr los objetivos.

El proceso para la gestión del riesgo debe estar alineado con la cultura, procesos, estructura y estrategia de la organización. El contexto interno es todo aquello dentro de la organización que pueda tener influencia en la forma en que se gestiona el riesgo.

El contexto interno puede incluir:

- ✓ Gobierno, estructura organizacional, funciones y responsabilidades.
- ✓ Políticas, objetivos y estrategias.
- ✓ Capacidades en términos de recursos y conocimientos.
- ✓ Las relaciones con las partes involucradas internas y sus percepciones.
- ✓ Cultura organizacional.
- ✓ Sistemas de información, flujos de información y procesos de toma de decisiones.

5.2.3 Contexto para la gestión de riesgos

Se recomiendan establecer los objetivos, estrategias, alcance y parámetros de las actividades de la organización, o de aquellas partes de la organización en donde se aplica el proceso para la gestión del riesgo. La gestión de riesgos debería ser llevada a cabo tomando en consideración los recursos necesarios, las responsabilidades y autoridades.

El contexto para la gestión de riesgos puede incluir:

- ✓ Definición de las metas y objetivos de las actividades de gestión del riesgo.
- ✓ Definición de responsabilidades del proceso de gestión de riesgos.
- ✓ Definición del alcance.
- ✓ Definición de actividades, procesos, funciones, proyectos, servicios o activos.
- ✓ Definición de las relaciones entre el proyecto, proceso o actividad.
- ✓ decisiones.
- ✓ Definición de la metodología para la valoración del riesgo.

5.2.4 Definir los criterios del riesgo

En esta etapa se deben definir los criterios contra los cuales se va evaluar el riesgo. Los criterios del riesgo deben ser consistentes con la política para la gestión del riesgo de la organización. Deben ser definidos antes de iniciar el proceso de gestión de riesgos y ser revisados continuamente.

Los criterios del riesgo deben incluir:

- ✓ La naturaleza y los tipos de causas, consecuencias, y la forma en que se van a medir.
- ✓ Cómo se va definir la probabilidad.
- ✓ Cómo se va determinar el nivel del riesgo.
- ✓ Los puntos de vista de las partes involucradas.
- ✓ El nivel en el cual el riesgo se torna aceptable o tolerable.

Según lo mencionado anteriormente se recomienda hacer una clasificación de los riesgos, de la siguiente manera:

Tabla 1. Clasificación de los riesgos.

Clasificación	Descripción	Escenario de Riesgos
Social/Cultural	Se refiere a las condiciones de riesgos asociadas a un grupo expuesto, desde el punto de vista sectorial, social o cultural.	Comunidades locales, personas, sociedad, grupos sociales, entre otros.
Operativo	Afectan los procesos misionales de la organización, comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información, de la definición de los procesos y la estructura organizacional.	Fallas negligentes o involuntarias de las obligaciones frente a los clientes, ejecución y administración de procesos.
Financiero/Económico	Afectan los recursos financieros, económicos y logísticos de la organización, donde se incluye la planeación y ejecución presupuestal, elaboración de estados financieros, pagos, manejos de bienes, contratación, etc.	Aspectos económicos y financieros.
Legal/Político	Se relacionan con la capacidad de la organización para cumplir con los requisitos legales, contractuales, de transparencia y en general con su compromiso ante la comunidad.	Aspectos legales, contractuales, políticos, acuerdos, entre otros.
Técnico/Tecnológico	Se asocian con la capacidad tecnológica de la organización, de tal manera que satisfaga las necesidades actuales, futuras y soporten el cumplimiento de la misión.	Aspectos tecnológicos y técnicos.
Ambiental	Se refiere a las condiciones de riesgo asociadas a factores ambientales y climáticos.	Aspectos ambientales y climáticos (inundaciones, incendios, sismos, ruidos, contaminación, entre otros).

El establecimiento del contexto es la base para la identificación de los riesgos asociados a los objetivos de los procesos. El análisis se realiza a partir del conocimiento de situaciones del entorno (internas y externas) de la organización y la aplicación de varias herramientas técnicas como la matriz (DOFA), análisis de factores (PESTA), inventario de eventos, talleres de trabajo, análisis de flujo de procesos, entre otras.

