## RESUMEN – TRABAJO DE GRADO

| | |
|---|---|
| AUTOR | **LORENA TATIANA ACUÑA BARRERA**<br>**YINETH YURIZA PEINADO PACHECO** |
| FACULTAD | **FACULTAD DE INGENIERÍAS** |
| PLAN DE ESTUDIOS | **INGENIERÍA DE SISTEMAS** |
| DIRECTOR | **Esp. JOSÉ ALEXANDER SANTIAGO DURÁN** |
| TÍTULO DE LA TESIS | **GUÍA DE GESTIÓN DE RIESGOS PARA EL DEPARTAMENTO DE SISTEMAS DEL HOTEL TARIGUA OCAÑA S.A.S, BASADOS EN LA NORMA ISO/IEC 27001** |


**RESUMEN**
**(70 palabras aproximadamente)**

**EL ANÁLISIS DE RIESGOS CONSTITUYE UNA HERRAMIENTA IMPORTANTE PARA EL TRABAJO DEL EMPRESARIO, POR CUANTO IMPLICA EL DIAGNÓSTICO DE LOS MISMOS PARA VELAR POR SU POSIBLE MANIFESTACIÓN O NO, EL HOTEL TARIGUA DEBE TOMAR CONCIENCIA DE LA NECESIDAD DE ALINEAR SUS OBJETIVOS INSTITUCIONALES, ASEGURAR EL FLUJO DE INFORMACIÓN, OPTIMIZAR RECURSOS Y GARANTIZAR LA CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD DE LA MISMA, ASEGURANDO DE ESTA FORMA EL LOGRO DE LOS OBJETIVOS DE LA ENTIDAD.**


**CARACTERÍSTICAS**

| | | | |
|---|---|---|---|
| PÁGINAS: 87 | PLANOS: | ILUSTRACIONES: | CD-ROM: 1 |

# GUÍA DE GESTIÓN DE RIESGOS PARA EL DEPARTAMENTO DE SISTEMAS DEL HOTEL TARIGUA OCAÑA S.A.S, BASADOS EN LA NORMA ISO/IEC 27001

AUTORES:

LORENA TATIANA ACUÑA BARRERA

CÓD.: 850207

YINETH YURIZA PEINADO PACHECO

CÓD.: 850203

**Trabajo de grado presentado como requisito para Optar el título de Especialista en Auditoria de Sistemas**

DIRECTOR:

Esp. JOSÉ ALEXANDER SANTIAGO DURÁN

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

OCAÑA, COLOMBIA FEBRERO, 2019

# Índice

# Lista de tablas

# Lista de figuras

# Lista de apéndices

# Resumen

Hoy en día muchas de las empresas tienen dentro de sus objetivos corporativos mejorar de manera continua sus procesos, para esto gestionan y miden cada parámetro, lo que les permite determinar cuándo una variación puede afectar la producción o los servicios que brindan. Lo anterior está ligado con la seguridad de la información, siendo este uno de los parámetros que permite medir y analizar los incidentes, es decir, los eventos no deseados que se detectan en la red o en los servicios y que pueden poner en riesgo la disponibilidad, la confidencialidad o la integridad de la información (Reporte digital, 2017).

Teniendo en cuenta "la importancia de la seguridad en la información de las empresas, se alude que sin importar la actividad económica a la que se dedica, debe considerar planes para el aseguramiento de la información, generando políticas y controles bien sea en busca de garantizar la continuidad del negocio o de una certificación como carta de presentación y de distinción ante la competencia" (Ruiz & Caicedo, 2014).

En la actualidad, el análisis de riesgos constituye una herramienta importante para el trabajo del empresario, por cuanto implica el diagnóstico de los mismos para velar por su posible manifestación o no, el Hotel Tarigua debe tomar conciencia de la necesidad de alinear sus objetivos institucionales, asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma, asegurando de esta forma el logro de los objetivos de la entidad.

# Introducción

El Sistema de Gestión de Seguridad de la Información ISO 27001 persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada. Los términos seguridad de la información y garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

Teniendo en cuenta lo anterior se alude que en el hotel Tarigua Ocaña S.A.S, se han evidenciado inconvenientes en el manejo de la información debido a que la entidad ha ido creciendo a pasos agigantados y no se ha tomado conciencia por parte de los directivos, de la importancia de asegurar la información existente; siendo para esto indispensable realizar un análisis de riesgos de la seguridad de la información, por lo anterior se propusieron objetivos como son el diagnóstico del departamento de sistemas, para establecer el contexto e identificar, valorar y tratar los riesgos, una metodología de evaluación de riesgos que permita definir las vulnerabilidades y amenazas de seguridad existentes, se identificaron los dominios de la norma ISO 27001, más pertinentes para la entidad, finalmente se elaboró un documento que guie la gestión del riesgo, en el Hotel Tarigua Ocaña S.A.S. Las empresas privadas no pueden ser ajenas al tema de los riesgos y deben buscar cómo manejarlos partiendo de la base de su razón de ser y su compromiso con la sociedad; por esto se debe tener en cuenta que los riesgos no sólo son de carácter económico y están directamente relacionados con entidades financieras o con lo que se ha denominado riesgos profesionales, sino que hacen parte de cualquier gestión que se realice.

# Capítulo 1. Guía de Gestión de Riesgos para el Departamento de Sistemas del Hotel Tarigua Ocaña S.A.S, basados en la norma ISO/IEC 27001

## 1.1 Planteamiento del problema

La Norma ISO-27001 se creó teniendo en cuenta un proceso de seguridad de la información basado en el famoso ciclo de Deming ciclo de mejora continua o ciclo PDCA (por las iniciales de Plan, Do, Check y Act), creando con ello lo que se llamó el Sistema de Gestión de la Seguridad de la Información (conocido en inglés como el ISMS, Information Security Management System) (Acevedo, 2011).

Antes de revisar qué es un sistema de gestión de seguridad de la información, es importante definir qué se entiende por "seguridad de la información". Aunque para muchos pareciera un concepto demasiado básico, lo cierto es que no todo mundo lo tiene claro y por lo mismo se debe ser reiterativo antes que dejar fuera a aquellos que se inician en esto de la seguridad informática. Los clásicos definen la seguridad de la información como el logro, gestión y mantenimiento de tres características elementales:

- Confidencialidad. La información sólo debe ser vista por aquellos que tienen permiso para ello, no debe poder ser accedida por alguien sin el permiso correspondiente.
- Integridad. La información podrá ser modificada solo por aquellos con derecho a cambiarla.
- Disponibilidad. La información deberá estar disponible en el momento en que los usuarios autorizados requieren acceder a ella (Acevedo Juarez, 2011).

Con base en la anterior afirmación es necesario decir que en la ciudad de Ocaña desde hace varios años viene prestando sus servicios a la comunidad el hotel Tarigua S.A.S, entidad que ofrece servicios de alojamiento a propios y extraños en la ciudad, brindando comodidad y confort a sus clientes, dicho ente económico desde su creación no ha contado con un sistema de seguridad en la información manejada al interior, que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta la información presente en cada uno de los procesos internos, de igual forma no se tienen estandarizados controles que lleven a mitigar delitos informático o amenaza a los que están expuestos los datos comprometiendo la integridad, confidencialidad y disponibilidad de la información.

De otra parte en la entidad 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, problema que de presentarse 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 siendo esto muy delicado para la actividad económica realizada, este aspecto, 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 debe efectúa el departamento de sistemas en beneficio del hotel.

Por último se debe decir que en el hotel se han evidenciado inconvenientes en el manejo de la información debido a que la entidad ha ido creciendo a pasos agigantados y no se ha tomado conciencia por parte de los directivos, de la importancia de asegurar la información existente;

siendo para esto indispensable realizar un análisis de riesgos de la seguridad de la información, como también hacer recomendaciones de la seguridad que se debe empezar a implementar en la entidad.

## 1.2 Formulación del problema

¿Qué beneficios puede traer al hotel Tarigua Ocaña S.A.S, la identificación de riesgos y amenazas en la seguridad de la información?

## 1.3 Objetivos

**1.3.1 Objetivo General.** Proponer una guía de Gestión de Riesgos para el Departamento de Sistemas del Hotel Tarigua Ocaña S.A.S, basados en la norma ISO/IEC 27001.

### 1.3.2 Objetivos Específicos.

- Realizar un diagnóstico situacional al departamento de sistemas del Hotel Tarigua Ocaña S.A.S, identificando, definiendo y valorando riesgos de la misma forma vulnerabilidades de seguridad existentes.
- Identificar los dominios de la norma ISO 27001, pertinentes para el departamento de sistemas del Hotel Tarigua Ocaña S.A.S, haciéndose necesario el diseño de una guía de gestión y/o administración de riesgos logrando minimizar amenazas presentes.

- Elaborar un documento que guie la gestión del riesgo, presente en el departamento de sistemas del Hotel Tarigua Ocaña S.A.S, mediante el diseño de formatos relacionados con la consulta, identificación, tratamiento y valoración de riesgos.

**1.4 Justificación**

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 (El tiempo, 2014).

De lo anterior radica la importancia de la evaluación comparando 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 (Banco Central de Uruguay, 1999).

Afortunadamente en los últimos años se han creado herramientas como la norma ISO 27001 que ofrece la protección ante cualquier amenaza que pueda poner en peligro a las organizaciones, tanto públicas como privadas, la realidad nos ofrece que las empresas se enfrentan diariamente a un enorme número de riesgos e inseguridad que proviene de una elevada variedad de fuentes diferentes, entra las que se pueden entrar los nuevos negocios y nuevas herramientas relacionadas con la tecnología de la información y la comunicación, que los

directores generales y los directores informáticos de la organización deben aplicar. (Blog especializado en sisetma de gestion de seguridad de la información, 2015).

Teniendo en cuenta “la importancia de la seguridad en la información de las empresas, se debe decir que sin importar la actividad económica a la que se dedica, debe considerar planes para el aseguramiento de la información, generando políticas y controles bien sea en busca de garantizar la continuidad del negocio o de una certificación como carta de presentación y de distinción ante la competencia” (Perafan Ruiz & Caicedo Cuchimba, 2014). Por lo que empresas como el Hotel Tarigua debe tomar conciencia de la necesidad de alinear sus objetivos institucionales, asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma, asegurando de esta forma el logro de los objetivos de la entidad.

Por último se debe mencionar que el no tomar las medidas de seguridad en la información del Hotel Tarigua, va a llevar a que esté, expuesta al acceso no autorizado de personas ajenas a la empresa, que pueden ocasionar daños a red informática o a los equipos que en ella se encuentran y puede ocasionar en la gran mayoría de los casos graves problemas, como es el riesgo de robo de información sensible y confidencial, el cual puede ocasionar hasta el cierre de una empresa solida financieramente.

## 1.5 Delimitaciones

**1.5.1 Delimitación Geográfica.** El desarrollo del trabajo de grado se llevó a cabo en la ciudad de Ocaña, Norte de Santander, específicamente en el Hotel Tarigua Ocaña S.A.S, ubicado en Carrera 12 No 8 – 47, barrio Centro.