- **MATRIZ DOFA**

Es una herramienta que permite generar un cuadro de la situación actual de la organización, permitiendo de esta manera obtener un diagnóstico preciso que permita en función de ello tomar decisiones acordes con los objetivos y políticas formuladas.

De estas cuatro variables, fortalezas y debilidades se refieren a aspectos internos de la organización, por lo que posible actuar directamente sobre ellas. En cambio, las oportunidades y las amenazas se refieres a factores externos, por lo que en general resulta difícil poder modificarlas.

Debilidades: Son aquellos factores que provocan una posición desfavorable frente a la competencia. Recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente, etc.

Amenazas: Son aquellas situaciones que provienen del entorno y que pueden llegar a atentar incluso contra la permanencia de la organización.

Fortalezas: Son las capacidades especiales con las que cuenta la organización y por las que posee una posición privilegiada frente a la competencia. Recursos que se controlan, capacidades y habilidades que se poseen, actividades que se desarrollan positivamente, etc.

Oportunidades: Son aquellos factores que resultan positivos, favorables, explotables, que se deben descubrir en el entorno en el que actúa la organización, y que permiten obtener ventajas competitivas.

- **PESTA**

Es una herramienta de gran utilidad con la cual se organizan los aspectos más relevantes del entorno y la forma en que pueden afectar la viabilidad futura; reconoce cinco grandes factores que se deben tener en cuenta cuando se planea un nuevo proyecto o se modifica un negocio.

Está compuesto por las iniciales de factores Políticos, Económicos, Sociales, Tecnológicos y Ambientales, los cuales le dan una estructura lógica que permite entender, presentar, discutir y tomar decisiones.

Político/Legal: Regulaciones estatales y gubernamentales, lineamientos de las comunidades, normas, deberes y derechos.

Económico: Presupuesto, finanzas, inversión, equipamientos.

Social: Género, clases sociales, pobreza, salud, desempleo, vivienda, educación, incluyendo los aspectos culturales, orden público, seguridad, tranquilidad, salubridad, ornato, ecología y violencia.

Tecnología: Medios, equipos y comunicaciones, rapidez con que sobrevienen los cambios y actualizaciones tecnológicas.

Ambientales: Agrupa al conjunto de normas, regulaciones y permisos ambientales requeridos para operar.

- **INVENTARIO DE EVENTOS**

Son listas de eventos posibles utilizadas con relación a un proyecto, proceso o actividad determinada. Son útiles para asegurar una visión coherente con otras actividades similares dentro de la entidad.

- **TALLERES DE TRABAJO**

Habitualmente reúnen a funcionarios de diversos niveles. El propósito es aprovechar el conocimiento colectivo del grupo y desarrollar una lista de acontecimientos que están relacionados con un proceso, proyecto o programa.

- **ANÁLISIS DE FLUJO DE PROCESOS**

Representación esquemática de interrelaciones de ENTRADAS, TAREAS, SALIDAS Y RESPONSABILIDADES. Una vez realizado el esquema los eventos son analizados frente a los objetivos del proceso. Esta técnica puede utilizarse para tener una visión a cierto nivel de detalle del proceso analizado.

Para realizar el establecimiento del contexto ver **Anexo B. Formato de establecimiento del contexto,** basado en la herramienta PESTA.

5.3 VALORACIÓN DEL RIESGO

La valoración del riesgo es el proceso total de la identificación, análisis y evaluación del riesgo.

5.3.1 Identificación del Riesgo

Una vez realizado el establecimiento del contexto (factores internos y externos) de la organización, se buscan identificar los riesgos a gestionar, se debe hacer de una manera amplia utilizando un proceso sistemático bien estructurado, pues los riesgos potenciales que no se identifiquen en esta etapa pueden ser excluidos en un análisis posterior.

Los riesgos deben ser incluidos en esta identificación estén o no bajo control de la organización, ya que es la base del análisis de los riesgos la que permite avanzar hacia una adecuada implementación de políticas que conduzcan a su control; esta etapa constituye la fase más crítica dentro del proceso de gestión integral de riesgos.

Una manera de visualizar, conocer y entender la importancia de gestionar los riesgos, es a través de la utilización de un formato para su identificación, el cual contiene los siguientes elementos:

Concepto	Descripción	Ejemplo
Clasificación	Representa los diferentes tipos de riesgo.	Pueden clasificarse en estratégicos, operativos, técnicos, tecnológicos, financieros y de cumplimiento.
Riesgo	Representa la posibilidad de ocurrencia de un evento o suceso que pueda afectar el cumplimiento de los objetivos de la organización.	Fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.
Fuente de Riesgo	Constituye los sujetos u objetos que tienen la capacidad de originar o generar un riesgo; se podrían clasificar en	Cada fuente de riesgo tiene numerosos componentes, que pueden dar lugar a un riesgo. Las fuentes genéricas de riesgo incluyen: • Relaciones comerciales y legales:

	cinco categorías: personas, materiales, equipos, instalaciones y entorno.	Entre la organización y otras organizaciones (proveedores, arrendatarios, subcontratistas). • Circunstancias económicas: De la organización, país, internacionales como factores que contribuyen a esas circunstancias (tipos de cambio). • Comportamiento humano: Involucrados y no involucrados en la organización. • Eventos naturales. • Circunstancias políticas: Incluyendo cambios legislativos y factores que pueden influenciar a otras fuentes. • Aspectos tecnológicos y técnicos (internos o externos). • Actividades y controles gerenciales. • Actividades individuales.
Áreas de Impacto	Constituyen las posibles áreas sobre las cuales ocasionarán consecuencias provocadas por un hecho o actuación que afecta a un entorno o ambiente social o natural. Las áreas de impacto incluyen a las siguientes: base de activos y recursos de la organización, comunidad, desempeño, ambiente, entre otras.	Las áreas de impacto son o pueden ser las siguientes: • Base de activos y recursos de la organización, incluyendo al personal. • Ingresos y derechos. • Costos de las actividades, tanto directos como indirectos. • Personas. • Comunidad. • Desempeño. • Cronograma y programa de actividades.

		• El ambiente. • Intangibles tales como la imagen organizacional, gestos de buena voluntad, calidad de vida. • Comportamiento organizacional.
Evento	Representa un incidente o una situación, que ocurre en un lugar particular durante un intervalo de tiempo particular.	Comportamientos irregulares del personal del departamento de sistemas, que pueden afectar la moral, la ética, los principios y valores organizacionales para obtener beneficios personales.
Causas	Razones o motivos por los cuales se genera un riesgo. Influyen directamente en la probabilidad de ocurrencia de los eventos y tienen incidencia en el establecimiento de políticas para su disminución o eliminación, estas se complementan con las identificadas en el formato de contexto estratégico.	Incumplimiento de los protocolos de selección e incorporación de personal.
Consecuencias	Constituyen los efectos de la ocurrencia del riesgo sobre los objetivos de la organización; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimientos,	Investigaciones disciplinarias, penales, etc. Desprestigio de la imagen organizacional.

	sanciones, pérdidas económicas, de información, de imagen, de credibilidad y confianza, interrupción del servicio y daño ambiental.	

Tabla 2. Elementos de la identificación del riesgo.

La identificación de riesgos posibilita conocer los eventos que presentan algún grado de amenaza al logro de los objetivos trazados en la organización, con efectos desfavorables para sus partes interesadas, a partir de los cuales se analizan las causas y las consecuencias que se pueden presentar con su ocurrencia.

La identificación del riesgo pretende resolver los siguientes interrogantes:

- ✓ ¿Qué puede suceder?
- ✓ ¿Dónde puede suceder?
- ✓ ¿Cuándo puede suceder?
- ✓ ¿Por qué y cómo puede suceder?

5.3.2 Análisis de Riesgos

El Análisis de Riesgos es el proceso para comprender la naturaleza y determinar el nivel del riesgo. El análisis depende de la información obtenida en la fase de identificación de riesgos y proporciona las bases para la evaluación del riesgo.