**1.5.2 Delimitación Temporal.** El proyecto de grado se realizó en cuatro (4) meses, de acuerdo a las diferentes actividades a realizar durante el desarrollo del mismo.

**1.5.3 Delimitación Conceptual.** Los conceptos pertenecientes al área de conocimiento de este proyecto se relacionan con la Seguridad de la Información, Sistema de Gestión de Seguridad de la Información (SGSI), Riesgos, información, vulnerabilidad, amenazas, entre otros.

**1.5.4 Delimitación Operativa.** Los inconvenientes que se pueden presentar a lo largo del trabajo de grado, pueden ser la falta de tiempo, poca información acerca del tema que se trabaja, veracidad de la información, problemas climáticos, entre otros, de surgir algún inconveniente esto será informado a la directora del trabajo de grado y al comité curricular para tomar los correctivos necesarios.

# Capítulo 2. Marco Referencial

## 2.1 Marco histórico

### 2.1.1 Antecedentes de la ISO/IEC 27001 y la seguridad en la información a nivel internacional.

En los últimos años, con el desarrollo de las tecnologías de información y su relación directa con los objetivos de las organizaciones, el universo de amenazas y vulnerabilidades crece, por lo tanto es necesario proteger uno de los activos más importantes de la organización, la información, garantizando siempre la disponibilidad, confidencialidad e integridad de la misma.

Debido a que actualmente existen diversos escenarios de amenazas, tales como: la fuga de información o un ataque de ingeniería social, que en cualquier momento pueden manifestarse, con el fin de obtener información confidencial y hacer colapsar a la empresa; es necesario que el negocio cuente con una estrategia de continuidad de negocio, claramente definida por cada escenario de amenaza identificado para así poder reanudar las operaciones rápidamente (Tola Franco D. E., 2015).

La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos. El presente proyecto de titulación reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2005, para asegurar la protección de los activos de información y otorgar

confianza a los clientes de A&CGroup S.A. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

De lo anterior se pudo concluir que debido a que en las organizaciones es primordial la optimización de recursos, el establecimiento del alcance del sistema de gestión de seguridad de la información se convierte en una actividad muy importante ya que delimita el campo de acción y el uso de recursos, la adopción de la metodología MAGERIT para el análisis de riesgos, permitirá identificar de manera oportuna la probabilidad y el impacto de que 117 se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos y los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, se basan en la prevención, por lo tanto es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales (Tola Franco D. E., 2015).

De otra parte es necesario afirmar que hoy en día son múltiples los riesgos asociados a que equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad.

Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, es por ello la necesidad de una estrategia completa de seguridad, de manera

de prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas (misma organización), que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios. No se pueden obviar los factores de riesgos por desastres que al no estar previstos eficientemente y sin planes de contingencia y/o de recuperación pueden provocar daños irreparables en tiempo y costos de recuperación (Burgos Salazar & Campos, 2012).

Esto, que es difícilmente cuantificable, puede incluso determinar la continuidad de una organización. En este trabajo se presenta un modelo basado en estándares y normas internacionales, para evitar y/o disminuir las fallas en los sistemas, redes, Internet y todo el patrimonio informático ( hardware, software y datos) de ataques o desastres, antes que éstos ocurran, a través de un proceso de establecimiento de políticas, procedimientos, registros, controles y documentación. Este modelo puede ser utilizado como base para que cualquier tipo de organización pueda realizar un uso seguro de sus TIC.

Según informes y publicaciones de distintos medios e inclusive algunos elaborados por la brigada de Ciber Crimen de Investigaciones de Chile, dan cuenta que sobre el 90% de las empresas Chilenas son ignorantes en temas de seguridad de la información, donde el 96% de ellas 236 son incapaces de detectar un ataque o intromisión a sus sistemas, y donde el 99% de ellas no posee especialistas ni herramientas para detectar el fraude informático. En Chile, con excepción de grandes compañías multinacionales que tranzan valores en la bolsa Chilena y/o en la de Estados Unidos de Norte América y el mayor porcentaje de las empresas bancarias, no

existe la adecuada conciencia ni entendimiento de la seguridad de la información de las TIC (Burgos , Salazar & Campos, 2012).

**2.1.2 Antecedentes de la ISO/IEC 27001 y la seguridad en la información a nivel nacional.** Las Tecnologías de la Información y la Comunicación TIC han llevado a las organizaciones a estar a la vanguardia con los adelantos tecnológicos, la información se convierte entonces en un recurso primordial para lograr ser competitivos, esta es la razón por la cual debe ser protegida de diferentes formas, con el uso de las nuevas tecnologías, las compañías se han vuelto más vulnerables ante ataques informáticos.

Para proteger la información es necesario confeccionar un estudio muy detallado que permita identificar los riesgos a los que se encuentra expuesta la empresa, de esta forma se puede establecer cuál es la forma correcta de implementar medidas para contrarrestar esta deficiencia y salvaguardar los activos, una forma eficaz para realizar estos procesos es un análisis para la implementación de un Sistema de Gestión de Seguridad Informática y esto es exactamente lo que aborda este trabajo de grado, un análisis concienzudo de todas las vulnerabilidades a las que está expuesta la empresa Servidoc S.A. en temas relacionados con seguridad informática (Giraldo Cepedan, 2016).

El análisis se realizó por medio de fases, donde se incluyeron entrevistas, observación directa y la aplicación de la metodología de análisis de riesgos Magerit entre otras, esta metodología permitió realizar un análisis para la implementación de un SGSI que permita identificar amenazas, vulnerabilidades y riesgos que pueden afectar la organización

específicamente en las áreas de contabilidad, facturación e historias clínicas, el resultado final permitió la identificación de los riesgos y la forma de mitigar esos riesgos, para ello se hicieron recomendaciones y se sugirieron proyectos que la empresa debe implementar para cubrir estas debilidades, adicionalmente se logró identificar el nivel en el que se encuentra la organización en cuanto a seguridad informática y el resultado fue muy negativo, puesto que falta mucho por hacer para proteger los activos de la empresa (Giraldo, 2016).

Siguiendo con el tema se puede mencionar que en la Secretaria de Educación de Nariño, se realizar un diagnóstico de la seguridad informática en el área financiera, teniendo en cuenta que es un proceso que adquiere importancia y relevancia dado el continuo desarrollo de la tecnología y del acceso a los diferentes canales de comunicación. Así las cosas es de mucha relevancia para el área financiera y para la entidad en general contar con una herramienta que le aporte para la toma de decisiones tendientes a ajustar o eliminar las falencias que se puedan estar presentando tanto en el sistema que soporta los procesos como en el manejo mismo de la información al interior del área y de la entidad (Aguirre & Sambrano, 2015).

El problema principalmente radica en que en la Secretaría de Educación del Departamento de Nariño no se tiene implementado un Sistema de Gestión de la Seguridad de la Información (SGSI), hasta el momento no se ha realizado un proceso de auditoría de los sistemas de información en general, que permita establecer los riesgos que se presentan en cuanto a la seguridad informática y de la información, y el sistema de control es incipiente para la mitigación de las eventuales amenazas y riesgos que puedan presentarse. Así las cosas la presente investigación busca minimizar el impacto y la probabilidad de las amenazas y riesgos

potenciales a que ve expuesta el área financiera mediante un diagnóstico de la seguridad informática y de la información que ayude a la implementación de un SGSI basado en la norma ISO/IEC 27001 en la Secretaría de Educación de Nariño.

Para tal propósito el presente trabajo se divide en seis capítulos. En un primer capítulo se define la línea de investigación, el nombre del proyecto y el tema, posteriormente el segundo capítulo se encarga de encauzar los elementos propios del problema de investigación así como también propone el marco referencial del proyecto; el capítulo tercero delimita la investigación en su enfoque metodológico; el capítulo cuarto se encarga de distribuir la presentación de resultados en atención al cumplimiento de cada uno de los objetivos específicos del proyecto y posteriormente las capítulos quinto y sexto se dedican a formular las conclusiones y recomendaciones obtenidas con base en los hallazgos proyectados en el trabajo de campo de la investigación (Aguirre Tobar & Sambrano Ordoñez, 2015).

## 2.2 Marco contextual

El Hotel Tarigua, está ubicado en el centro de la ciudad de Ocaña, a unos pasos del parque principal, en plena zona comercial y a sólo dos cuadras del complejo histórico de la Gran Convención. Somos un hotel acogedor, dónde los detalles son cuidados con atención. Un equipo de profesionales, siempre atentos a sus necesidades, les recibe en un agradable ambiente familiar.

## 2.3 Marco conceptual

**2.3.1 Seguridad de la Información.** La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta. La seguridad informática comprende software, bases de datos, datos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. (Reyes, 2014)

**2.3.2 Sistema de Gestión de Seguridad de la Información (SGSI).** SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. (ISO 7000).

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (ISO 27000).

**2.3.3 Riesgos.** La palabra riesgo es tan antigua como la propia existencia humana. Podemos decir que con ella se describe, desde el sentido común, la posibilidad de perder algo (o alguien) o de tener un resultado no deseado, negativo o peligroso. (Tocabens, 2011).

El riesgo de una actividad puede tener dos componentes: la posibilidad o probabilidad de que un resultado negativo ocurra y el tamaño de ese resultado. Por lo tanto, mientras mayor sea la probabilidad y la pérdida potencial, mayor será el riesgo. (Horgath 2010).

**2.3.4 Vulnerabilidad.** Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software. (codejobs.biz, 2012)

**2.3.5 Amenazas.** Una amenaza a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo. (Codejobs.2012).

## 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 (Figuerola, 2013).

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 (Figuerola, 2013).

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. 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 (Estándar Australiano, 2017).

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 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 (Instituto Colombiano de Normas Técnicas y Certificación, 2011).

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 (Instituto Colombiano de Normas Técnicas y Certificación, Gestión del riesgo, Vocabulario. GTC 137:2011., 2011).

La norma ISO 17799 es un código de buenas prácticas para la Gestión de la Seguridad de la Información, esta norma surge como evolución histórica de la norma británica BS 7799 y actualmente existen varias adaptaciones de la misma que convergerán en un futuro próximo a las normas de la serie ISO 27000. La ISO 17799 introduce un cambio importante en los sistemas de gestión de la seguridad de la información ya que los aborda desde un punto de vista de continuidad de negocio y de mejora continua. Esta norma hereda muchos conceptos de la serie de normas ISO 9000 y subraya la seguridad entendida como proceso. (Villalon Huertas, 2016)

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO e IEC que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña; Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. (Villalon Huertas, 2016)

## 2.5 Marco legal

**2.5.1 Ley 1266 del 31 de diciembre de 2008.** El Congreso de Colombia decretó: “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la

información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones." (Congreso de Colombia, 2015)

**Artículo 71 de la Constitución Política de Colombia**. Este artículo otorga al Estado la responsabilidad de promover el desarrollo tecnológico e incentivar a quienes se dediquen a trabajar en este ámbito "… El Estado creará incentivos para personas e instituciones que desarrollen y fomenten la ciencia y la tecnología y las demás manifestaciones culturales y ofrecerá estímulos especiales a personas e instituciones que ejerzan estas actividades." (República de Colombia, 2012)

Es de gran importancia lo que se acaba de mencionar puesto que es precisamente la Constitución Política que estando por encima de todas las leyes, ampara la actividad de desarrollo tecnológico.