El análisis de riesgos intenta contestar preguntas como:

- ✓ ¿Qué puede salir mal?
- ✓ ¿Cuál es la probabilidad que algo salga mal?
- ✓ ¿Cuáles serían las consecuencias de que algo salga mal?
- ✓ ¿Qué se puede hacer para reducir la probabilidad y las consecuencias de que algo salga mal?

El análisis de riesgos es una predicción del futuro, basándose en el pasado histórico y un análisis cuidadoso de los eventos; el análisis involucra prestar consideración a las fuentes de riesgos, sus consecuencias, sus probabilidades de ocurrencia y la identificación de factores que las afectan.

Las consecuencias y probabilidades deberían analizarse en el contexto de los controles existentes. Se recomienda llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

Dependiendo de las circunstancias, el análisis de riesgos puede ser cualitativo, semi-cuantitativo, o cuantitativo o una combinación de estos. En la práctica, a menudo se utiliza primero el análisis cualitativo para obtener una indicación general del nivel de riesgo. Luego puede ser necesario llevar a cabo un análisis cuantitativo más específico.

- **Análisis Cualitativo:** El análisis cualitativo consiste en evaluar cuál es el impacto y la probabilidad de ocurrencia de cada uno de los riesgos identificados.

- **Análisis semi-cuantitativo:** El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo. Se debe tener precaución con el uso del análisis semi-cuantitativo pues los

números seleccionados podrían no reflejar apropiadamente las relatividades, lo que podría conducir a resultados inconsistentes.

- **Análisis cuantitativo:** El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semi-cuantitativos). La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados.

- **Análisis de sensibilidad:** Dado que algunas de las estimaciones realizadas en el análisis cuantitativo son imprecisas, deberá llevarse a cabo un análisis de sensibilidad para comprobar el efecto de los cambios en los supuestos y en los datos.

Para la realización del análisis de riesgos se sugiere aplicar los siguientes pasos:

5.3.2.1 Identificación de controles existentes

Se requiere identificar los controles existentes (políticas, dispositivos, procedimientos, etc.) para controlar los riesgos. Para la identificación pueden utilizar herramientas o técnicas como: check lists, juicios basados en la experiencia y en los registros, diagramas de flujo, brainstorming, análisis de sistemas y análisis de escenarios, asimismo los enfoques tales como inspecciones y técnicas de auto-evaluación de controles.

- **Check Lists:** Las Check Lists, listas de control u hojas de verificación, son formatos creados para realizar actividades repetitivas, controlar el cumplimiento de una lista de requisitos o recolectar datos ordenadamente y de forma sistemática. Son herramientas útiles con un propósito específico: **realizar una serie de pasos sin que se olvide ninguno de ellos.**

- **Juicios basados en la experiencia y en los registros:** El juicio de expertos se define como una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones, así como los registros.

- **Diagramas de Flujo:** Un **diagrama de flujo** es una representación gráfica de un proceso. El diagrama de flujo ofrece una descripción visual de las actividades implicadas en un proceso mostrando la relación secuencial entre ellas, facilitando la

rápida comprensión de cada actividad y su relación con las demás, el flujo de la información y la existencia de bucles repetitivos.

- **Brainstorming:** Es una herramienta de trabajo grupal que facilita el surgimiento de nuevas ideas sobre un tema o problema determinado. La lluvias de ideas (Brainstorming), es una técnica de grupo para generar ideas.

- **Análisis de Sistemas:** Es la separación de las partes de un todo para conocer sus elementos, sus características representativas, así como sus interrelaciones.

- **Análisis de Escenarios:** Es la distinción del lugar, entorno o contexto donde se desarrolla los acontecimientos o eventos.

Criterios	Ponderación
No existen controles.	4
Los controles existentes no son efectivos.	3
Los controles existentes no están documentados, pero son efectivos.	2
Los controles están documentados, se aplican y son efectivos.	1

Tabla 3. Criterios y valoración de controles existentes.

5.3.2.2 Análisis De Consecuencias Y Probabilidad

Las consecuencias y probabilidades se evalúan en el contexto de los controles existentes. Se combinan para producir un nivel de riesgo y se pueden determinar utilizando análisis y cálculos estadísticos. Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular.

Para evitar prejuicios subjetivos cuando se analizan consecuencias y probabilidades, deberán utilizar las mejores técnicas y fuentes de información disponibles.

Se pueden incluir las siguientes fuentes de información:

- ✓ Registros anteriores
- ✓ Experiencias relevantes
- ✓ Investigaciones de mercado
- ✓ Opiniones y juicios de especialistas y expertos.

Las técnicas incluyen:

- ✓ Entrevistas estructuradas con expertos en el área de interés
- ✓ Utilización de grupos multidisciplinarios de expertos
- ✓ Evaluaciones individuales utilizando cuestionarios

Las consecuencias pueden ser estimadas a partir de estudios experimentales o datos del pasado, también pueden ser expresadas en términos de criterios operativos, técnicos, financieros, legales, sociales, humanitarios u otros. La forma en que se exponen las probabilidades, las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo, variarán de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de éste.

NIVEL	PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
A	Casi Certeza	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año.
B	Probable	Probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez en el último año.
C	Posible	Podría ocurrir en algún momento	Al menos una vez en los últimos 2 años.
D	Improbable	Pudo ocurrir en algún momento	Al menos una vez en los últimos 5 años.
E	Raro	Puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.

Tabla 4. Tabla de probabilidad.

NIVEL	PROBABILIDAD	DESCRIPCIÓN
1	Insignificante	Sin perjuicios, baja pérdida financiera
2	Menor	Tratamiento de primeros auxilios, liberado localmente se contuvo inmediatamente, pérdida financiera media
3	Moderado	Requiere tratamiento médico, liberado localmente contenido con asistencia externa, pérdida financiera alta
4	Mayor	Perjuicios extensivos, pérdida de capacidad de producción, liberación externa, sin efectos nocivos, pérdida financiera mayor
5	catastrófico	Muerte, liberación toxica externa con efectos nocivos, enorme pérdida financiera

Tabla 5. Tabla de consecuencia o impacto.

PROBABILIDAD	CONSECUENCIAS				
	Insignificante	Menor	Moderado	Mayor	Catastrófica
	1	2	3	4	5
(A) Casi Certeza	Alto	Alto	Extremo	Extremo	Extremo
(B) Probable	Medio	Alto	Alto	Extremo	Extremo
(C) Posible	Bajo	Medio	Alto	Extremo	Extremo
D) Improbable	Bajo	Bajo	Medio	Alto	Extremo
(E) Raro	Bajo	Bajo	Medio	Alto	Alto

Tabla 6. Matriz de análisis de riesgo.

5.3.3 Evaluación de riesgos

El propósito de la evaluación de riesgos es facilitar la toma de decisiones, basadas en los resultados de dicho análisis, acerca de cuáles riegos necesitan tratamiento y la prioridad para la implementación del tratamiento.

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 controles existentes.

De acuerdo a la matriz de análisis de riesgo se establece que los niveles de Riesgos Extremo y alto deberán ser tratados de manera inmediata, los niveles de Riesgo Medio se deben aplicar medidas que bajen el impacto y los niveles de Riesgos Bajos podrán ser asumidos pero requieren de una monitorización constante para evitar que suba de nivel.

PRIORIZACIÓN	NIVEL DE RIESGO	DESCRIPCIÓN
4	Extremo	Requiere acción inmediata.
3	Alto	Necesita atención de la alta gerencia, además de acciones de control y monitoreo permanente.
2	Medio	Debe especificarse responsabilidad gerencial y seguir aplicando los controles existentes y hacer monitoreo periódico.
1	Bajo	Se Administrará mediante procedimientos de rutina y se debe seguir aplicando los controles existentes y hacer monitoreo periódico.

Tabla 7. Priorización de riesgos.

Para realizar la valoración de riesgos ver **Anexo C. Formato de valoración y tiramiento de riesgos.**

5.4 TRATAMIENTO DEL RIESGO

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos. Una vez implementados, el tratamiento suministra controles o los modifica.