**2.5.2 Ley 1273 del 5 de enero de 2009.** El Congreso de Colombia decretó: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." (Ley N° 1273, 2009).

**2.5.3 Ley 1581 del 17 de octubre de 2012.** El Congreso de Colombia decretó que esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer,

actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política de Colombia; así como el derecho a la información consagrado en el artículo 20 de la misma. (República de Colombia, Ley 1581 de 2012, 2012).

# Capítulo 3. Diseño Metodológico

## 3.1 Tipo de investigación

Méndez, A.C. (2003), La investigación descriptiva identifica características del universo, formas de conducta y actitudes del universo investigado, establece comportamientos concretos y descubre y comprueba la asociación entre las variables enunciadas en la investigación.

Para el estudio, se aplicó el tipo de investigación descriptiva, buscando responder 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 y muestra

Se tomó como población objeto de estudio a los trece (13) empleados, los cuales tienen directa relación con la información manejada al interior del hotel Tarigua, de igual forma por ser tan reducida la población se tomó en su totalidad y estos aportaron los datos necesarios para realizar el proyecto.

### 3.3 Técnicas para la recolección de la información

Como técnica de indagación directa se utilizó la observación documental siendo el más viable para el desarrollo de los objetivos y el instrumento de recolección de información más importante que consiste en el registro sistemático, válido y confiable de comportamientos o conducta manifiesta.

### 3.4 Procesamiento de la información recolectada

Teniendo en cuenta la información recolectada esta fue presentada de forma cualitativa describiendo cada uno de los aspectos relevantes para la investigación y desarrollo de los objetivos.

### 3.5 Metodología

La siguiente tabla muestra a manera de diagnóstico un análisis de los objetivos establecidos en el proyecto con las respectivas actividades efectuadas en la investigación

**Tabla 1.**
*Metodología*

| Objetivos | Actividades |
|---|---|
| Realizar un diagnóstico situacional del Realizar un diagnóstico situacional al departamento de sistemas del Hotel Tarigua Ocaña S.A.S, estableciendo su contexto, identificando y valorando riesgos, definiendo vulnerabilidades y amenazas de seguridad existentes. | Se realizará observación y análisis de la situación actual del hotel verificando y auditando documentos y procedimientos existentes emitiendo un diagnostico acorde a la actual realidad de la organización. |
| Identificar los dominios de la norma ISO 27001, pertinentes para el Hotel Tarigua Ocaña S.A.S, haciéndose necesario el diseño de una guía de gestión y/o administración de riesgos para el departamento de sistemas del Hotel Tarigua Ocaña S.A.S, logrando minimizar posibles amenazas presentes. | Se tendrá en cuenta los dominios de la norma ISO 27001 analizando necesidades presentes en el hotel, elaborando un documento donde se expongan los estándares que ayuden al hotel a evitar riesgos en la información |
| Elaborar un documento que guie la gestión del riesgo, según la información recolectada en el departamento de sistemas del Hotel Tarigua Ocaña S.A.S. | Con la información recolectada a través del desarrollo del trabajo de grado, se propondrá una guía y el diseño de formatos relacionados con la identificación, tratamiento y valoración de riesgos los cuales contribuyen a mitigar falencias existentes en el hotel. |

**Nota.** Fuente. Autores del proyecto

# Capítulo 4. Presentación de resultados

Para el desarrollo de la guía de gestión de riesgos para el departamento de sistemas del hotel Tarigua del municipio de Ocaña, Norte de Santander con base en la Norma ISO/IEC 27001 se han estructurado el desarrollo de 3 objetivos enfocados en la gestión de riesgos partiendo inicialmente con el diagnóstico situacional.

## 4.1 Diagnóstico situacional al departamento de sistemas del Hotel Tarigua Ocaña S.A.S, identificando, definiendo y valorando riesgos de la misma forma vulnerabilidades de seguridad existentes

La siguiente información es sustraída de entrevistas efectuadas al propietario y empleados de la parte administrativa y operativa del Hotel Tarigua del municipio de Ocaña Norte de Santander, quienes de manera verbal expresaron su punto de vista frente a la gestión de riesgos presentes alrededor del hotel específicamente en el departamento de sistemas, complementario a lo anterior, se efectuó revisión y análisis por parte de las autoras del estudio de documentación interna que reposa en el hotel para dar un diagnóstico subjetivo de acuerdo a los objetivos trozados en la presente investigación.

El Hotel Tarigua S.A.S, se encuentra ubicado en el municipio de Ocaña Norte de Santander y de acuerdo con su inscripción en la Cámara de Comercio tiene por objeto social la prestación de servicios de alojamiento, turismo, agencias de viajes, gastronómicos (restaurante y cafetería), recreativos, desarrollar actividades de eventos y congresos, así mismo podrá realizar cualquier

otra actividad económica lícita, tanto en Colombia como en el extranjero, la sociedad podrá llevar a cabo en general, todas las operaciones de cualquier naturaleza que ellas fueren relacionadas con el objeto mencionado, así como cualquier actividad similar conexa o complementaria que permita facilitar o desarrollar el comercio o la industria hotelera.

En desarrollo de su objeto social podrá adquirir, arrendar, gravar o enajenar inmuebles y otros bienes inmuebles y demás artículos relacionados con él, dar o recibir dinero en mutuo, celebrar toda clase de actos o contratos necesarios o convenientes para el desarrollo del objeto principal, recibir o dar en hipoteca o prenda los bienes muebles e inmuebles de la sociedad en garantía de las operaciones que celebre, negociar toda clase de títulos, valores, otorgados, endosados, pagarlos, descargarlos y en general toda clase de operaciones comerciales o financieras que se relacionen directamente con el objeto social (Cámara de comercio Ocaña, 2017).

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. SGSI. Bogotá: Kimpress, 2010. Por lo descrito anteriormente, el análisis de riesgos para el departamento de sistemas del Hotel Tarigua, constituye una herramienta importante en la eficiencia y eficacia del trabajo efectuado por la persona responsable del almacenamiento y guarda de la información, implica la identificación, análisis, tratamiento y valoración de los riesgos velando por su posible manifestación o no.

La administración de riesgos en el departamento de sistemas, implica que los procesos, personas, tecnología y conocimiento están alineados manejando toda incertidumbre que la empresa puede enfrentar (Sullivan 2.014).

Es importante para el hotel y específicamente para el departamento de sistemas, contar con una herramienta, que garantice la correcta evaluación de los riesgos a los cuales están sometidos los procesos y procedimiento contribuyendo al cumplimiento de sus objetivos y metas; aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y dirección. (Sullivan 2.014).

A través de la auditoria efectuada al departamento de sistemas y a información suministrada por la población objeto de estudio trece (13) trabajadores, las autoras del presente documento identificaron, establecieron y dieron valoración a los riesgos presentes los cuales tienen incidencia en cada uno de los procesos llevados al interior del hotel, con la finalidad de emitir un documento orientado a la prevención de fraudes, quebrantos patrimoniales, ineficiencias operativas y en general riesgos que puedan afectar la buena marcha de la organización; de la misma forma se optó por controlar la aplicación y promocionar el desarrollo de normas, procedimientos de acuerdo con los Sistemas Comunes de Gestión Corporativos, revisando la aplicación de los planes de gestión, la adecuada realización y supervisión de los trabajos y la puntual distribución de los resultados obtenidos.

Según análisis efectuado al interior del departamento de sistemas y buscando definir tipologías de riesgos, las autoras del presente documento, establecieron una valoración del riesgo

con base a los procedimientos, tareas, mecanismos y actividades llevadas a cabo en el hotel Tarigua, definiéndolo y caracterizándolo como alto, medio o bajo, se tuvo en cuenta la siguiente metodología.

La siguiente tabla muestra a manera de diagnóstico la valoración de riesgos presentes en el departamento de sistemas del hotel Tarigua y su respectiva incidencia en la operatividad del hotel.

**Tabla 2.**
*Valoración y Ponderación del riesgo departamento de sistemas Hotel Tarigua*

| Valoración | Ponderación |
|---|---|
| RIESGO BAJO | Afecta un poco el contexto administrativo, contable, flujo y manejo de información del Hotel en lo que refiere a correcta operatividad y funcionamiento |
| RIESGO MEDIO | Afecta una parte el contexto administrativo, contable, flujo y manejo de información del Hotel para su correcta operatividad y funcionamiento. |
| RIESGO ALTO | Afecta totalmente o parcialmente el contexto administrativo, contable, flujo y manejo de información del Hotel para su correcta operatividad y funcionamiento. |

Fuente: Autores del proyecto

Una vez es valorado y ponderado el riesgo, el paso a seguir fue la de establecer el riesgo observado e identificado con base en la información auditada determinando la descripción del riesgo, sus posibles consecuencias, el plan o manejo que se debe dar y su ponderación de acuerdo a su nivel de incidencia, se busca mitigar posibles impactos o vulnerabilidades impidiendo la propagación de los mimos.

Se especifica, se describe, se denota posibles consecuencias, del plan de manejo del riesgo y su respectiva ponderación de riesgos presentes alrededor del Hotel Tarigua. Información expresada por las autoras de la investigación.

**Tabla 3.**
*Identificación, valoración de riesgos departamento de sistemas Hotel Tarigua*

| FACTOR DE RIESGO | DESCRIPCIÓN | POSIBLES CONSECUENCIAS | PLAN DE MANEJO DE RIESGO | PONDERACIÓN |
|---|---|---|---|---|
| **Estructura funcional y operativa del sistema informativo** | Cambio frecuente de las políticas y estrategias de control de la información.<br><br>Precariedad en los sistemas de evaluación y seguimiento de las estrategias de lucha contra las debilidades y amenazas presentes en el hotel. | Tráfico de influencias, falta de oportunidad y pertinencia en la formulación de prioridades. | Diseño e implementación de una estructura organizacional bien definida para la tenencia de información confiable y precisa cuando esta se desee | Riesgo Medio |
| **Proceso de planeación de control de la información** | La planeación del control se reduce a un cronograma para la recopilación de informes.<br><br>Ausencia de estudios de seguimiento y evaluación. | Se pierde la visión de conjunto para realizar la evaluación de la gestión de los recursos disponibles en el Hotel Tarigua.<br><br>Entorpece el análisis sobre las falencias y fortalezas de las estrategias de optimización, sus prioridades y sus dificultades del sistema de control interno en la detección de prácticas corruptas | Diseño de un cronograma de actividades en el cual se fijen las tareas a llevar acabo y el tiempo de cumplimiento | Riesgo Medio |

*Continuación Tabla 3. Identificación, valoración de riesgos departamento de sistemas Hotel Tarigua*

| FACTOR DE RIESGO | DESCRIPCIÓN | POSIBLES CONSECUENCIAS | PLAN DE MANEJO DE RIESGO | PONDERACIÓN |
|---|---|---|---|---|
| **Influencia en las auditorías** | Desaparición de información para dificultar las auditorías<br><br>Complicidad de trabajadores<br>No se denuncian prácticas poco adecuadas<br>Predisposición de algunos funcionarios encaminados a impedir varios tipos de visita de inspección. | Pérdida de recursos y de confiabilidad | Sistematización de la información contables y administrativa del Hotel evitando de esta manera la perdida de información | Riesgo Medio |
| **Inexistencia de un sistema de información empresarial.** | La información que se produce al interior del Hotel se encuentra dispersa y desordenada. | Duplicación de esfuerzos y costos.<br><br>Desgreño administrativo. | Sistematización de la información en un software de evaluación y gestión de riesgos informáticos evitando la pérdida y adulteración de la misma. | Riesgo Alto |

Fuente. Autores del proyecto

Según documentos observados verificados y analizados que reposan en el departamento de sistemas del Hotel Tarigua, los cuales fueron auditados por las proponentes, se deducen algunas vulnerabilidades de seguridad existentes las cuales se contextualizan en los siguientes parámetros.

**Políticas de Seguridad**: En la actualidad el Hotel Tarigua, no cuenta con una política establecida bajo su área administrativa en busca de regular la seguridad de las TI; se carece de un documento que delimite y promueva las políticas para la protección y uso correcto de los activos de información ocasionado vulnerabilidad para la protección de información confidencial de la empresa.

**Aspectos organizativos de la seguridad de la información**: Según lo observado y verificado el Hotel Tarigua ha sido omisivo desde el componente administrativo para delimitar dentro de la organización los aspectos organizativos de seguridad de la información puesto que la primera iniciativa debía ser la puesta en marcha de políticas de seguridad y no existe compromiso ni voluntad para su planteamiento dentro de las acciones a mejorar. Dentro de este mismo aspecto la organización Hotel Tarigua no cuenta con un sistema de gestión para organizar administrativamente las funciones y responsabilidades que permitan la protección de los activos con los que se cuenta dentro de la misma desencadenando un vacío regulatorio para la protección y seguridad de cada uno de ellos.

Dentro de los aspectos organizativos del Hotel Tarigua, se carece de un sistema que formalice los procesos, procedimientos, funciones, responsabilidades y demás de la planta de personal dificultado la prevención de riesgos en la información de la organización que decantaría en insatisfacción del cliente.

De manera análoga la problemática expuesta se presenta en procesos como la contratación del personal puesto que no son claros en la vinculación contractual para la estipulación de cláusulas de confidencialidad que resguarden la información que se maneja, sin embargo lo hacen de manera paralela con una solicitud de reserva total de información que podría en algunos casos tipificar responsabilidades respecto a la vulneración de la información que maneja la organización.

Finalmente ante la desafortunada ausencia de una política de seguridad de la información y estipulación de procedimientos, procesos y funciones de responsabilidad la toma de decisiones se hace limitada y por ende esto termina por no permitir la planificación de un plan de capacitación que permita obtener la información clara y precisa a la hora del manejo de información que afecta el correcto funcionamiento del Hotel Tarigua. En la actualidad solo se hace uso del correo institucional a través del cual se hacen campañas de prevención pero no se planifica dentro de sus acciones de mejora siendo esta una necesidad latente.

**Seguridad ligada a los recursos humanos:** Frente al proceso de seguridad ligada a los recursos humanos se realiza la recepción del curriculum, se verifican datos a través de las plataformas digitales en cuanto a antecedentes disciplinarios, penales y demás, se sistematiza la vinculación del empleado.

De otra parte el proceso de contratación que hoy en día debe ser una prioridad del área de gestión del talento humano se hace con contratos elaborados sobre plantillas pero sobre ellos no existe copia digital ni copia de seguridad en los PC, no se trabaja sobre planes de capacitación, sin tener la prioridad dentro del área administrativa y cuando se hace solo se dan instrucciones básicas mas no se profundiza en la importancia de la seguridad de la información ni de la buenas practicas TI.

**Gestión de Activos**: Para el dominio sobre la gestión de activos en el Hotel Tarigua se presentan unas debilidades identificadas en la auditoría realizada. La primera de ellas está enfocada en que el hotel no cuenta desde la parte administrativa con un inventario que debería

ser gestionado a través de un software que permita el trabajo más ágil y práctico para los funcionarios, además de la seguridad de sus inventarios, esta situación ocasiona que además no se cuente con una clasificación de los activos puesto que la indebida organización hace que la gestión de sus activos no sea una realidad descuidando aspectos importantes y vitales para la prestación del servicio, en relación con las licencias de software como activo de información, están bajo la responsabilidad y custodia.

**Control de Accesos**: De acuerdo con los hallazgos obtenidos durante el proceso de auditoria el Hotel Tarigua no cuenta con una política de seguridad de la información lo que limita el establecimiento de reglas de control de acceso y con los derechos que tienen los trabajadores para el ingreso a los sistemas de información de la organización.

**Seguridad Física y Ambiental:** La auditoría realizada permitió evidenciar dentro del dominio de la seguridad física y ambiental que en el Hotel Tarigua Ocaña no se prioriza sobre las medidas efectivas para controlar el acceso a las áreas críticas S.A.S. Esta debilidad dentro de la dirección administrativa de la empresa permite evidenciar un alto nivel de riesgo en el área y la integridad, confidencialidad y disponibilidad de la información que allí se maneja.

Para la protección de los equipos cuentan con un sistema de refrigeración adecuada (18ºC). En cuanto al manejo ambiental son participes de políticas de protección del medio ambiente y para la protección de los empleados estos son afiliados a la ARL que mitiga y protege de los riesgos laborales dentro de las funciones que desempeñan cada uno de los trabajadores.

**Seguridad Operativa:** En cuanto a la seguridad de la parte operativa en el Hotel Tarigua se toman medidas previas a la contratación cuando se requiere del manejo de las TI se exige dentro de los requisitos para vincularse laboralmente. Estos empleados si están en continua capacitación y actualización que permitan la mitigación de los riesgos que sufren los sistemas de información.

Se hace preciso mencionar que la auditoria evidencio en la parte operativa la necesidad de implementar un sistema de gestión integrado que permita establecer un mapa de procesos en el cual se identifiquen la misión, visión, objetivos, principios, procesos, formatos, guías, caracterización y demás.

**Adquisición, desarrollo y mantenimiento de los sistemas de información:** Los hallazgos de la auditoria permitieron que se evidenciara en cuanto a la adquisición de sistemas de información lo hacen bajo la asesoría de especialistas en software y sistemas de información.

Para el mantenimiento de los equipos, la entidad, cuenta con un servicio alterno al Hotel que bajo una programación trimestral realiza dicho servicio dentro de los sistemas de información con los que se cuenta actualmente en la organización.

**Relaciones con Proveedores**: Respecto a la relación con los Proveedores en el Hotel Tarigua se halló que para el registro de entrada de productos y demás manejan formatos pero no establecen un manual de responsabilidades de esta función ocasionando una amenaza para la

recepción de servicios y productos puesto que esta debilidad puede poner el servicio y los sistemas de información en situaciones de riesgo.

**Gestión de incidentes en la seguridad de la información:** Para la gestión de incidentes en el Hotel Tarigua no registran antecedentes de amenazas para atacar los sistemas de información sin embargo la falta de políticas de seguridad si pone en riesgo a la organización al no contar con los protocolos en caso de presentarse un ataque a alguno de los sistemas que maneja el hotel.

La figura 1 describe brevemente los procesos de cada uno de los ciclos para el funcionamiento efectivo y eficiente de la organización y de la confidencialidad, integridad y disponibilidad de su información (Pallas 2.009).

Las autoras del estudio toman como referencia el Ciclo de Deming, las organizaciones se encuentran inmersas en un entorno competitivo y con cambios constantes cada vez más frecuentes.

Es por ello que la calidad y mejora de procesos se convierten en un imperativo para la supervivencia de estas empresas. Las empresas necesitan gestionar sus actividades y recursos con la finalidad de orientarlos hacia la consecución de buenos resultados, mediante la adaptación de herramientas y metodologías que permitan a las organizaciones configurar su proceso de gestión y mejora continua.

Su principal objetivo es la autoevaluación, destacando los puntos fuertes que hay que tratar de mantener y las áreas de mejora en las que se deberá actuar (Pallas 2.009).

| Ciclo PHVA | Procesos |
|---|---|
| **Planear** (***Plan***) | Establecer el contexto.<br>Alcance y Limites<br>Definir Política del SGSI<br>Definir Enfoque de Evaluación de Riesgos<br>Identificación de riesgos<br>Análisis y Evaluación de riesgos<br>Evaluar alternativas para el Plan de tratamiento de riesgos<br>Aceptación de riesgos<br>Declaración de Aplicabilidad |
| **Hacer** (***Do***) | Implementar plan de tratamiento de riesgos<br>Implementar los controles seleccionados<br>Definir las métricas<br>Implementar programas de formación y sensibilización<br>Gestionar la operación del SGSI<br>Gestionar recursos<br>Implementar procedimientos y controles para la gestión de incidentes de seguridad |
| **Verificar** (***Check***) | Ejecutar procedimientos de seguimiento y revisión de controles.<br>Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI.<br>Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad.<br>Revisión de la evaluación de riesgos periódicamente.<br>Realizar auditorías internas<br>Revisión de alcance y líneas de mejoras del SGSI por la Dirección.<br>Actualizar los planes de seguridad<br>Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI |
| **Actuar** (***Act***) | Implementar las mejoras identificadas para el SGSI<br>Implementar las acciones correctivas y preventivas pertinentes.<br>Comunicar acciones y mejoras a todas las partes involucradas.<br>Asegurarse que las mejoras logren los objetivos previstos. |

**Figura 1.** Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 27001
**Fuente:** (Pallas Mega, 2009).

Basados y direccionados en los procesos que describe la figura 1 del ciclo de Deming, es preciso recomendar al Hotel Tarigua la adecuada disposición de sus recursos físicos, financieros, administrativos y tecnológicos.

La implementación del ciclo Deming en el entorno del hotel permitirá determinar las reglas organizacionales para prevenir amenazas contra la confidencialidad e integridad de su información, cumplir con los requerimientos legales del ordenamientos jurídico colombiano para la protección y seguridad de la información, obtener un reconocimiento en la región por la implementación de políticas y medidas de seguridad de la información y resolver problemáticas de organización dentro del área administrativa al establecer los procesos propios del servicio que prestan.

Un sistema de gestión de la calidad permite a una organización desarrollar políticas, establecer objetivos y procesos, y tomar las acciones necesarias para mejorar su rendimiento. En este contexto resulta de gran utilidad utilizar la metodología PDCA (Ciclo de Mejora Continua) impulsada por Deming, como una forma de ver las cosas que puede ayudar a la empresa a descubrirse a sí misma y orientar cambios que la vuelvan más eficiente y competitiva (Pallas Mega, 2009).

## 4.2 Identificar los dominios de la norma ISO 27001, pertinentes para el Hotel Tarigua Ocaña S.A.S, haciéndose necesario el diseño de una guía de gestión y/o administración de riesgos para el departamento de sistemas del Hotel Tarigua Ocaña S.A.S, logrando minimizar posibles amenazas presentes

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento. (ISO 27001).

La seguridad de la información además de requerir un diagnóstico previo y una metodología apropiada, es necesario salvaguardar la información que fluye en el hotel Tarigua producto de la actividad económica que efectúa en las diferentes actividades comerciales. Se requiere de controles para la gestión de su seguridad enmarcada en la norma ISO/IEC 27001 asociados a dominios que específica la norma.

Tomando como referencia para el estudio los dominios de la Norma ISO/IEC 27001 se efectúa una referenciación sobre los mismos, siendo estos de vital necesidad para solventar posibles riegos en la tenencia de información que fluye al interior del hotel.

Basados en la norma ISO/IEC 27001. En su libro Nueve Claves del éxito, Calder (2006) las autoras de la investigación efectúan una descripción y análisis acerca del contenido de cada uno de los dominios:

Dominio A.5. Política de Seguridad de la información

Dominio A.6. Organización de seguridad de la Información

Dominio A.7. Gestión de Activos de información (AI)

Dominio A.8. Seguridad de los recursos humanos

Dominio A.9. Seguridad Física y Medioambiental

Dominio A.10. Gestión de operaciones y comunicaciones

Dominio A.11. Control de acceso lógico

Dominio A.12. Adquisición, desarrollo y mantenimiento de sistemas de información

Dominio A.13. Gestión de incidentes de seguridad de la información

Dominio A.14. Gestión de la continuidad de las operaciones

Dominio A.15. Cumplimiento Regulatorio

Los once (11) dominios referenciados, están direccionados a la protección, confidencialidad, integridad y disponibilidad de la información, siendo elementos esenciales para el adecuado flujo de información almacenada en las bases de datos del hotel Tarigua producto de la actividad económica que efectúa.

Tomando como referencia lo expuesto por Calder (2006), acerca de los dominios de la norma ISO/IEC 27001, es de vital necesidad que trabajadores del hotel tarigua, identifiquen, analicen y den tratamiento a problemas que pueden afectar la información almacenada en el departamento de sistemas del hotel, (es decir, efectuar un análisis de la evaluación e incidencia de riesgos) así mismo se debe definir lo que es necesario hacer para evitar que estos problemas se produzcan mitigando o dando tratamiento al riesgo.

Con base en lo anterior, los riesgos informáticos comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos asi como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo producto de la no tenencia de un software seguro (Valero 2.014).

Es esencial que el hotel tarigua cuente con una herramienta, que garantice la correcta evaluación de los riesgos presentes, a los cuales puede estar sometido.

Para minimizar amenazas, en el departamento de sistemas del hotel, se debe dar cumplimiento con requerimientos legales, cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con sus políticas de seguridad.

La filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá una mejor organización en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no sabe qué hay que hacer, cuándo y quién debe hacerlo.

La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados (Giraldo Cepedan, 2016).

Las autoras de la investigación recomiendan al propietario del hotel tarigua la utilización del Dominio denominado Política de Seguridad de la información buscando proporcionar al hotel el soporte y la gestión para la seguridad de la información de acuerdo a los requerimientos institucionales y requisitos legales pertinentes, se debe optar por establecer la política alineada a los objetivos institucionales demostrando el compromiso con la Seguridad de la Información.

**Ventajas de la gestión del riesgo según la norma ISO 27001.** Los beneficios que aporta la implementación de la norma ISO 27001 se centran en los siguientes campos. En el ámbito de la empresa, ya que se genera un importante compromiso con la seguridad de la información.

La existencia de registros y medidas de control permiten que la seguridad de la información que den garantizados en la empresa y que estos esfuerzos puedan demostrarse.

En el cumplimiento legal de las exigencias, manifestándose la conformidad de la organización en el cumplimiento de todos los requisitos legales que le son de aplicación para la región en la que la empresa tenga su domicilio y para la actividad que realice.

En el ámbito funcional, ya que se desarrolla una adecuada gestión de los riesgos. La organización conoce de manera exhaustiva su empresa y los sistemas de información que aplican, los problemas que se producen y los medios de protección que se aplican, para así terminar garantizando la mejora disponibilidad de los materiales y datos, además de asegurarse de su continuidad sin alteraciones perniciosas no controladas.

En el aspecto comercial, se genera cierta credibilidad y confianza entre nuestros clientes, se debe tener presente que nos encontramos ante una sociedad que tiene falta de confianza de nuestros clientes que afecta a nuestras ventas de la misma forma que la calidad y la funcionalidad de nuestros productos, y por lo tanto, se debe cuidar tanto un aspecto como el otro.

En el aspecto financiero, las empresas consiguen reducir los costes de producción que se encuentran vinculados a todos los incidentes y se consiguen minimizar las primas de seguros.

En el aspecto humano, se produce una sensibilización del personal en relación a la importancia de la correcta manipulación de la información, dentro de la aplicación adecuada a las medidas de seguridad que deben adoptarse y a las responsabilidades personales y de la organización con relación a la información de la que disponen, además de los dueños de la información.

La implementación y mantenimiento de una gestión del riesgo le permite al hotel. 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.

**Mapa de administración de riesgos departamento de sistemas Hotel Tarigua.**

Actualmente la dirección moderna concibió una disciplina denominada “Administración de

riesgos" o "Gerencia de riesgos", que es una función de muy alto nivel dentro de la organización privada para definir un conjunto de estrategias que a partir de los recursos (físicos, humanos y financieros) busca, en el corto plazo mantener la estabilidad informática de la empresa, protegiendo la información generada en una entidad producto de su actividad económica (Morales 2.014).

En éste contexto, las empresas privadas no pueden ser ajenas al tema de los riesgos y deben buscar cómo manejarlos partiendo de la base de su razón de ser y su compromiso con la sociedad; por esto se debe tener en cuenta que los riesgos no sólo son de carácter económico y están directamente relacionados con entidades financieras o con lo que se ha denominado riesgos profesionales, sino que hacen parte de cualquier gestión que se realice en su parte operativa.

De acuerdo con lo anterior las autoras de la investigación propendiendo por la eficiencia y eficacia organizacional y del flujo adecuado de información, han desarrollado una metodología que permite el diseño de una guía de gestión para la administración de riesgos, su análisis y manejo, de tal forma que se garantice el cumplimiento de los objetivos empresariales y la supervivencia de la empresa con base a la información que reposa en sus archivos documentales. Se busca reducir el riesgo y controlar la presencia de los mismos.

**Reducción de Riesgos**. Los riegos en hotel tarigua pueden ser reducidos con: programas de seguridad, guardias de seguridad, alarmas y estimación de futuras pérdidas de información con la asesoría de personas expertas.

**Control de Riesgos.** Es una técnica diseñada para minimizar la posible pérdida de información causada por los riesgos a que esté expuesta la organización. Para el hotel, el establecimiento de riesgos implica confiabilidad e integridad de la información; eficacia y eficiencia de las operaciones; control de los recursos de todo tipo a disposición de la entidad y cumplimiento de las leyes, reglamentos, políticas y contratos.

Por lo descrito anterior se hace de vital necesidad diseñar un mapa de administración de riesgos orientado a la administración de impactos, su incidencia y riesgos en el almacenamiento y retroalimentación de la información. Establecimiento de riesgos para minimizar posibles amenazas presentes en el departamento de sistemas del hotel Tarigua tomando como referencia los dominios especificados.

**Tabla 4.**

*Establecimiento de riesgos ante amenazas presentes tomando como referencia dominios de la norma ISO 27001, pertinentes para el Hotel Tarigua Ocaña S.A.S,*

| RIESGO | DESCRIPCIÓN DEL RIESGO | POSIBLES CONSECUENCIAS DEL RIESGO | PLAN MANEJO Y MINIMIZACIÓN DEL RIEGO | PODERACIÓN DEL RIESGO |
|---|---|---|---|---|
| **Uso indebido de información** | Desorganización en el flujo de información | Presentación de informes contradictorios | Adquisición de un software para el almacenamiento de la información del Hotel, evitando de esta manera la adulteración de la misma | Riesgo Alto |
| | Carencia de indicadores de gestión y de resultados. | Baja calidad técnica en los informes | | |
| | Manipulación de la información | Poco análisis de resultados | | |
| | La entrega de información no es oportuna, confiable y segura | Desconocimiento de aumentos de gastos y costos | | |
| | Retardo injustificado en datos, e informes finales | Decisiones inadecuadas. | Soportes de la información financiera en tiempos oportunos | Riesgo Alto |

*Continuación Tabla 4. Establecimiento de riesgos ante amenazas presentes tomando como referencia dominios de la norma ISO 27001, pertinentes para el Hotel Tarigua Ocaña S.A.S,*

| | | | | |
|---|---|---|---|---|
| **Atraso en la información administrativa, contable y financiera** | Los estados financieros no son utilizados como herramienta básica para la toma de decisiones. | Aplicación inoportuna de correctivos.<br><br>Falta de control y conocimiento real de los bienes o activos fijos de la entidad.<br><br>Falta de algunas conciliaciones por ineficiencia de entidades bancarias en el suministro de la información. | Diseño de un plan de acción fijando metas y objetivos a lograr a corto, mediano o largo plazo | Riesgo Medio |
| **Inadecuado manejo de expedientes y documentos** | La información no fluye de manera eficaz ni cuando se requiere.<br><br>Deficiencia en legalización y resultados de las dependencias | Desorden administrativo | | |

Fuente. Autores del proyecto

## 4.3 Elaborar un documento que guie la gestión del riesgo, presente en el departamento de sistemas del Hotel Tarigua Ocaña S.A.S mediante el diseño de formatos relacionados con la consulta, identificación, tratamiento y valoración de riesgos

De acuerdo con los objetivos planteados durante el desarrollo de la investigación se evidencia que la Norma ISO/IEC 27001 prevé dentro de sus alcances la protección, confidencialidad, integridad y seguridad de la información dentro de las organizaciones, siendo esta la mejor opción para salvaguardarla.

Una vez identificados la presencia de hallazgos, por parte de las autoras de la investigación a través de la auditoria efectuada basada en la ISO/IEC 27001, se optó por diseñar un diagnóstico acerca de los dominios, la metodología y los estándares bajos los cuales se le recomienda a la organización tomar las medidas necesarias que mitiguen los riesgos a los cuales están expuestos actualmente, estableciendo el uso de políticas de seguridad de la información y buenas practicas TI.

La información expuesta basada en la normatividad y el diagnóstico realizado a través de los resultados de la auditoria permiten deducir la urgente necesidad que presenta la empresa a la hora de diseñar políticas de seguridad en pro de salvaguardar sus activos, la calidad del servicio, la organización administrativa y la seguridad y confidencialidad de la información.

A partir de la necesidad presente, las autoras del presente proyecto de investigación desde el aporte académico propone una modelo de guía para establecer los parámetros de seguridad de la información para el Hotel Tarigua S.A.S. ubicado en el municipio de Ocaña en aras de proveer de los recursos normativos y organizacionales y de esta forma contribuir en aspectos tan importantes como la prevención de violaciones a la seguridad, reducir costos, mejorar la organización y dar cumplimiento a lo establecido en el marco legal de Colombia para la seguridad de la información.

Se realizó el diseño de la guía y se encuentra adjunta en el capítulo de los apéndices identificado con el apéndice 3 en busca de contextualizar y dar solución a la problemática de

seguridad que presenta la organización y además de ello estructurar el cumplimiento al objetivo general planteado en la presente investigación.

Buscando mecanismos para la identificación, prevención, minimización, valoración y control del riesgo en el departamento de sistemas del hotel Tarigua producto de la actividad económica que efectúa y optando por salvaguardar la información producida en la empresa se propone el diseño de los siguientes formatos (Ver Apéndices). Los cuales están orientados a mitigar o tratar consecuencias relacionadas con la seguridad de la información producida en la organización.

# Conclusiones

Se realizó un diagnostico situacional donde se evidencio la necesidad de establecer políticas de seguridad de la información que reposa en el departamento de sistemas del hotel Tarigua, la falta de políticas y de un sistema de gestión para la seguridad de la información evidencia inminentes riesgos para la prestación del servicio, mejoramiento de la organización, prevención de violaciones a la seguridad e incumplimiento a las medidas adoptadas por el marco legal en Colombia para la protección, confidencialidad e integridad de la información.

Basados en la Norma ISO/IEC 27001 y en los dominios definidos para el Hotel Tarigua se hace necesario el establecimiento de una política de seguridad de la información, un especial seguimiento para que los controles a través de los dominios propuestos sean el objetivo más asertivo en la consecución de su misión y visión institucional.

Se diseñó la guía para la gestión de riesgos la cual permite establecer un marco teórico práctico sobre la gestión de riesgos como mecanismo de control y mejoramiento del departamento de sistemas del hotel Tarigua Ocaña S.A.S.

# Recomendaciones

El trabajo de investigación a través de sus autoras recomienda a través de los órganos directivos del Hotel Tarigua S.A.S. que en aras de un reconocimiento y mejoramiento de sus procesos implemente dentro de su organización la auditoria constante como una medida de evaluar y hallar las debilidades y fortalezas en el proceso de protección de la seguridad de la información.

A partir de las actividades de auditoria es preciso que la organización direccione su planeación encaminada al mejoramiento continuo y a la puesta en marcha de una política de seguridad de la información que priorice sobre los dominios que establece la norma ISO/IEC 27001 y la metodología del ciclo Deming asociada a planear, hacer, verificar y actuar, se debe establecer dentro de las políticas de seguridad un acuerdo de confidencialidad para cada uno de los empleados del hotel en el momento de su contratación o cuando haya algún cambio de puesto de trabajo, que contemple los requerimientos para proteger la información, utilizando términos legalmente ejecutables y especificando entre otros aspectos, el tipo de información que debe protegerse, la duración esperada del acuerdo, las responsabilidades para usar información confidencial, así como para evitar su divulgación, condiciones específicas de terminación del contrato laboral y las sanciones impuestas para los casos de incumplimiento de dicho acuerdo.

Implementar un proceso de gestión bajo estándares internacionales reconocidos y probados, para minimizar el impacto sobre la empresa, por eventos no intencionados como

desastres naturales, accidentes, fallas en los equipos o cualquier otro incidente cometido de forma deliberada.

# Referencias

Acevedo Juarez, H. (8 de 11 de 2011). ISO 27001. Obtenido de http://www.magazcitum.com.mx/?p=1574#.WOJjcaU2vIU.

Aguirre Tobar, R. A., & Sambrano Ordoñez, A. F. (2015). Estudio para la implemenatción del sistema de gestión de seguridad de la información para la secretaria de educación depertamental de Nariño basado en la norma ISO/IEC 27001. Pasto.

Banco Central de Uruguay. (1999). Estándar australiano administración de riesgos. AS/NZS 4360:1999. Montevideo.

Blog especializado en sisetma de gestion de seguridad de la información. (23 de Abril de 2015). http://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/. Obtenido de La importancia de la norma ISO 27001.

Bosca, J. E., & M.J, M. (2004). Efectos Macroeconómicos de las Inversiones en Infraestructuras Públicas. Valencia.

BSI. (10 de Septiembre de 2016). http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/. Obtenido de Norma ISO/IEC 27001 - Gestión de la Seguridad de la Información.

Bsigroup.com. (2017). https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/. Obtenido de Sistema de gestión ISO/IEC 27001 de Seguridad de la Información.

Burgos Salazar, J., & Campos, P. (2012). Modelo Para Seguridad de la Información en TIC . Chile: Universidad del Bío-Bío.

Calder, A. (2006). Nueve Claves para el Éxito: Una visión general de la implementación de la norma NTC – ISO/IEC 27001. Bogota : nstituto Colombiano de Normas Técnicas y Certificación ICONTEC.

Cámara de comercio Ocaña. (2017). Certificado de representacion legal. Ocaña.

Castro Toro, J. P. (2010). Compilacion bibliografica. Manizales: Universidad de Caldas.

Certificación, I. C. (2011). Gestión del riesgo, Vocabulario. GTC 137. Bogotá: Icontec.

codejobs.biz. (2012). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? . Recuperado el 01 de Mayo de 2018, de https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Congreso de Colombia. (1 de Agosto de 2015). http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf. Obtenido de Ley 1273 del 5 de enero de 2009.

Congreso de Colombia. (1 de Agosto de 2015). Ley estatutaria No. 1266 del 31 de diciembre de 2008. Obtenido de http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf.

Congreso de la Republica, Ley 1273 del 5 de enero de 2009. Recuperado el 01 de Mayo de 2018, de http://www.mintic.gov.co/portal/604/w3-article-3705.html

El tiempo. (20 de Agosto de 2014). Cada segundo se crean 4 nuevos virus informáticos. Obtenido de http://www.eltiempo.com/archivo/documento/CMS-14408656.

Estándar Australiano. (2017). AS/NZS 4360:1999, administracion de riesgos. Bogotá.

Federación Internacional de Sociedades de la Cruz Roja. (2010). Que es la vulnerabilidad.

Figuerola, N. (2013). Análisis Cuantitativo de los Riesgos Propósito, Técnicas y Utilidad. Buenos Aires.

Giraldo Cepeda, L. E. (s.f.). Analisis para la implementacion de un sistema de gestión de la seguridad de la información segun la norma ISO 27001 en la empresa SERVIDOC S.A.

Giraldo Cepedan, L. E. (2016). Analisis para la implementacion de un sistema de gestión de la seguirdad de la información segun la norma ISO 27001 en al empresa SERVIDOC S.A. Cali: Universidad Abierta y a Distancia Unad.

Hack Hispano. (2017). Comunidad de seguridad informatica y nuevas tecnologias. España.

Instituto Colombiano de Normas Técnicas y Certificación. (2011). Gestión del riesgo, principios y directrices. NTC-ISO 31000. Bogotá: Icontec.

Instituto Colombiano de Normas Técnicas y Certificación. (2011). Gestión del riesgo, Vocabulario. GTC 137:2011. Bogotá: Icontec.

iso27000. (s.f.). Recuperado el 01 de Mayo de 2018, de Sistema de Gestión de la Seguridad de la Informacion: http://www.iso27000.es/download/doc_sgsi_all.pdf

Ministerio de las TIC. (2017). https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf. Obtenido de Seguridad y privacidad de lainformación.

Ministerio de las TICs. (28 de Octubre de 2016). http://www.mintic.gov.co/gestionti/615/w3-article-5482.html. Obtenido de Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ministerio de tecnologia de la infromación y la comunicación. (12 de Julio de 2012). http://www.mintic.gov.co/portal/604/articles-5259_doc_pdf.pdf. Obtenido de Infrome de gestion.

Paez Garcia, L. E. (2009). Historia de la Región de Ocaña. . Bogotá: Jaguar Group Producciones.

Perafan Ruiz, J. J., & Caicedo Cuchimba, M. (2014). Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Popayan.

Reporte digital. (2017). Los beneficios y la importancia de gestionar la seguridad de la información. Obtenido de http://reportedigital.com/seguridad/importancia-gestionar-seguridad-informacion/.

República de Colombia. (2012). Constitucion Política de Colombia. Bogotá: Cupido.

República de Colombia. (2012). Ley 1581 de 2012. Bogotá.

Reyes, M. (2014). Seguridad En Los Sistemas Informaticos. Recuperado el 01 de Mayo de 2018, de http://marareyes79.blogspot.com.co/2014/08/normal-0-21-false-false-false-es-ec-x_30.html

RM, H. (2010). Los seguros y la seguridad después del 11 de Septiembre: ¿Acaso el mundo se ha vuelto un lugar más "riesgoso"? Recuperado el 01 de Mayo de 2018, de http://www.cholonautas.edu.pe/modulo/upload/Segur.pdf

Sanso, R. (2011). Psicología aplicada a la seguridad informática.

Seguros y pensiones para todos. (1 de Septiembre de 2016). Riesgos. Obtenido de https://segurosypensionesparatodos.fundacionmapfre.org/syp/es/seguros/definicion-seguro-asegurar/el-riesgo-asegurar/que-es-el-riesgo-asegurar/.

Sgs.co. (2017). http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx. Obtenido de ISO 27001:2013 – Sistema de Gestión de seguridad de la información.

Tocabens, B. E. (2011). Definiciones acerca del riesgo y sus implicaciones. Revista Cubana de Higiene y Epidemiología. Recuperado el 01 de Mayo de 2018, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1561-30032011000300014

Tola Franco, D. E. (2015). Implementacin de un sistema de seguridad en la información para la empresa con sultoria y auditoria aplicando la norma ISO/IEC 27001". Guayaquil: Escuela superior politecnica del litoral.

Tola Franco, D. I. (s.f.). Implementación de un sistema de gestión de seguridad de la información información para una empresa de consultoria y auditoria, aplicando la Norma ISO/IEC 27001.

Unisdr. (2004). https://www.unisdr.org/2004/campaign/booklet-spa/page4-spa.pdf. Obtenido de Amenazas.

Vargas, A. C. (Agosto de 2016). http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf. Obtenido de Que es el sistema de gestión de seguridad de la información.

Villalon Huertas, A. (29 de Octubre de 2016). http://www.shutdown.es/ISO17799.pdf. Obtenido de Sistema de gestion de seguridad de la información.

# Apéndices

**Apéndice A.** Certificado de Cámara de comercio

CAMARA DE COMERCIO DE OCANA
CERTIFICADO EXPEDIDO A TRAVES DEL PORTAL DE SERVICIOS VIRTUALES (SII)
CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL
HOTEL TARIGUA OCAÑA SAS
Fecha expedición: 2017/03/01 - 17:12:10, Recibo No. S000005661, Operación No. 01K010301026

**CODIGO DE VERIFICACIÓN: 3XcuWzA3Kc**

LA MATRÍCULA MERCANTIL PROPORCIONA SEGURIDAD Y CONFIANZA EN LOS NEGOCIOS
RENUEVE SU MATRÍCULA A MÁS TARDAR EL 31 DE MARZO Y EVITE SANCIONES DE HASTA 17 S.M.L.M.V

CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL O INSCRIPCION DE DOCUMENTOS.
LA CAMARA DE COMERCIO DE OCAÑA , CON FUNDAMENTO EN LAS MATRICULAS E INSCRIPCIONES DEL REGISTRO MERCANTIL,

CERTIFICA:

NOMBRE : HOTEL TARIGUA OCAÑA SAS
N.I.T: 900471948-1
DIRECCION COMERCIAL:CARRERA 12 8-47
BARRIO COMERCIAL: EL TORITO
DOMICILIO : OCAÑA
TELEFONO COMERCIAL 1: 5625424
TELEFONO COMERCIAL 2: 3106067667
DIRECCION DE NOTIFICACION JUDICIAL :CARRERA 12 8-47
BARRIO NOTIFICACION: EL TORITO
DIRECION PAGINA WEB (URL) : www.hoteltarigua.com
MUNICIPIO JUDICIAL: OCAÑA
E-MAIL COMERCIAL:hoteltarigua@hotmail.com

E-MAIL NOT. JUDICIAL:hoteltarigua@hotmail.com

TELEFONO NOTIFICACION JUDICIAL 1: 5625424
TELEFONO NOTIFICACION JUDICIAL 2: 3106067667
FAX NOTIFICACION JUDICIAL:

CERTIFICA:

QUE EL MATRICULADO TIENE LA CONDICION DE PEQUEÑA EMPRESA DE ACUERDO CON LO ESTABLECIDO EN EL NUMERAL 1 DEL ARTÍCULO 2 DE LA LEY 1429 DE 2010.

CERTIFICA:

ACTIVIDAD PRINCIPAL:
5511 ALOJAMIENTO EN HOTELES

CERTIFICA:

ACTIVIDAD SECUNDARIA:
5611 EXPENDIO A LA MESA DE COMIDAS PREPARADAS

ACTIVIDAD ADICIONAL 1:
5621 CATERING PARA EVENTOS

CERTIFICA:

MATRICULA NO. 00022742
FECHA DE MATRICULA EN ESTA CAMARA: 21 DE OCTUBRE DE 2011

********** CONTINUA **********

Pag. 1 de 5

RENOVO EL AÑO 2016 , EL 17 DE MARZO DE 2016

CERTIFICA:

CONSTITUCION : QUE POR ACTA DE NOTARIA SEGUNDA DE OCAÑA DEL 10 DE SEPTIEMBRE DE 2011 , INSCRITA EL 21 DE OCTUBRE DE 2011 BAJO EL NUMERO 00002478 DEL LIBRO IX,
SE CONSTITUYO LA PERSONA JURIDICA: HOTEL TARIGUA OCAÑA SAS

CERTIFICA:

REFORMAS:

| DOCUMENTO | FECHA | ORIGEN | CIUDAD | INSCRIPCION | FECHA |
|---|---|---|---|---|---|
| 0000005 | 2014/02/13 | ASAMBLEA EXTRAORDINAOCA | | 00003071 | 2014/02/18 |

CERTIFICA:

VIGENCIA: QUE EL TERMINO DE DURACION DE LA PERSONA JURIDICA ES INDEFINIDO

CERTIFICA:

OBJETO SOCIAL: LA SOCIEDAD TENDRA COMO OBJETO PRINCIPAL PRESTAR, PROMOVER Y COMERCIALIZAR LOS SERVICIOS DE ALOJAMIENTO, TURISMO, AGENCIAS DE VIAJES, GASTRONOMICOS ( RESTAURANTE Y CAFETERI A) RECREATIVOS, DESARROLLAR LA ACTIVIDAD DE EVENTOS Y CONGRESOS; ASI MISMO, PODRA RELIZAR CUALQUIER OTRA ACTIVIDAD ECONOMICA LICITA TANTO EN COLOMBIA COMO EN EL EXTRANJERO; LA SOCIEDAD PODRA LLEVAR A CABO, EN GENERAL, TODAS LAS OPERACIONES, DE CUALQUIER NATURALEZA QUE ELLAS FUEREN, RELACIONADAS CON EL OBJETO MENCIONADO, ASI COMO CUALESQUIERA ACTIVIDADES SIMILARES, CONEXAS O COMPLEMENTARIAS QUE PERMITAN FACILITAR O DESARROLLAR EL COMERCIO O LA INDUSTRIA DE LA SOCIEDAD; EN DESARROLLO DE SU OBJETO LA SOCIEDAD PODRA ADQUIRIR, ARRENDAR GRAVAR Y ENAJENAR INMUEBLES Y OTROS BIENES MUEBLES Y DEMAS ARTICULOS RELACIONADOS CON EL, DAR O RECIBIR DINERO EN MUTUO, CELEBRAR TODA CLASE DE ACTOS O CONTRATOS NECESARIOS O CONVENIENTES PARA EL DESARROLLO DEL OBJETO PRINCIPAL, RECIBIR O DAR EN HIPOTECA O PRENDA LOS BIENES MUEBLES O INMUEBLES DE LA SOCIEDAD EN GARANTIA DE LAS OPERACIONES QUE CELEBRE, NEGOCIAR TODA CLASE DE TITULOS VALORES, OTORGADOS, ENDOSARLOS, PAGARLOS, DESCARGARLOS ETC. Y EN GENERAL TODA CLASE DE OPERACIONES COMERCIALES O FINANCIERAS QUE SE RELACIONEN DIRECTAMENTE CON EL OBJETO SOCIAL.

CERTIFICA:

CAPITAL:

********** CONTINUA **********

CAMARA DE COMERCIO DE OCANA
CERTIFICADO EXPEDIDO A TRAVES DEL PORTAL DE SERVICIOS VIRTUALES (SII)
CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL
HOTEL TARIGUA OCAÑA SAS

Cámara de Comercio de Ocaña

Fecha expedición: 2017/03/01 - 17:12:10, Recibo No. S000005661, Operación No. 01K010301026

**CODIGO DE VERIFICACIÓN: 3XcuWzA3Kc**

**LA MATRÍCULA MERCANTIL PROPORCIONA SEGURIDAD Y CONFIANZA EN LOS NEGOCIOS**
**RENUEVE SU MATRÍCULA A MÁS TARDAR EL 31 DE MARZO Y EVITE SANCIONES DE HASTA 17 S.M.L.M.V**

** CAPITAL AUTORIZADO **
VALOR :$500,000,000.00
NO. DE ACCIONES:500,000.00
VALOR NOMINAL :$1,000.00
** CAPITAL SUSCRITO **
VALOR :$350,000,000.00
NO. DE ACCIONES:350,000.00
VALOR NOMINAL :$1,000.00
** CAPITAL PAGADO **
VALOR :$350,000,000.00
NO. DE ACCIONES:350,000.00
VALOR NOMINAL :$1,000.00

CERTIFICA:

** NOMBRAMIENTOS : **
QUE POR ACTA DE NOTARIA SEGUNDA DEL 10 DE SEPTIEMBRE DE 2011 , INSCRITA EL 21 DE OCTUBRE DE 2011 BAJO EL NUMERO 00002478 DEL LIBRO IX , FUE(RON) NOMBRADO(S):

| NOMBRE | IDENTIFICACION |
|---|---|
| REPRESENTANTE LEGAL | |
| VERA CASTILLO PEDRO JULIO | C.C.00013363993 |

CERTIFICA:

REPRESENTACION LEGAL: LA REPRESENTACION LEGAL DE LA SOCIEDAD POR ACCIONES SIMPLIFICADA ESTARA A CARGO DE UNA PERSONA NATURAL O JURIDICA, ACCIONISTA O NO, QUIEN NO TENDRA SUPLENTES; EN AQUELLOS CASOS EN QUE EL REPRESENTANTE LEGAL SEA UNA PERSONA JURIDICA, LAS FUNCIONES QUEDARAN A CARGO DEL REPRESENTANTE LEGAL DE ESTA; FACULTADES: LA SOCIEDAD SERA GERENCIADA, ADMINISTRADA Y REPRESENTADA LEGALMENTE ANTE TERCEROS POR EL REPRESENTANTE LEGAL, QUIEN NO TENDRA RESTRICCIONES DE CONTRATACION POR RAZON DE LA NATURALEZA NI DE LA CUANTIA DE LOS ACTOS QUE CELEBRE; POR LO TANTO, SE ENTENDERA QUE EL REPRESENTANTE LEGAL PODRA CELEBRAR O EJECUTAR TODOS LOS ACTOS Y CONTRATOS COMPRENDIDOS EN EL OBJETO SOCIAL O QUE SE RELACIONEN DIRECTAMENTE CON LA EXISTENCIA Y EL FUNCIONAMIENTO DE LA SOCIEDAD; EL REPRESENTANTE LEGAL SE ENTENDERA INVESTIDO DE LOS MAS AMPLIOS PODERES PARA ACTUAR EN TODAS LAS CIRCUNSTANCIAS EN NOMBRE DE LA SOCIEDAD, CON EXCEPCION DE AQUELLAS FACULTADES QUE, DE ACUERDO CON LOS ESTATUTOS, SE HUBIEREN RESERVADO LOS ACCIONISTAS; EN LAS RELACIONES FRENTE A TERCEROS, LA SOCIEDAD QUEDARA OBLIGADA POR LOS ACTOS Y CONTRATOS CELEBRADOS POR EL REPRESENTANTE LEGAL; LE ESTA PROHIBIDO AL REPRESENTANTE LEGAL Y A LOS DEMAS ADMINISTRADORES DE LA SOCIEDAD, POR SI O POR INTERPUESTA PERSONA, OBTENER BAJO CUALQUIER FORMA O MODALIDAD JURIDICA PRESTAMOS POR PARTE DE LA SOCIEDAD U OBTENER DE PARTE DE LA SOCIEDAD AVAL, FIANZA O

********** CONTINUA **********

CUALQUIER OTRO TIPO DE GARANTIA DE SUS OBLIGACIONES PERSONALES. 4. EL REPRESENTANTE LEGAL, QUEDA FACULTADO PARA GRAVAR CON HIPOTECA, PRENDA O CUALQUIER OTRA LIMITACIÓN AL DOMINIO, LOS BIENES INMUEBLES DE PROPIEDAD DE LA SOCIEDAD, CON EL ÚNICO Y EXCLUSIVO FIN DE GARANTIZAR LAS OBLIGACIONES QUE ADQUIERA CON ENTIDADES FINANCIERAS O TERCEROS, TANTO LA SOCIEDAD HOTEL TARIGUA OCAÑA SAS, COMO SUS SOCIOS PEDRO JULIO VERA CASTILLO Y/O RUTH CRIADO ROJAS, O AQUELLAS PERSONAS, QUE SEAN DEBIDAMENTE DETERMINADAS EN UN ACTA DE JUNTA DE SOCIOS, DEBIDAMENTE REALIZADA Y APROBADA POR LOS SOCIOS POR UNANIMIDAD.

CERTIFICA:

QUE LA PERSONA JURIDICA TIENE MATRICULADOS LOS SIGUIENTES ESTABLECIMIENTOS :

NOMBRE : HOTEL TARIGUA OCAÑA
MATRICULA NO. 00022743 DEL 21 DE OCTUBRE DE 2011
RENOVACION DE LA MATRICULA : EL 17 DE MARZO DE 2016
ULTIMO AÑO RENOVADO : 2016

CERTIFICA:

ACTIVIDAD PRINCIPAL:
5511 ALOJAMIENTO EN HOTELES

CERTIFICA:

ACTIVIDAD SECUNDARIA:
5611 EXPENDIO A LA MESA DE COMIDAS PREPARADAS

ACTIVIDAD ADICIONAL 1:
5621 CATERING PARA EVENTOS

CERTIFICA:

QUE NO FIGURAN INSCRIPCIONES ANTERIORES A LA FECHA DEL PRESENTE CERTIFICADO, QUE MODIFIQUEN TOTAL O PARCIALMENTE SU CONTENIDO.

DE CONFORMIDAD CON LO ESTABLECIDO EN EL CODIGO DE PROCEDIMIENTO ADMINISTRATIVO Y DE LO CONTENCIOSO Y DE LA LEY 962 DE 2005, LOS ACTOS ADMINISTRATIVOS DE REGISTRO AQUI CERTIFICADOS QUEDAN EN FIRME DIEZ (10) DIAS HABILES DESPUES DE LA FECHA DE INSCRIPCION, SIEMPRE QUE NO SEAN OBJETO DE RECURSOS.

**VALOR DEL CERTIFICADO: $5,200**



********** CONTINUA **********

CAMARA DE COMERCIO DE OCANA
CERTIFICADO EXPEDIDO A TRAVES DEL PORTAL DE SERVICIOS VIRTUALES (SII)
CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL
HOTEL TARIGUA OCAÑA SAS
Fecha expedición: 2017/03/01 - 17:12:10, Recibo No. S000005661, Operación No. 01K010301026

## CODIGO DE VERIFICACIÓN: 3XcuWzA3Kc

**LA MATRÍCULA MERCANTIL PROPORCIONA SEGURIDAD Y CONFIANZA EN LOS NEGOCIOS**
**RENUEVE SU MATRÍCULA A MÁS TARDAR EL 31 DE MARZO Y EVITE SANCIONES DE HASTA 17 S.M.L.M.V**

La firma digital no es una firma digitalizada o escaneada, por lo tanto, la firma digital que acompaña este documento la podrá verificar a través de su aplicativo visor de documentos pdf.

No obstante, si usted va a imprimir este certificado, lo puede hacer desde su computador, con la certeza de que el mismo fue expedido a través del canal virtual de la cámara de comercio y que la persona o entidad a la que usted le va a entregar el certificado impreso, puede verificar por una sola vez el contenido del mismo, ingresando al enlace http://siiocana.confecamaras.co/cv.php seleccionando allá la cámara de comercio e indicando el código de verificación 3XcuWzA3Kc.

Al realizar la verificación podrá visualizar (y descargar) una imagen exacta del certificado que fue entregado al usuario en el momento que se realizó la transacción.

La firma mecánica que se muestra a continuación es la representación gráfica de la firma del secretario jurídico (o que haga sus veces) de la Cámara de Comercio quien avala este certificado. La firma mecánica no reemplaza la firma digital en los documentos electrónicos.

Melisa Lorena Ávila Ariza.

**Apéndice B.** Guía para la gestión de riesgos

La guía contiene aspectos esenciales a considerar para gestionar riesgos, cuya base son los estándares ISO 27001. 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. 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.

## POLÍTICA DE GESTIÓN DEL RIESGO

Establecer, formalizar y poner en práctica una metodología integral para la gestión del riesgo. Definir y establecer el nivel aceptable de los riesgos, contar con la aprobación explícita de los planes de mitigación de los riesgos, realizar evaluaciones periódicas de los procedimientos en uso para el control de los riesgos y mantener informadas a las partes involucradas sobre el estado y el perfil de riesgos del hotel.

Los lineamientos, principios y definiciones que se mencionan a continuación y el modelo de gestión a usar que se explica más adelante, constituyen la base sobre la cual aplica la Política de Gestión de Riesgos.

## OBJETIVOS

Mejorar la seguridad del hotel, 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.

## 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.

## VALORACIÓN DEL RIESGO

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

**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:

Identificación de riesgos

| 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 cinco categorías: personas, materiales, equipos, instalaciones y entorno. | Cada fuente de riesgo tiene numerosos componentes, que pueden dar lugar a un riesgo. Las fuentes genéricas de riesgo incluyen:<br>Relaciones comerciales y<br><br>legales:<br>Entre la organización y otras organizaciones (proveedores, arrendatarios, subcontratistas).<br>Circunstancias económicas: De la organización, país, internacionales como factores que contribuyen a esas circunstancias (tipos de cambio).<br>Comportamiento humano: Involucrados y no involucrados en la organización.<br>Eventos naturales.<br>Circunstancias políticas: Incluyendo cambios legislativos y factores que pueden influenciar a otras fuentes. |

| | | |
|---|---|---|
| | | Aspectos tecnológicos y técnicos (internos o externos).<br>Actividades y controles gerenciales.<br>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:<br>Base de activos y recursos de la organización, incluyendo al personal.<br>Ingresos y derechos.<br>Costos de las actividades, tanto directos como indirectos.<br>Personas.<br>Comunidad.<br>Desempeño.<br>Cronograma y programa de actividades.<br>El ambiente.<br>Intangibles tales como la imagen organizacional, gestos<br>Pág. 18-27<br><br>de buena voluntad, calidad de vida.<br>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 | Incumplimiento de los protocolos de selección e incorporación de personal. |

| | | |
|---|---|---|
| | identificadas en el formato de contexto estratégico. | |
| **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, sanciones, pérdidas económicas, de información, de imagen, de credibilidad y confianza, interrupción del servicio y daño ambiental. | Investigaciones disciplinarias, penales, etc.<br>Desprestigio de la imagen organizacional |

Fuente. Autoras del proyecto

**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.

## 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. 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.

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

**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. 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.

**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 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.

## 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.

**Apéndice C.** Formato de comunicación y consulta de riesgos.

El presente formato se diseña con el fin de identificar y clasificar riesgos con sus respectivas causas y consecuencias

| | | |
|---|---|---|
| HOTEL TARIGUA<br>MATRICULA N° 00022743 Octubre del 2.011<br><br>COMUNICACIÓN Y CONSULTA DE RIESGOS | Código: | |
| | Versión: | |
| | Elaborado: | |
| | Página: | |

| **COMUNICACIÓN – VERIFICACIÓN DE RIESGOS** | | |
|---|---|---|
| COMUNICANTE | Fecha: | Dependencia: |
| | Nombre: | Cargo: |

| | |
|---|---|
| **COMUNICADO** | Riesgo Identificado : |
| | Posibles Causas: |
| | Posibles Consecuencias: |

Formato de valoración y tratamiento del riesgo

| | | |
|---|---|---|
| HOTEL TARIGUA<br>MATRICULA N° 00022743 Octubre del 2.011<br><br>COMUNICACIÓN Y CONSULTA DE RIESGOS | Código: | |
| | Versión: | |
| | Elaborado: | |
| | Página: | |

**Valoración – Ponderación del Riesgo**

**Opción Tratamiento**

| 1 | 2 | 3 | 4 |
|---|---|---|---|

(I) Impacto

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

(P) Probabilidad

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

(N) Nivel Riesgo

| 1 | 2 | 3 | 4 |
|---|---|---|---|

| ACCIONES/ DECISIONES TOMADAS | FECHA | RESPONSABLE(S) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

**Conclusiones:**

| HOTEL TARIGUA<br>MATRICULA N° 00022743 Octubre del 2.011<br><br>COMUNICACIÓN Y CONSULTA DE RIESGOS | Código: | |
|---|---|---|
| | Versión: | |
| | Elaborado: | |
| | Página: | |

**Recomendaciones efectuadas por el responsable para minimizar el 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 | | |

**Apéndice D.** Formato de establecimiento del contexto.

| | | |
|---|---|---|
| ESTABLECIMIENTO DEL CONTEXTO | Código: | |
| | Versión: | |
| | Elaborado: | |
| | Página: | |

| **ESTABLECIMIENTO DEL CONTEXTO** |
|---|
| Empresa o Dependencia: |
| Proceso: |
| Objetivo: |
| Alcance: |
| Responsable: |

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

| | |
|---|---|
| Elaborado Por: | Fecha: |
| Revisado Por: | Fecha: |
| Aprobado Por: | Fecha: |

**Apéndice E.** Formato de valoración y tratamiento de riesgos.

| | | |
|---|---|---|
| HOTEL TARIGUA<br>MATRICULA N° 00022743 Octubre del 2.011<br><br>VALORACIÓN Y TRATAMIENTO DE RIESGOS | Código: | |
| | Versión: | |
| | Elaborado: | |
| | Página: | |

| **Empresa o Dependencia:** | | | | | | |
|---|---|---|---|---|---|---|
| **Responsable:** | | | | | | |
| **IDENTIFICACIÓN DE RIESGOS** | | | | | | |
| **Clasificación del riesgo** | **Riesgo** | **Fuente de Riesgo** | **Área de Impacto** | **Evento – Efecto** | **Causas** | **Consecuencias** |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | | |
|---|---|---|
| HOTEL TARIGUA<br>MATRICULA N° 00022743 Octubre del 2.011<br><br>VALORACIÓN Y TRATAMIENTO DE RIESGOS | Código: | |
| | Versión: | |
| | Elaborado: | |
| | Página: | |

| **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** | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

| | | |
|---|---|---|
| HOTEL TARIGUA<br>MATRICULA N° 00022743 Octubre del 2.011<br><br>VALORACIÓN Y TRATAMIENTO DE RIESGOS | Código: | |
| | Versión: | |
| | Elaborado: | |
| | Página: | |

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

| | |
|---|---|
| Elaborado Por: | Fecha: |
| Revisado Por: | Fecha: |
| Aprobado Por: | Fecha: |

**Apéndice F.** Formato de monitoreo y revisión de riesgos.

| | | |
|---|---|---|
| HOTEL TARIGUA<br>MATRICULA N° 00022743 Octubre del 2.011<br><br>MONITOREO Y REVISIÓN DE RIESGOS | Código: | |
| | Versión: | |
| | Elaborado: | |
| | Página: | |

| **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: |