El tratamiento del riesgo implica un proceso cíclico de:

- ✓ Valoración del tratamiento del riesgo.
- ✓ Decidir si los niveles de riesgo residual son tolerables.
- ✓ Si no son tolerables, generar un nuevo tratamiento para el riesgo.
- ✓ Valoración de la eficacia de dicho tratamiento.

Con la etapa de tratamiento de riesgos se establece e implementan las acciones a tomar para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización. Dentro de las acciones a tomar encontramos principalmente: evitar, mitigar, transferir y aceptar.

Las opciones para el tratamiento del riesgo, pueden incluir las siguientes:

- ✓ Evitar el riesgo al decidir no iniciar o continuar la actividad que lo originó,
- ✓ Tomar o incrementar el riesgo para perseguir una oportunidad.
- ✓ Retirar la fuente de riesgo.
- ✓ Cambiar la probabilidad.
- ✓ Cambiar las consecuencias.
- ✓ Compartir el riesgo con una o varias partes.
- ✓ Retener el riesgo mediante una decisión informada.

Para llevar a cabo el tratamiento de riesgos se sugiere aplicar los siguientes pasos:

5.4.1 Selección de las opciones para el tratamiento del riesgo

Como parte del tratamiento se definen las posibles acciones a seguir sobre los riesgos y se establece un plan según la priorización previa que se realizó. Este plan debe definir recursos, responsabilidades y actividades teniendo en cuenta las posibles restricciones a nivel económico, legal, temporal, técnico, operativo, político, cultural y las demás que sean determinadas. Los controles que sean recomendados deben incluir un análisis costo-beneficio.

Se puede considerar y aplicar una cantidad de opciones para el tratamiento ya sea individual o en combinación.

Al seleccionar las opciones para tratar los riesgos, es importante considerar los valores y percepciones de las partes involucradas. Estas pueden tener impacto en el riesgo en otras partes de la organización o para otras partes involucradas, deben ser incluidas en las decisiones, ya que pueden ser más aceptables para algunas partes involucradas que para otras.

La opción de tratamiento que se le dará a los riesgos identificados será definida de acuerdo a la decisión de la Gerencia y a los Jefes de proceso, teniendo en cuenta la posibilidad de ocurrencia, el impacto, el valor del riesgo y datos históricos de sucesos que haya enfrentado la empresa.

OPCIÒN DE TRATAMIENTO	
EVITAR EL RIESGO	Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
MITIGAR EL RIESGO	Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.
TRANSFERIR EL RIESGO	Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.
ASUMIR EL RIESGO	Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Tabla 8. Opciones de tratamiento.

Durante esta etapa pueden surgir nuevos riesgos significativos o secundarios, por lo cual es necesario que el monitoreo sea parte integral del plan de tratamiento para garantizar la eficacia del mismo.

5.4.2 Preparación e implementación de los planes para el tratamiento del riesgo

El plan debe ser documentado y deben ser definidas las opciones de tratamiento seleccionadas a implementar; en este punto es importante que el plan sea consistente con las metas y objetivos en la parte de planificación del proceso de gestión, maneje tiempos acordes con los definidos al inicio y con el tiempo de vida útil de los activos, además de dar paso a la siguiente etapa de mejora continua. El plan de tratamiento debe definir los pasos detallados para gestionar los riesgos sin dejar espacio a nuevos posibles riesgos que ocurran como consecuencia de errores en la implementación de las acciones del tratamiento mismo.

Los planes de tratamiento deberían incluir:

- ✓ Las razones para la selección de las opciones de tratamiento.
- ✓ Los responsables de aprobar e implementar el plan.
- ✓ Acciones propuestas.
- ✓ Requisitos de recursos.
- ✓ Requisitos de monitoreo y reporte.
- ✓ Tiempo y cronograma.

Los responsables de tomar las decisiones y otras partes involucradas deben conocer la naturaleza y extensión del riesgo residual después del tratamiento del riesgo. Es importante que este se documente y someta a monitoreo, revisión y cuando así corresponda a tratamiento adicional.

Para realizar el tratamiento de riesgos ver **Anexo C. Formato de valoración y tratamiento de riesgos.**

5.4 MONITOREO Y REVISIÓN

Una vez diseñado y validado el plan para gestionar los riesgos, es necesario monitorearlo teniendo en cuenta que no dejan de ser una amenaza para la organización.

El monitoreo y la revisión debe ser una parte integral del proceso para la gestión del riesgo e incluir verificaciones continuamente. Es necesario monitorear los riesgos, la efectividad del plan de tratamiento y las medidas de control, las estrategias y el sistema de gestión que se establece para controlar la implementación y asegurar que las circunstancias cambiantes no alteren las prioridades del riesgo, es esencial que esta etapa se realice durante todo el proceso para asegurar que el plan de gestión se mantenga relevante.

El monitoreo debe estar a cargo de:

- Los responsables (directores o jefes) del proceso.
- El Comité de Gestión de Riesgos y el Gestor de Riesgos.

Su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.

El Gestor de Riesgos junto con el Comité de Gestión de Riesgos dentro de su función asesora, comunicará y presentará luego del seguimiento y evaluación sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

Los procesos de monitoreo y revisión deben comprender todos los aspectos del proceso para la gestión del riesgo con el fin de:

- ✓ Garantizar que los controles son eficaces y eficientes.
- ✓ Obtener información adicional para mejorar la valoración del riesgo.
- ✓ Analizar y aprender lecciones a partir de los eventos.
- ✓ Detectar cambios en el contexto externo e interno, criterios del riesgo y en el mismo riesgo que puedan exigir revisiones posteriores.
- ✓ Identificar riesgos emergentes.

Para realizar el monitoreo y revisión de riesgos ver **Anexo D. Formato de monitoreo y revisión de riesgos.**

BIBLIOGRAFÍA

BANCO CENTRAL DE URUGUAY. Estándar australiano administración de riesgos. AS/NZS 4360:1999. Montevideo: BCU, 1999. 36 p.

COSTA SANTOS, Jesús. Seguridad informática. Bogotá: Ediciones de la U, 2011.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Cartillas de Administración pública [en línea]. [Citado 20 octubre 2014]. Disponible en Internet en: http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=558.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la Administración del riesgo. 4 ed. Bogotá: DAFP, 2011.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Compendio Sistema de Gestión de Seguridad de la Información –SGSI. Bogotá: Kimpress, 2010.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo, principios y directrices. NTC-ISO 31000. Bogotá: ICONTEC, 2011. 34 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo, Vocabulario. GTC 137:2011. Bogotá: ICONTEC, 2011.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana de Gestión del Riesgo. NTC-5254:2006. Bogotá: ICONTEC, 2006. 33 p.

UNIVERSIDAD DE ANTIOQUIA. Manual institucional de gestión de riesgos. Versión 2 [en línea]. [Citado 20 octubre 2014]. Disponible en Internet en: http://www.udea.edu.co/portal/page/portal/BibliotecaPortal/GestionAcademicoAdministrativa/SGC/Viceadministrativa/ElementosDiseno/Manuales/m-5200-001.pdf.

ANEXOS

ANEXO A. FORMATO DE COMUNICACIÓN Y CONSULTA DE RIESGOS.

COMUNICACIÓN Y CONSULTA DE RIESGOS	Código:	F- GR- 01
	Versión:	01
	Elaborado:	12-01-2015
	Página:	1 de 3

COMUNICACIÓN Y COSULTA DE RIESGOS		
COMUNICANTE	**Fecha:**	**Empresa o Dependencia:**
	Nombre:	**Cargo:**
COMUNICADO	**Riesgo:**	
	Causas:	
	Consecuencias:	

COMUNICACIÓN Y CONSULTA DE RIESGOS	Código:	F- GR- 01
	Versión:	01
	Elaborado:	12-01-2015
	Página:	43 de 3

Valoración Riesgo

(I) Impacto

1	2	3	4	5

(P) Probabilidad

1	2	3	4	5

(N) Nivel Riesgo

1	2	3	4

Opción Tratamiento

1	2	3	4

ACCIONES/DECISIONES	FECHA	RESPONSABLE(S)

Conclusiones:

COMUNICACIÓN Y CONSULTA DE RIESGOS	Código:	F- GR- 01
	Versión:	01
	Elaborado:	12-01-2015
	Página:	3 de 3

Recomendaciones:

(I) Impacto	**(P) Probabilidad**	**(N) Nivel Riesgo**	**Opción Tratamiento**
1 Insignificante	1 Raro	1 Bajo	1 Mitigar
2 Menor	2 Improbable	2 Medio	2 Evitar
3 Moderado	3 Posible	3 Alto	3 Transferir
4 Mayor	4 Probable	4 Extremo	4 Aceptar
5 Catastrófico	5 Casi certeza		

ANEXO B. FORMATO DE ESTABLECIMIENTO DEL CONTEXTO.

ESTABLECIMIENTO DEL CONTEXTO	Código:	F- GR- 02
	Versión:	01
	Elaborado:	12-01-2015
	Página:	1 de 2

ESTABLECIMIENTO DEL CONTEXTO
Empresa o Dependencia:
Proceso:
Objetivo:
Alcance:
Responsable:
Recursos:
Relación:

DIAGNÓSTICO DEL CONTEXTO EXTERNO (FACTORES DE RIESGO) – AMENAZAS	
POLÍTICOS	**ECONÓMICOS**
SOCIALES	**TECNOLÓGICOS**
AMBIENTALES	

ESTABLECIMIENTO DEL CONTEXTO	Código:	F- GR- 02
	Versión:	01
	Elaborado:	12-01-2015
	Página:	2 de 2

DIAGNÓSTICO DEL CONTEXTO INTERNO (FACTORES DE RIESGO) – DEBILIDADES	
POLÍTICOS	**ECONÓMICOS**
SOCIALES	**TECNOLÓGICOS**
AMBIENTALES	

Elaborado Por:	Fecha:
Revisado Por:	Fecha:
Aprobado Por:	Fecha:

ANEXO C. FORMATO DE VALORACIÓN Y TRATAMIENTO DE RIESGOS.

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	47 de 4

Empresa o Dependencia:	
Responsable:	

IDENTIFICACIÓN DE RIESGOS						
Clasificación	**Riesgo**	**Fuente de Riesgo**	**Área de Impacto**	**Evento**	**Causas**	**Consecuencias**

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	2 de 4

ANÁLISIS Y EVALUACIÓN DE RIESGOS									
Controles Existentes	**Está Documentado**		**Se Aplica el Control**		**Minimiza el Riesgo**		**Calificación del Control**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**
	Si	**No**	**Si**	**No**	**Si**	**No**				

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	3 de 4

TRATAMIENTO DE RIESGOS					
Opción de Tratamiento	**Acciones Propuestas**	**Responsable**	**Recursos y/o Requisitos**	**Tiempo o Fecha de Ejecución**	**Periodicidad del Monitoreo**

VALORACIÓN Y TRATAMIENTO DE RIESGOS	Código:	F- GR- 03
	Versión:	1
	Elaborado:	12/01/2015
	Página:	4 de 4

SEGUIMIENTO RIESGO RESIDUAL											
Fecha de seguimiento	**Está Documentado**		**Se Aplica el Control**		**Minimiza el Riesgo**		**Calificación del Control**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**	**Opción de Tratamiento**	**Observaciones**
	Si	**No**	**Si**	**No**	**Si**	**No**						

Elaborado Por:	Fecha:
Revisado Por:	Fecha:
Aprobado Por:	Fecha:

ANEXO D. FORMATO DE MONITOREO Y REVISIÓN DE RIESGOS.

MONITOREO Y REVISIÓN DE RIESGOS	Código:	F- GR- 04
	Versión:	1
	Elaborado:	12/01/2015
	Página:	1 de 1

MONITOREO Y REVISIÓN DE RIESGOS								
Riesgo	**Fecha**	**Logros**	**Justificación**	**Indicador**	**Reportado A**	**Existe Riesgo Emergente**		**Observaciones**
						Si	**No**	

Elaborado Por:	Fecha:
Revisado Por:	Fecha:
Aprobado Por:	Fecha: