RESUMEN – TRABAJO DE GRADO

AUTORES	**GINA PAOLA CLARO ROPERO** **JESUS EDUARDO ESPINEL BLANCO**
FACULTAD	**DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS**
DIRECTOR	**RODRÍGUEZ CHINCHILLA ANA MELISSA**
TÍTULO DE LA TESIS	**PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MOTEL DUBAI, COMO MEDIDA DE PROTECCIÓN A LAS ÁREAS VITALES DE LA EMPRESA**

RESUMEN
(70 palabras aproximadamente)

LA EMPRESA DUBÁI IDENTIFICA LA NECESIDAD DE GARANTIZAR DE FORMA FUNDAMENTAL LA INFORMACIÓN Y ACCESO A LAS ÁREAS IMPORTANTES, PARA LLEVAR A CABO EL PROYECTO, SE HIZO NECESARIO INICIALMENTE REALIZAR UN DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA MOTEL DUBÁI; LUEGO SE REVISÓ Y ESTABLECIÓ DESDE EL PUNTO DE VISTA DE LOS PROCESOS MISIONALES SU ESTADO DE MADUREZ, FRENTE A LOS REQUERIMIENTOS METODOLÓGICOS Y DE ACUERDO A LOS DOMINIOS Y CONTROLES.

CARACTERÍSTICAS

PÁGINAS: 137	PLANOS: 0	ILUSTRACIONES:6	CD-ROM:1

PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL MOTEL DUBAI, COMO MEDIDA DE PROTECCIÓN A LAS ÁREAS VITALES DE LA EMPRESA

AUTORES

GINA PAOLA CLARO ROPERO

JESUS EDUARDO ESPINEL BLANCO

proyecto de grado como requisito para obtener el grado de Especialista en Auditoria de Sistemas

DIRECTORA

IS. Esp. MSc (c) ANA MELISSA RODRÍGUEZ CHINCHILLA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia **Agosto, 2019**

Índice

Lista de figuras

Lista de figuras

Lista de apéndices

Resumen

La empresa Dubái identifica la necesidad de garantizar de forma fundamental la información y acceso a las áreas importantes, para llevar a cabo el proyecto, se hizo necesario inicialmente realizar un diagnóstico de la situación actual de la gestión de la seguridad de la información en la empresa motel Dubái; Luego se revisó y estableció desde el punto de vista de los procesos misionales su estado de madurez, frente a los requerimientos metodológicos y de acuerdo a los dominios y controles.

En el presente documento se trabaja la creación de un plan de seguridad de la información a una empresa dedicada al sector de alojamiento. consta de las diferentes etapas que componen el plan de seguridad de la norma ISO IEC- 27001:2013, para esto se hizo un análisis de riesgos inicial, para identificar los activos críticos que podrían comprometer la continuidad del negocio en caso de incidente. Con este análisis inicial, posteriormente se analizarán las amenazas que pueden afectar a la empresa sujeta al análisis y con ello se obtendrán los resultados de los activos que se encuentran en riesgo potencial. A partir de estos resultados podrán diseñarse las estrategias necesarias para acercar a niveles óptimos la seguridad de los activos de la organización.

En el documento también se puede encontrar una auditoría interna y de cumplimiento con el objetivo de detectar la situación actual en la que se encuentra la organización y poder obtener un punto de partida a partir del cual comenzar a elaborar el plan de seguridad

Introducción

Las Tecnologías de Información y Comunicación (TIC) como se les conoce en la actualidad, las podemos observar a simple vista que están en continua mejora todos los días, lo cual está generando una mayor conciencia y a su vez está cambiando ese paradigma donde la seguridad, confiabilidad, disponibilidad de la información juegan un papel fundamental para protección de los activos de las empresas, permitiéndoles obtener buenos resultados salvaguardando mediante estrategias y lineamientos que son reconocidos mundialmente de posibles amenazas internas y externas que se enfrentan las organizaciones.

Por este motivo es que con el presente trabajo se busca diseñar, con el propósito de ofrecer mediante una herramienta como lo es un plan de gestión de seguridad de la información, que será fundamental para su elaboración guiar con los lineamientos de la norma NTC-ISO-IEC 27001:2013, que proporcione obtener una mayor claridad y conciencia de los empleados actuales de la empresa motel Dubai, lo fundamental y crítico que es proteger la información, de ser muy celosos con este activo tan esencial; de la misma forma logrando esto permitirá a los empleados y directivas a desempeñar sus labores de una condición óptima, generando garantías, confidencialidad, integridad y disponibilidad de la información.

Capítulo 1. Plan de gestión de seguridad de la información para el Motel Dubai, como medida de protección a las áreas vitales de la empresa.

1.1 Planteamiento del problema

En la actualidad las empresas están enfocando sus procesos en la utilización de tecnologías de información y comunicación TIC, para la administración segura, confiable e integra de toda la información que manejan; esto les ha permitido a las empresas el acceso, manipulación y resguardo de forma confiable permitiendo que los servicios ofrecidos y procesos internos continúen mejorando. En la industria dedicada al servicio de alojamiento, se conocen como aquellos establecimientos que suministran principalmente un servicio de hospedaje con o sin alimentación para usuarios ya sean permanentes o pueden ser transeúntes de este sector comercial el cual comprende además una serie de oferta variada, dentro de esta industria podemos encontrar a aquellos establecimientos que se dediquen a hospedería con pocas habitaciones, los que suministren alojamiento con fines específicos como este tipo de establecimientos que asimismo de privilegiar la discreción con la privacidad, ofrecen atractivos para una estancia cómoda y conforme a las necesidades.

Este sector de comercio o industria parece haber dado un vuelco muy notable en la actualidad, los moteles dejaron atrás la noción de zonas vistas como un tabú, para convertirse en espacios de un nivel y categoría más alta, con características innovadores, que ofrecen e integran detalles ecológicos, arquitectónicos dando una infraestructura de calidad que permite a los huéspedes hacer su estancia más agradable. Visto desde el punto de vista concreto, comúnmente

los administradores o gerentes de las empresas son los dueños, por tal motivo no establecen planes gestión de seguridad de la información que resguarden los activos de las empresas, una situación que se presenta es los relaciones de amistad con empleados; consintiendo facultades que no son convenientes, generando en vulnerabilidades para la empresa, planteando riesgos y/o fugas de información que perjudican el crecimiento y fortalecimiento empresarial.

Como toda empresa, cuenta con una infraestructura física y lógica que le permite desarrollar su actividad, conllevando que dentro de los activos existe gran cantidad de información, Hablar de vulnerabilidades en las organizaciones es decir de los riesgos que implica el adecuado manejo de la información, “quienes tratan de acceder esta información pueden ocasionar daños a la empresa, para beneficio propio o para simple satisfacción personal”, (Ugas, 2002) se deben tener controles que brinden la protección y así reducir los posibles riesgos.

La empresa carece de un plan de gestión de seguridad que le brinde ciertas garantías permita establecer las directrices para afrontar riesgos de seguridad lo cual lleva a que se den eventos negativos para la empresa como la perdida de activos o daño en equipos; afectando la calidad del servicio lo que de manera directa repercute en la perdida de usuarios; de la misma manera es importante mencionar que al no contar con el plan de gestión de seguridad definida que determine aspectos tan importantes como el control de acceso implica que los empleados puedan realizar manipulación de la información y no se cuente con evidencia de las configuraciones que se hagan, además el personal se siente con atribuciones para ingresar a todas las áreas de la empresa, sin importar las consecuencias de los movimientos que se hagan. (Arévalo, Bayona, & Rico, 2015)

1.2 Formulación del problema

¿El plan de gestión de seguridad de la información permitirá proteger áreas vitales de la empresa?

1. 3 Objetivos

1.3.1 General. Proponer el plan de gestión de seguridad de la información para el Motel Dubai

1.3.2 Específicos. Diagnosticar el estado actual de la seguridad de la información de la empresa.

Identificar los componentes que integraran el plan de gestión de seguridad de información de la empresa de acuerdo a las Normas ISO/IEC 27001:2013.

Establecer el plan de gestión de seguridad de la información mediante un procedimiento que brinde el control necesario a las áreas principales de la empresa.

1.4 Justificación

Las empresas que logran generar una estructura organizada permiten garantizar que sus procesos y/o servicios se elaboren de forma eficiente y de forma controlada que les permite

seguir generando productividad; El establecer un plan de seguridad de la información, aplicarlos y hacerles seguimientos producen resultados beneficiosos para la empresa. Aplicar este plan cimienta la responsabilidad de resguardar los activos y toda la información generada en los procesos de la empresa, de la misma forma es la evidencia de una administración y organización empresarial bien desempeñada, ya que gran porcentaje de las empresas afirman esto. Estas organizaciones subrayan lo fundamental que es la seguridad en el desempeño de sus objetivos de negocio, a pesar de esto no definen claramente las infraestructuras de seguridad que hoy en día existen y manejan, teniendo en cuenta que estas necesitan de un tiempo de reacción, debido que los ataques a la seguridad se efectúan con mayor porcentaje que cada día crece en sus modalidades.

Las empresas a veces no pueden reaccionar ante las nuevas y constantes amenazas de seguridad, esto con el ánimo de lograr disminuir que afecten a su ejercicio comercial, es por esto que administrar la seguridad de la información y sus infraestructuras, sumado al valor de negocio que ofrecen, es la prioridad y causante de preocupación principal, tanto así que la empresa Motel Dubai no es indiferente a ello y se inquieta por implementar los mejores procedimientos y practicas existentes por medio de normas que le permitan fortalecerse como empresa responsable.

Por esa razón el tener el plan de gestión de seguridad definido ayuda de manera precisa permitiendo indicar las pautas, de tal manera que permita hacer cumplir los requerimientos para minimizar los riesgos, contrarrestar los ataques previniendo afectaciones en los principales activos de las organizaciones.

La característica de un plan de gestión de seguridad es prevenir los posibles ataques que se pueden efectuar contra el activo a proteger, también en el caso posible que se genere presencia de amenazas se logre tener registro de los eventos para lograr identificar los responsables y permitir tomar los correctivos e implementar mejores controles (Angarita, Suarez, & Rodriguez, 2014), se debe ser claro al decir que si la organización no cuenta con el plan de gestión de seguridad, lo más seguro es que no sabrá cómo debe actuar, por consiguiente el riesgo es latente, será más vulnerable en todo tiempo, además cuando se fija este control se está dando el instructivo que permitirá prevenir y/o como corregir afectaciones a la información.

1.5 Hipótesis

Un plan de gestión de seguridad que integre las condiciones necesarias para el correcto funcionamiento de la empresa DUBAI, basada en las normas vigentes en Colombia.

1.6 Delimitaciones

1.6.1 Geográfica**.** Este estudio tendrá lugar en la empresa MOTEL Dubai, en la ciudad de Ocaña Norte de Santander.

1.6.2 Conceptual**.** Para la realizar esta propuesta se tendrá en cuenta los siguientes conceptos: plan de gestión, seguridad física, controles de acceso, seguridad de la información, vulnerabilidad, gestión de riesgo, administración, políticas de seguridad de la información.

1.6.3 Temporal**.** La duración de este proyecto será de 6 semanas, pero de ser necesario se ajustará con la aprobación del director y el comité curricular del plan de estudios, desarrollando cada objetivo, a partir de la aprobación del anteproyecto

1.6.4 Operativa**.** Para proteger la imagen corporativa de la empresa donde se desarrollará la actual propuesta se creó la denominación: “Motel Dubai” la cual representa a una empresa del sector motelero de la ciudad de Ocaña; Conformado por las áreas de gerencia, contabilidad y servicios.

Capítulo 2. Marco referencial

2.1 Marco histórico

La seguridad es un tema fundamental y más si es en el ámbito de las TIC, se dice que este tema de seguridad siempre estará atado al factor humano en todos los escenarios, la historia de la seguridad inició con una materia prima para su existencia: un riesgo, un peligro, una amenaza. En este sentido, el escenario de la seguridad física se desarrolló en el contexto de la guerra contra un enemigo, que no buscó otra cosa que vulnerar las estrategias de control y contención, entre otras, que tiene el objetivo atacado, para apoderarse de éste.

"Las definiciones de Gobierno Corporativo varían ampliamente. Bajo una definición restringida, el Gobierno Corporativo es una herramienta para crear una cultura administrativa que permite ofrecer participaciones accionarias para el público en general", (Rodríguez, 2010), Las empresas, no importa su tamaño, la industria en la que estén ubicadas o su naturaleza, tienen que ser creativas e innovadoras para poder mantenerse en los mercados y poder aumentar su competitividad. (Pérez, 2008)

La globalización implica el funcionamiento de los mercados las 24 horas del día y conlleva la necesidad de operar desde cualquier parte del mundo a cualquier hora, suponiendo un cambio en los patrones de consumo. Las TIC se presentan como un instrumento para responder rápidamente a los requerimientos del mercado. (Oliveros & Martínez, 2017)

“Para las empresas el estar amenazadas constantemente en sus Activos, puede representar miles o hasta millones de pesos en pérdidas. Esto se debe a las vulnerabilidades en los Sistemas Operativos, Sistemas de Información o acceso a la Información sin aprobación o de manera ilícita, por eso es de gran importancia conocer todos los conceptos y conocimientos para contrarrestar estos posibles ataques.” (Muñoz, 2017)

2.2 Marco conceptual

Se incluyó para la elaboración del proyecto el concepto de seguridad el cual se define según la Norma Normas ISO/IEC 27001:2013. Es la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso.

El término seguridad de la información se define en la Norma como la preservación de confidencialidad, integridad y disponibilidad de la información; además también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad; donde a su vez se define la confidencialidad como el aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso, la integridad es la garantía de la exactitud y completitud de la información y de los métodos de su procesamiento y la disponibilidad es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Seguridad de la Información. Es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

Activo. Cualquier cosa que tenga valor para la organización

Control. Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Vulnerabilidad. La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Riesgo. Combinación de la probabilidad de un evento y su ocurrencia.

Tratamiento del riesgo. Proceso de selección e implementación de medidas para modificar el riesgo

Amenaza. Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.

Control de acceso. Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular.

Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos (ej. acceso a una habitación donde hay servidores), recursos lógicos (ej. una cuenta de banco, de donde solo determinadas personas pueden extraer dinero) o recursos digitales (ej. un archivo informático que sólo puede ser leído, pero no modificado)

Sistemas biométricos. Se utilizan para la identificación automática de personas mediante el uso de características físicas del individuo o de su comportamiento. Estas pueden ser su cara, el iris de los ojos o sus huellas dactilares. Son rasgos únicos e intransferibles de cada persona.

2.3 Marco teórico

La Planificación estratégica de la Seguridad de la Información, es el proceso de estudiar, analizar y decidir las mejores estrategias de incorporación y uso de los sistemas informáticos (SI) y de las SGSI (Sistema de Gestión de Seguridad de la Información) en una Empresa.

ISO (International Organization for Standardization): La ISO es una unión internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente en cada país (entidad pública, privada).

La ISO desarrolla estándares requeridos por el mercado que representan un consenso de sus miembros (previo consenso nacional entre industrias, expertos, gobierno, usuarios,

consumidores) acerca de productos, tecnologías, sistemas y métodos de gestión, entre otros. Estos estándares, por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio.

Norma ISO/IEC 27000: Recoge los términos y definiciones empleados en el resto de normas de la serie, con esto se evitan distintas interpretaciones sobre los conceptos que aparecen a lo largo de las mismas. Además, incluye una visión general de la familia de normas en esta área, una introducción a los sistemas de Gestión de Seguridad de la información y una descripción del ciclo de mejora continua.

Norma ISO/IEC 27001: Es la norma principal de la serie. Se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y de su actividad. La norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información. Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo, especifica los requisitos para implementar controles y medidas de seguridad adaptados a las necesidades de cada organización.

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

la Norma ISO27001 está en el estándar británico BSI (British Stand Ards Institution) BS7799-Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de octubre de 2005.

Estándares de Seguridad Informática. Para garantizar el éxito en la gestión de la información, se toman en cuenta los referentes que brindan los estándares para su seguridad. Con esto se espera que la información se proteja celosamente y se garantice la implantación de las estrategias que propician la integridad, la confidencialidad y la disponibilidad de ésta hacia los clientes. Entre estos estándares se encentran:

Itil: Biblioteca de Infraestructura de Tecnologías de Información, como conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

Cobit: Objetivos de control para la información y la tecnología relacionada; concebida como un marco creado por ISACA para la tecnología de la información (TI) y el Gobierno de TI.

Planificar: Establecer el SGSI**.** Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Definir una política de seguridad que: Incluya el marco general y los objetivos de seguridad de la información de la organización, considere requerimientos legales o contractuales

relativos a la seguridad de la información, esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI, que establezca los criterios con los que se va a evaluar el riesgo, esté aprobada por la dirección, definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).

Identificar los riesgos: Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios, Identificar las amenazas en relación a los activos, Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas, Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

2.4 Marco legal

Constitución Política de Colombia. Artículo 6110. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

Norma ISO/IEC27002. Tecnología de la información, técnicas de seguridad11. Código para la práctica de la gestión de la seguridad de la información. Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

Ley 1273 de 2009 (5 de enero). El Congreso de la República de Colombia, establece la ley 1273 por medio de la cual se modifica el Código Penal, creando 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.

El proyecto tendrá como bases legales la ley 1273 de 2009, en sus artículos:

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96)

meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C. Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación

En el desarrollo del proyecto se utilizó el método basado en una investigación descriptiva con enfoque cuantitativo, la investigación descriptiva brinda una metodología apropiada para recolectar información básica para llevar a cabo el proyecto, ya que la misma describe de modo sistemático las características de una población, situación o área de interés, lo cual es manifestado Bernal Torres, Cesar Augusto en su libro Metodología de la Investigación, citando a SALKING, Neil "se reseñan las características o rasgos de la situación o fenómeno objeto de estudio". Con la aplicación de este método se buscó obtener información sobre la situación actual de la empresa Motel Dubai en lo referente a la seguridad (física y digital) del entorno de trabajo.

3.2 Población y muestra

La población objeto para el presente estudio, está conformada en su medio interno por el gerente la empresa Motel Dubai y sus catorce (14) empleados en el área administrativa. Tomando en cuenta dos (2) personas que realizan los fines de semanas para complemento.

3.2.1 Población**.** En cuanto a la población objeto de estudio se tomaron en cuenta todos los empleados que laboran, y tienen directa relación con la información que se maneja al interior de la de la empresa motel Dubai.

3.2.2 Muestra. Se recolecto información de todos los que colaboran con la empresa y que están vinculados laboralmente con la empresa. Técnicas de recolección de la información

Tabla 1 ***Relación de empleados Motel Duabi, Área administrativa y operativa, por seguridad de la empresa no se colocan nombres solo cargos y cantidad.***

NOMBRE →	**CARGO →**
Por seguridad	Gerente general
Por seguridad	Contador
Por seguridad	Recepcionista (2)
Por seguridad	Vigilantes (2)
Por seguridad	Camareras (4)
Por seguridad	Turneras (3)
Por seguridad	Electricista (1)

Fuente. Autores del proyecto.

Cabe resaltar que en la elaboración del proyecto se vio conveniente trabajar con el cien por ciento (100%) de la población, teniendo en cuenta que esta es finita, motivo por el cual no se requirió la aplicación de fórmulas estadísticas.

3.3 Técnicas de recolección de datos

La obtención de datos e información para esta investigación se efectuó mediante una serie de técnicas como observación, revisión documental, listas de chequeo, encuestas y entrevistas aplicadas al gerente de la empresa Motel Dubai y los empleados.

3.3.1 Fuentes primarias. Entrevistas: Al llevar a cabo las entrevistas a los empleados, se buscó inicialmente identificar la seguridad que se maneja en las áreas principales, el uso de contraseñas y usuarios autorizados en el manejo de equipos, el acceso a archivos. Se indago

acerca de las políticas de gestión de la seguridad que actualmente manejan, si tienen conocimiento, si recibieron alguna capacitación.

Observación: Por medio de la observación se identificó y registró, los controles que se tienen actualmente para el uso y manejo de la información en la empresa, con la intensión de reconocer los resultados junto con la gerencia de la empresa.

Documentales: Se tuvo en cuenta la documentación producida y gestionada por las dependencias y/o trabajadores en sus labores, como son aquellos manuales de funciones y procedimientos, consulta de auditorías anteriores si es el caso se hayan realizado, políticas y normas de seguridad de la información, entre otros.

3.3.2 Fuentes secundarias. Apoyo en leyes, estándares y normas relacionadas con la seguridad de la información, artículos científicos relacionados con la seguridad de la información y auditorias basadas en riesgos y administración de riesgos.

3.4 Análisis de resultados

Dando seguimiento a los objetivos propuestos Para el análisis de la información obtenida con los instrumentos, evaluada de forma cuantitativa y cualitativa representando de forma clara los resultados obtenidos, siempre siguiendo las normas ISO/IEC 27001 y 27002 para un buen desarrollo del proyecto.

Capitulo 4. Análisis y discusión de resultados

4.1 Diagnóstico de la seguridad física y de la información de la empresa Motel Dubai.

Hoy en día en los procesos de actividades comerciales junto con la infraestructura tecnológica están expuestos a un sin número amenazas tanto externas como internas colocando en riesgo la seguridad de la información, los activos usados para las actividades operacionales de la empresa, por tal razón es preciso realizar un dictamen a la empresa Motel Dubai que revele los riesgos actuales de su ambiente, para lograr encontrar un grado de seguridad física y lógico para la administración de la información.

Esta primera fase tiene como objetivo identificar el estado actual y manejo de la seguridad de la información, la importancia al implementar un plan de gestión en la empresa. Para lograr establecer y permitir cumplir con el objeto general del diagnóstico se desarrollaron y ejecutaron varias actividades para este fin, entre ellas podemos encontrar

4.1.1 Aplicación de la encuesta. La aplicación de encuesta a los empleados de motel DUBAI, con la realización de estas se busca recoger la información que luego de analizada revele la necesidad de diseñar el plan de gestión de seguridad para controlar el acceso a las áreas vitales de la empresa.

Los resultados obtenidos permitirán conocer políticas realizadas en la empresa para precisar el estado en el que se encuentra actualmente.

Resultados de la encuesta aplicada

Tabla 2 ***La empresa cuenta con un plan de gestión de seguridad de la información.***

RESPUESTA	CANTIDAD	PORCENTAJE
SI	0	**0%**
NO	14	**100%**
Total	**14**	**100%**

Fuente. Autores del proyecto

Se les realizo la siguiente pregunta a los empleados:

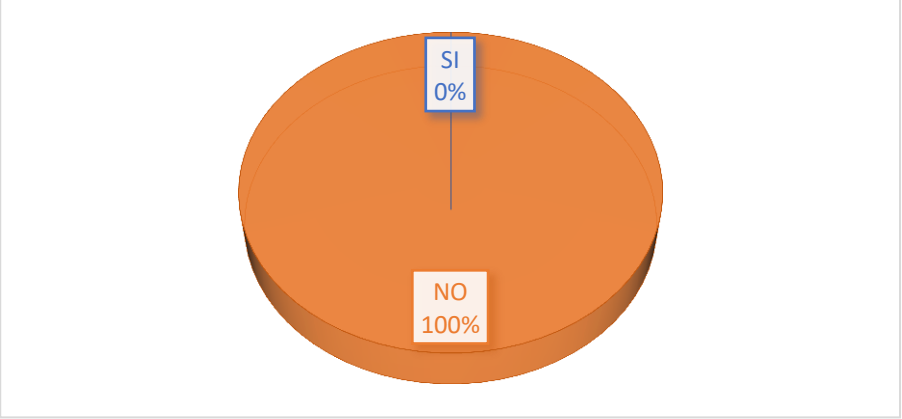


Figura 1. Conoce usted si la empresa tiene un plan de gestión de seguridad de la información.
Fuente. Autores del proyecto

Habiendo recolectado la respuesta a la pregunta anterior a la cual respondieron los empleados de Motel Dubai se puede identificar y afirmar que un porcentaje del 100% de los empleados reconoce que la empresa no cuenta con un plan de gestión de seguridad de la información, deduciendo naturalmente a evidecniar sucesos negativos para dicha empresa, uno de estos podrian ser la perdida de activos fisicos y logicos, daño en equipos de apoyo, perjudicando la normal prestacion del servicio dando como resultado posibles perdidas de usuarios y financieras.

Tabla 3. ***Se usa alguna demarcación de seguridad para proteger las zonas que contienen información y medios de procesamiento de la misma.***

RESPUESTA	CANTIDAD	PORCENTAJE
SI	6	**43%**
NO	8	**57%**
Total	**14**	**100%**

Fuente. Autores del proyecto

Se les realizo la siguiente pregunta a los empleados:

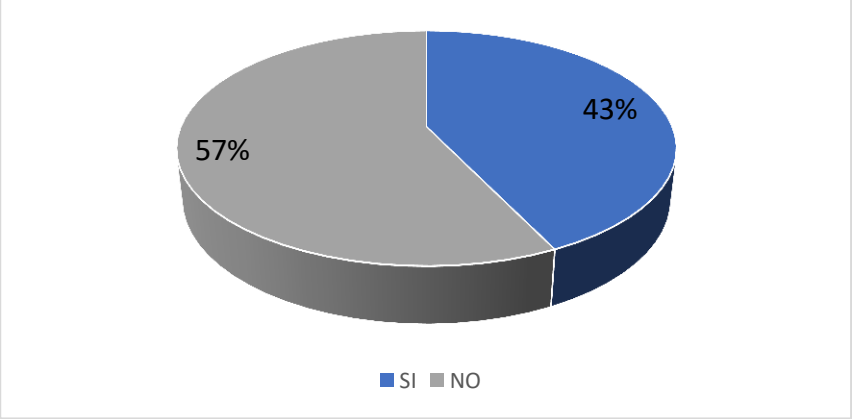


Figura 2. Se usa alguna demarcación de seguridad para proteger las zonas que contienen información y medios de procesamiento de la misma.
Fuente. Autores del proyecto

Según las respuestas dadas por el personal de la empresa motel Dubai; se establece que el 43% de ellos manifiestan que no existe demarcaciones de seguridad para protección de la información que estén definidos en la empresa, mientras que el 57% consideran como perímetros de seguridad algunas áreas donde se encuentran almacenados los equipos cómputo y de comunicaciones; lo que indica que debe definirse un contorno de seguridad protegido del acceso no autorizado, daño e interferencia, de igual manera se debe comunicar al personal sobre la existencia del mismo y realizar la debida señalización; permitiendo que sea identificado por el total de empleados.

Tabla 4 ***Existen componentes para el control de acceso a áreas vitales.***

RESPUESTA	CANTIDAD	PORCENTAJE
SI	14	**100%**
NO	0	**0%**
Total	**14**	**100%**

Fuente. Autores del proyecto

Se les realizo la siguiente pregunta a los empleados:

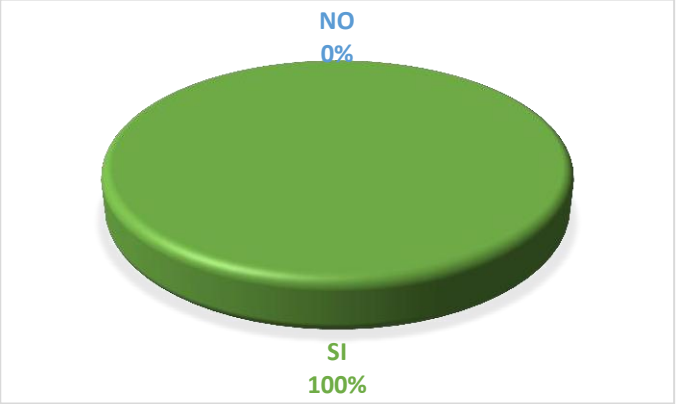


Figura 3. Existen componentes para el control de acceso a las áreas vitales.
Fuente. Autores del proyecto

Para la anterior pregunta realizada se determinó que 100% de los encuestados afirma conocer que existen controles o componentes de acceso a áreas vitales, teniendo en cuenta en cuenta las cerraduras, llaves, candados, rejas de seguridad y demás dispositivos físicos mecánicos que permiten brindar seguridad; lo cual indica que estas herramientas son para seguridad de las instalaciones que brindar un grado de protección.

Tabla 5 ***Dispositivos para el control de acceso utilizados en motel Dubái***

RESPUESTA	CANTIDAD	PORCENTAJE
Sistema	7	**50%**
Físico	7	**50%**
Total	**14**	**100%**

Fuente. Autores del proyecto

Se les realizo la siguiente pregunta a los empleados:

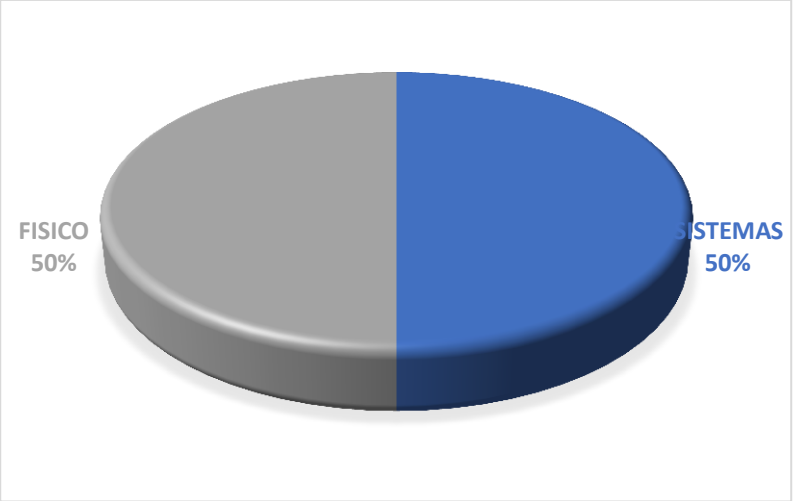


Figura 4. Dispositivos para el control de acceso utilizados en Motel Dubái
Fuente. Autores del proyecto

En respuesta se recolecto de los encuestados el 50% indico que los mecanismos para el control de acceso utilizados en el motel son físicos, y otro 50% indico que existen medidas en los equipos para ingresos seguros como programas y sistema de vigilancia de igual manera se presentan algunos comentarios sobre estos controles, algunos manifiestan que no son los más seguros para asegurar.

Tabla 6 ***Hay direccionamiento que permita laborar en las áreas vitales***

RESPUESTA	FRECUENCIA	PORCENTAJE
SI		**0%**
NO	14	**100%**
Total	**14**	**100%**

Fuente. Autores del proyecto

Se les realizo la siguiente pregunta a los empleados:

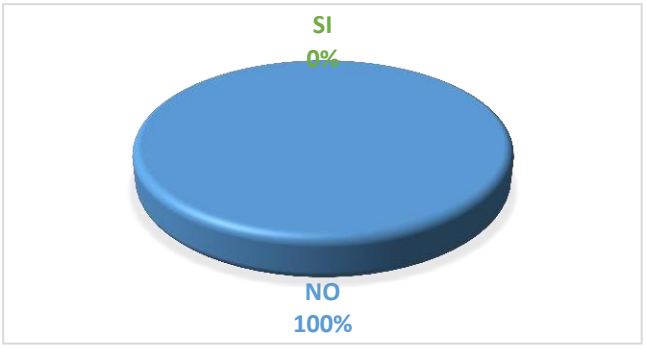


Figura 5. Hay direccionamiento que permita laborar en las áreas vitales
Fuente. Autores del proyecto

Luego de realizada la pregunta se tabula que el 100% del personal de trabajo del motel encuestado responde no conocer direccionamiento para laborar áreas vitales, esto puede permitir que los empleados no estén al tanto de la existencia de actividades dentro de las áreas, tampoco pueden estar supervisada con el ánimo de evitar intromisiones que coloquen en riesgo la información y datos.

Tabla 7 ***Conocimiento de técnicas de protección de equipos***

RESPUESTA	CANTIDAD	PORCENTAJE
SI	1	**7%**
NO	13	**93%**
Total	**14**	**100%**

Fuente. Autores del proyecto

Se les realizo la siguiente pregunta a los empleados:

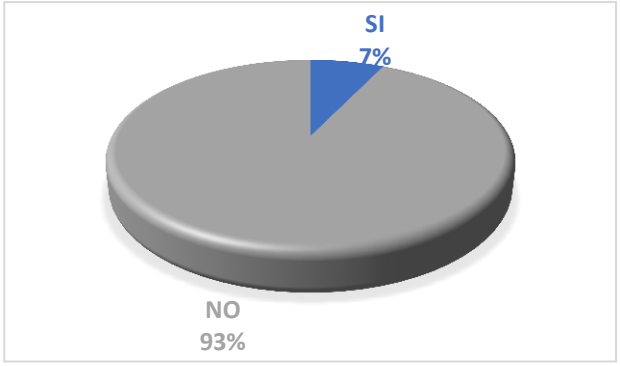


Figura 6. Conocimiento de técnicas de protección de equipos
Fuente. Autores del proyecto

Con la respuesta de los empleados encuestados se concluyó que el 93% del personal manifiesta que no conoce que existan técnicas u otros mecanismos de protección de equipos, esto produce que la información este expuesta a amenazas y riesgos de varios tipos por no contar con controles que protejan los equipos y minimizar el impacto. Pero un 7% de los empleados manifestó tener conocimiento y acceso algunas herramientas de seguridad.

Para establecer de forma general la estructura organizacional de las áreas vitales de la empresa motel Dubai, sus procesos principales, los objetivos misionales y la identificación del tipo de información gestionada por la empresa.

4.1.2 Direccionamiento estratégico de motel Dubai. El Motel Dubái nace a partir de un estudio de mercadeo que les permitió identificar algunas de los factores más demandantes en las personas, la empresa busca cubrir las necesidades del ser humano para comodidad, seguridad, descanso y otros servicios que aprueben disfrutar momentos agradables en el ambiente de hospedaje.

Es así como en el año 2013 con la idea original nace el primer motel temático de la ciudad. Es un lugar perfecto para todos los habitantes de la ciudad Ocaña y sus alrededores que quieran vivir momentos inolvidables y placenteros, con absoluta privacidad y fácil acceso. Ofrecemos 8 suites temáticas y 31 sencillas, todas inspiradas en culturas, países, personajes y situaciones de la vida cotidiana, convirtiéndonos en un referente turístico para todos aquellos que visitan nuestra hermosa ciudad.

Confortables y con un diseño vanguardista perfecto para disfrutar los mejores momentos de la vida, con una diversidad de habitaciones que se adaptan al presupuesto de todos nuestros clientes. En la actualidad funciona con una nómina de catorce (14) empleados;

La oferta del Motel Dubai es la siguiente:

- Precio asequible.
- Confort Limpieza y pulcritud.
- Rapidez del servicio
- Disponibilidad 24 horas
- Privacidad absoluta
- Variedad de productos y servicios

Modelo de Objetivos. La empresa motel Dubai este articulado con el objetivo principal con la misión y visión de la empresa. (Figura 1.)

Misión. Ofrecer a nuestros clientes una experiencia de armonía, exclusividad, seguridad, privacidad y comodidad en nuestras instalaciones, con un servicio impecable desde el primer instante. Todo esto con un compromiso de profesionalismo, con personal altamente capacitado y calificado; promoviendo al desarrollo integral de los colaboradores internos y logrando la satisfacción total de nuestros clientes.

Visión. Mantener el liderazgo en la línea motelera, siendo una empresa consolidada e innovadora que responda a las más estrictas exigencias, buscando exceder las necesidades y expectativas de nuestros clientes.

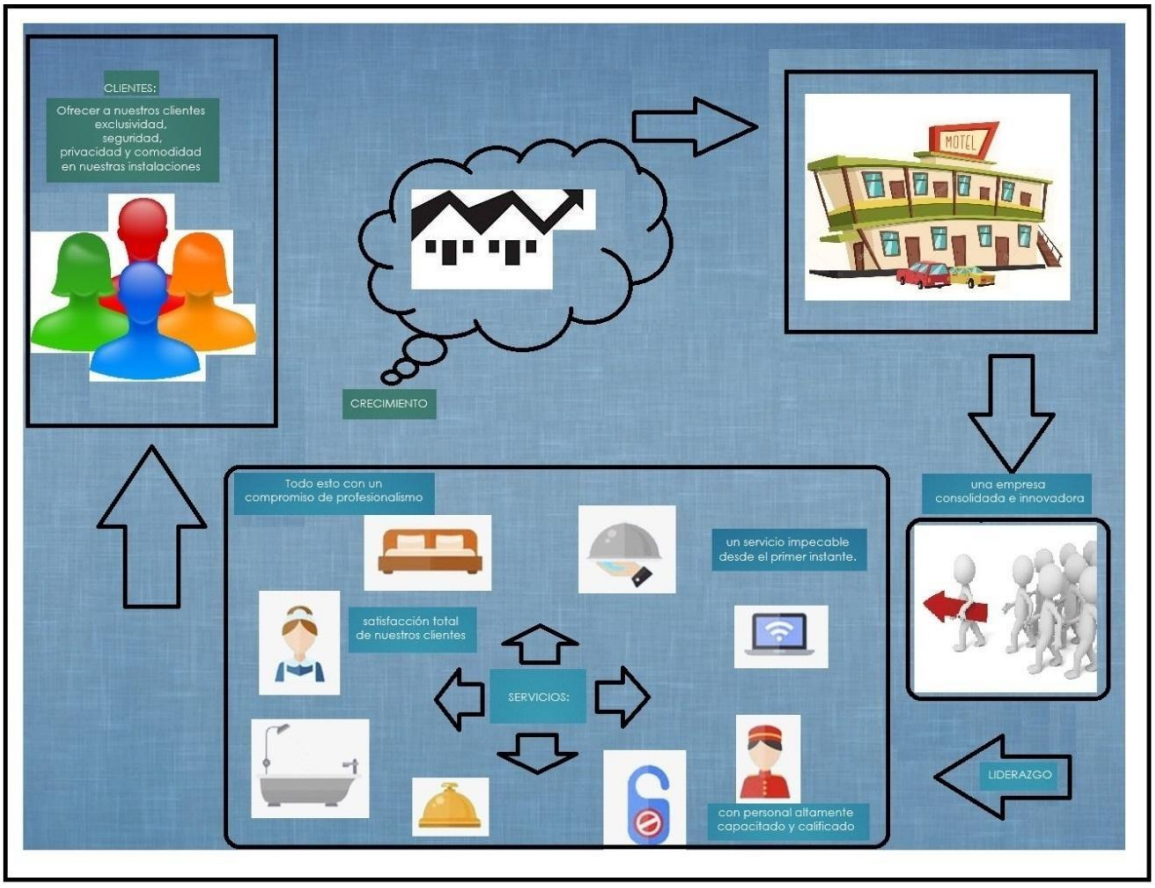


Figura 7. Objetivos de la empresa MOTEL DUBAI
Fuente. Autores del proyecto

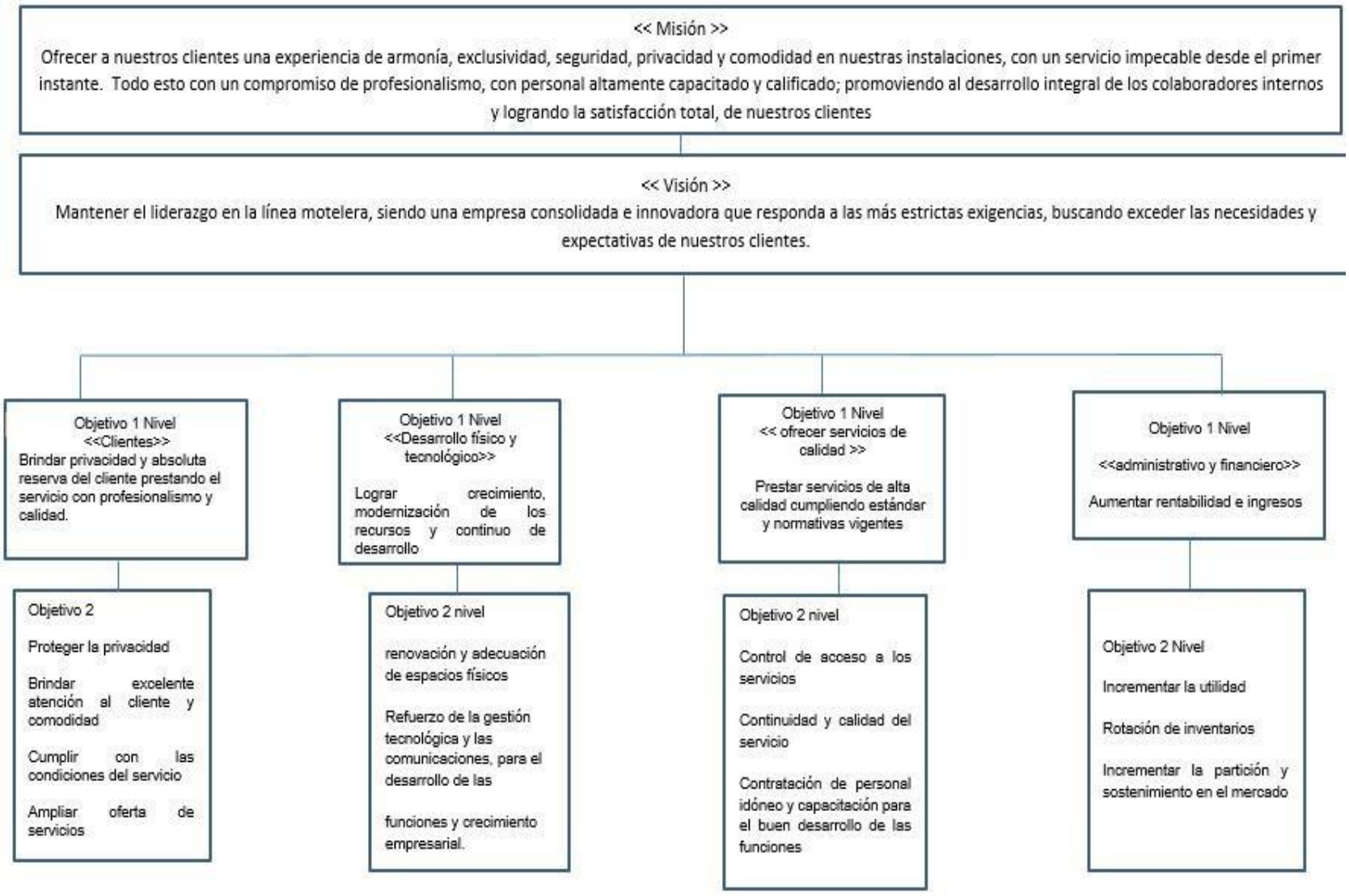


Figura 8. Mapa de Objetivos Misión, Visión y objetivos de la empresa MOTEL DUBAI
Fuente. Autores del proyecto

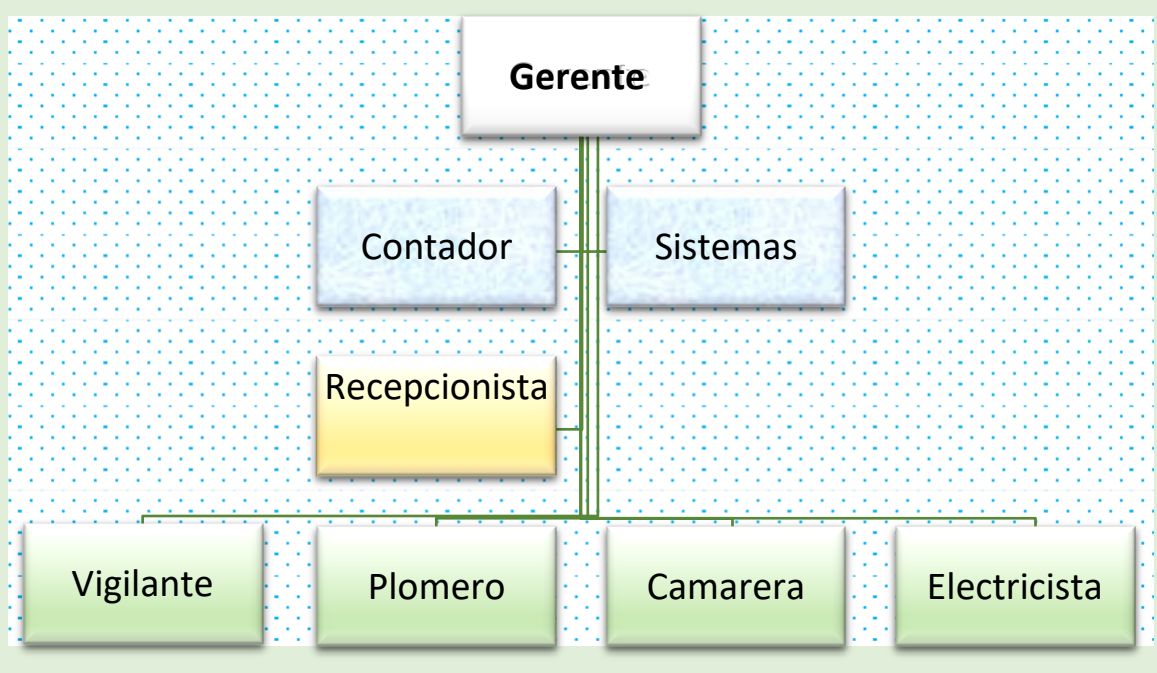


Figura 9. Estructura Organizacional Estructura Orgánica Motel Dubai
Fuente. Autores del proyecto

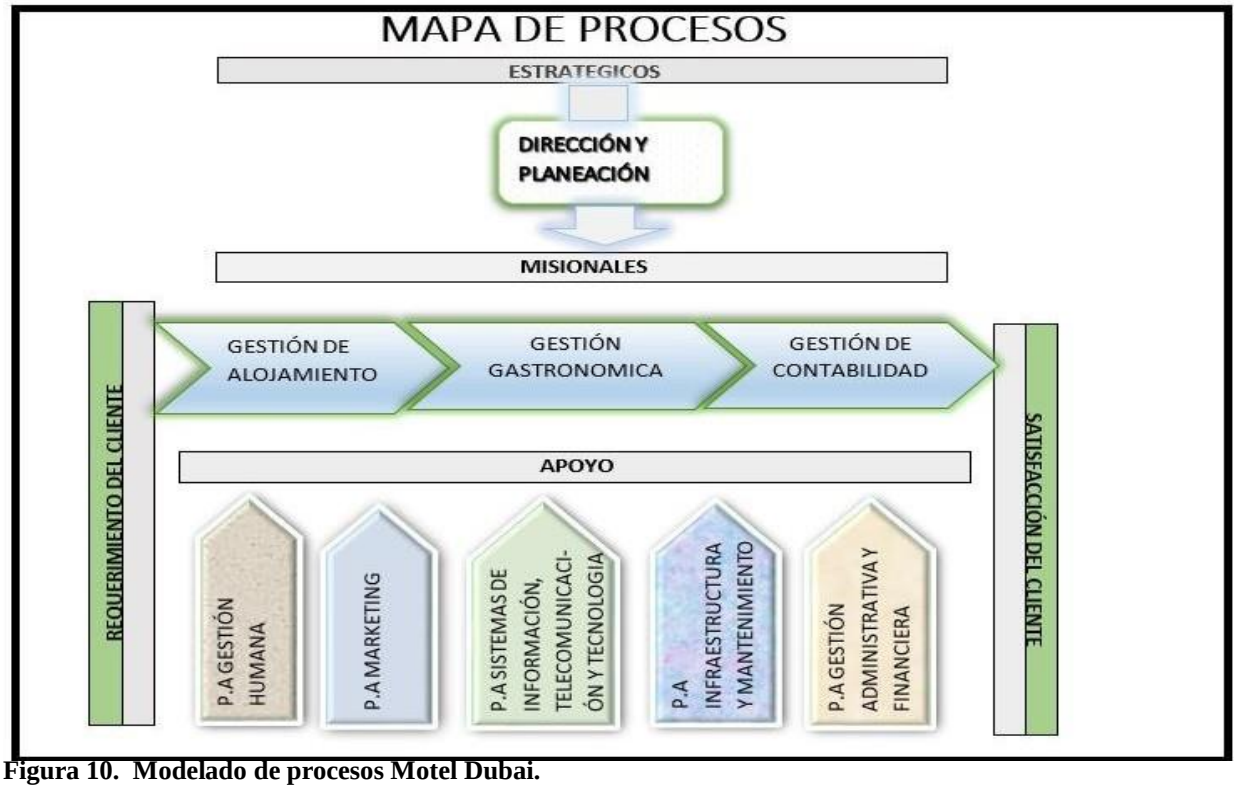


Figura 10. Modelado de procesos Motel Dubai.
Fuente. Autores del proyecto

Procesos Estratégicos. Dirección y Planeación: Garantizar la gestión de servicios prestados a los usuarios, la óptima gestión de los recursos, registro ordenado y sistematizado con garantía de seguridad de las operaciones de gastos, políticas de nómina, Compras y adquisición de insumos.

Procesos Misionales. Son los procesos relacionados con la funcionalidad de la empresa motel Dubai, los cuales son: Gestión de Gastronomía, Gestión de alojamiento, Gestión de Contabilidad.

Diagrama de procesos. A continuación, se muestra el diagrama de procesos de la empresa motel Dubai

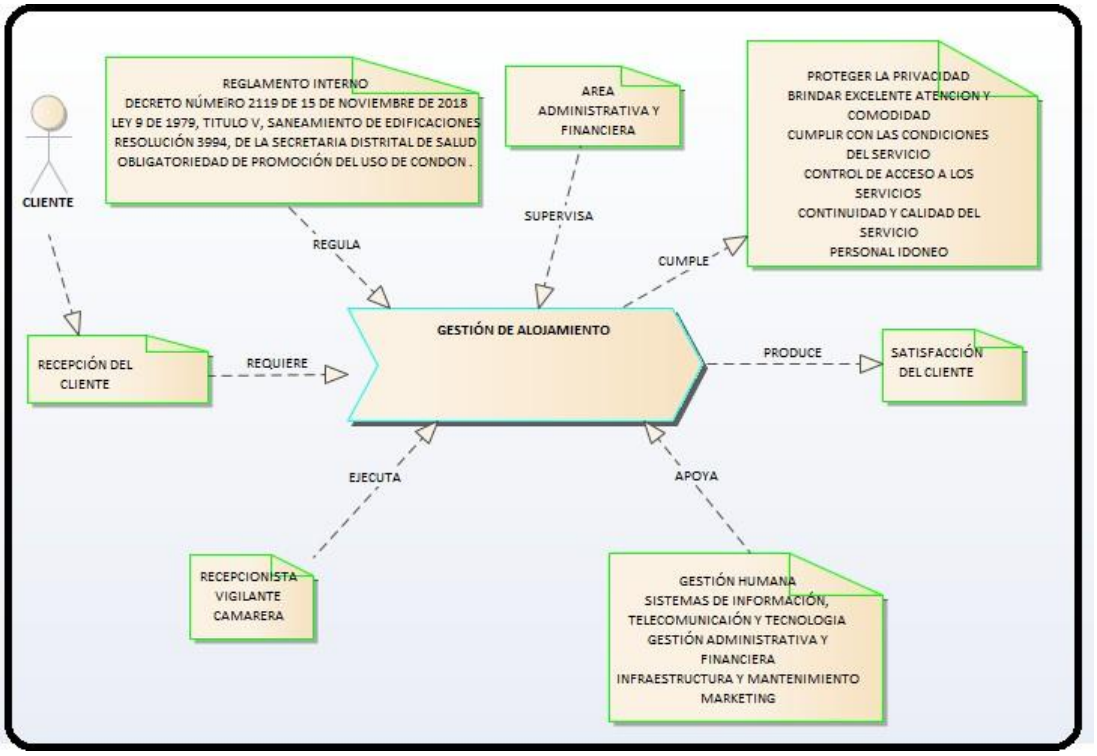


Figura 11. Procesos misional Alojamiento
Fuente. Autores del proyecto

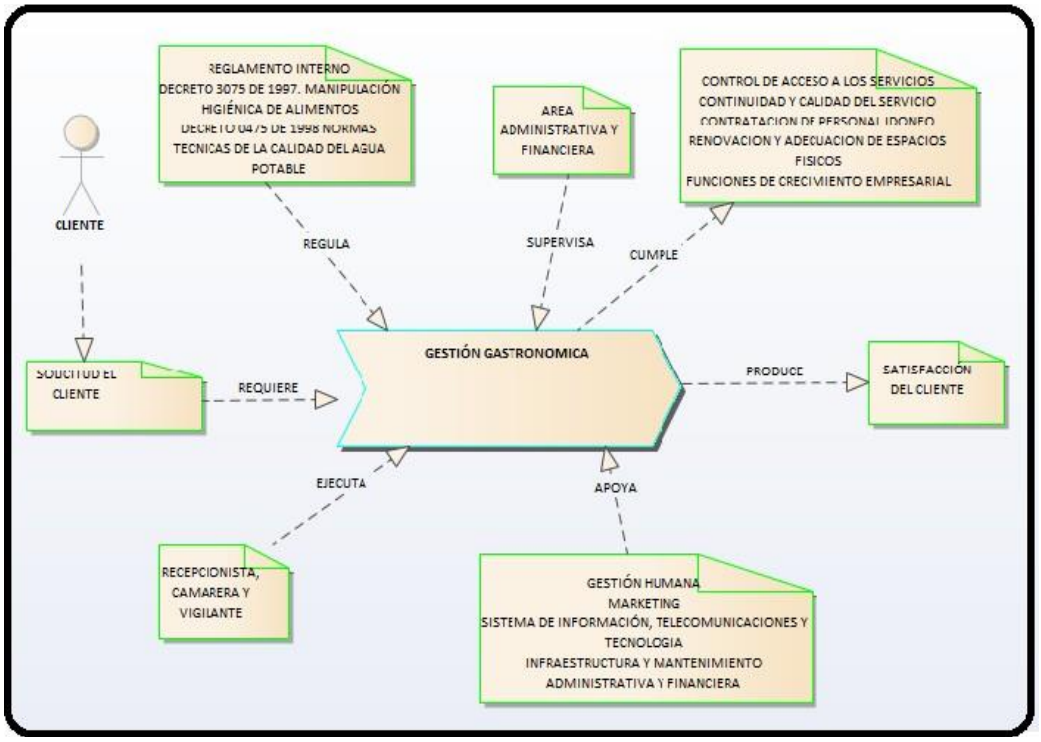


Figura 12. Procesos misional Gastronomía
Fuente. Autores del proyecto

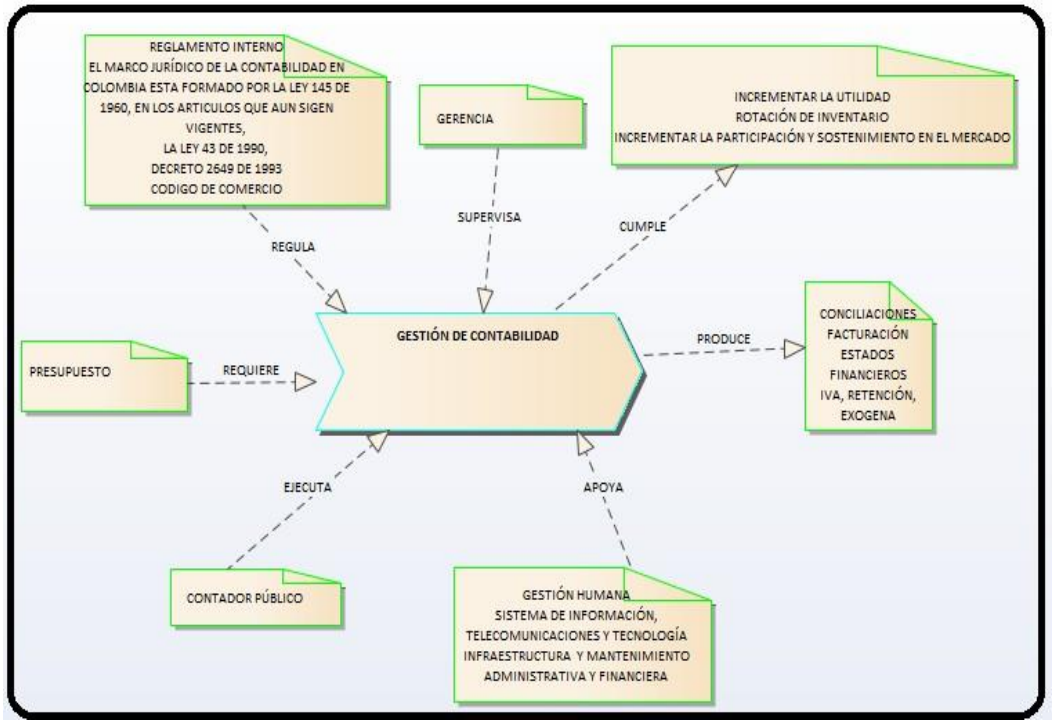


Figura 13. Procesos misional gestión de contabilidad
Fuente. Autores del proyecto

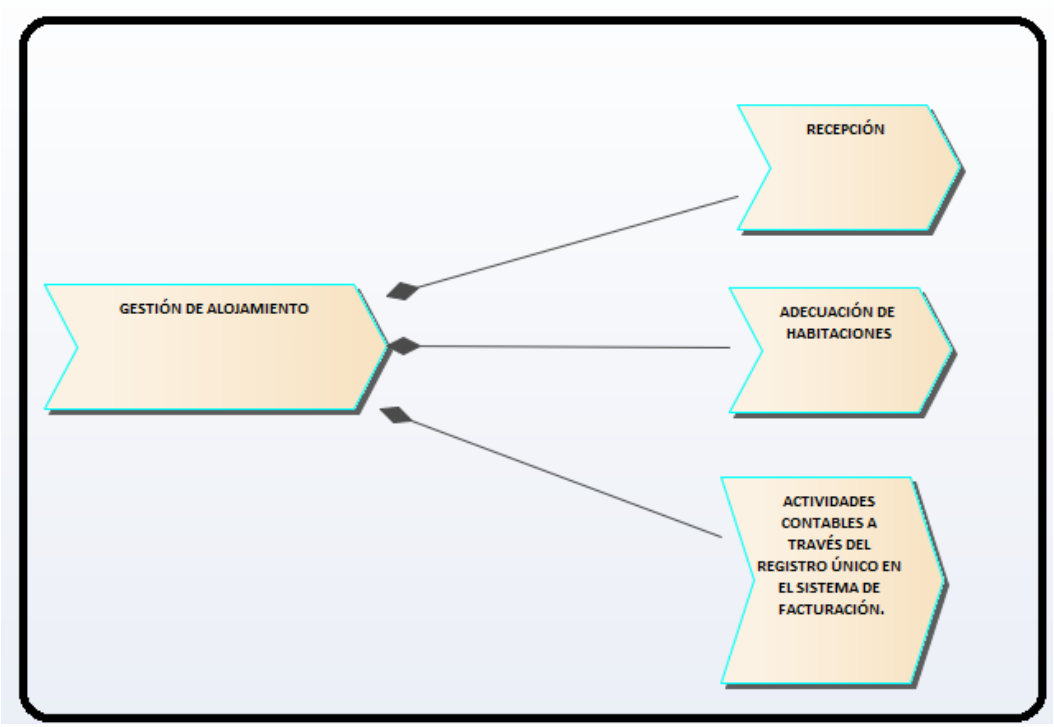


Figura 14. Descripción de Proceso de Alojamiento
Fuente. Autores del proyecto

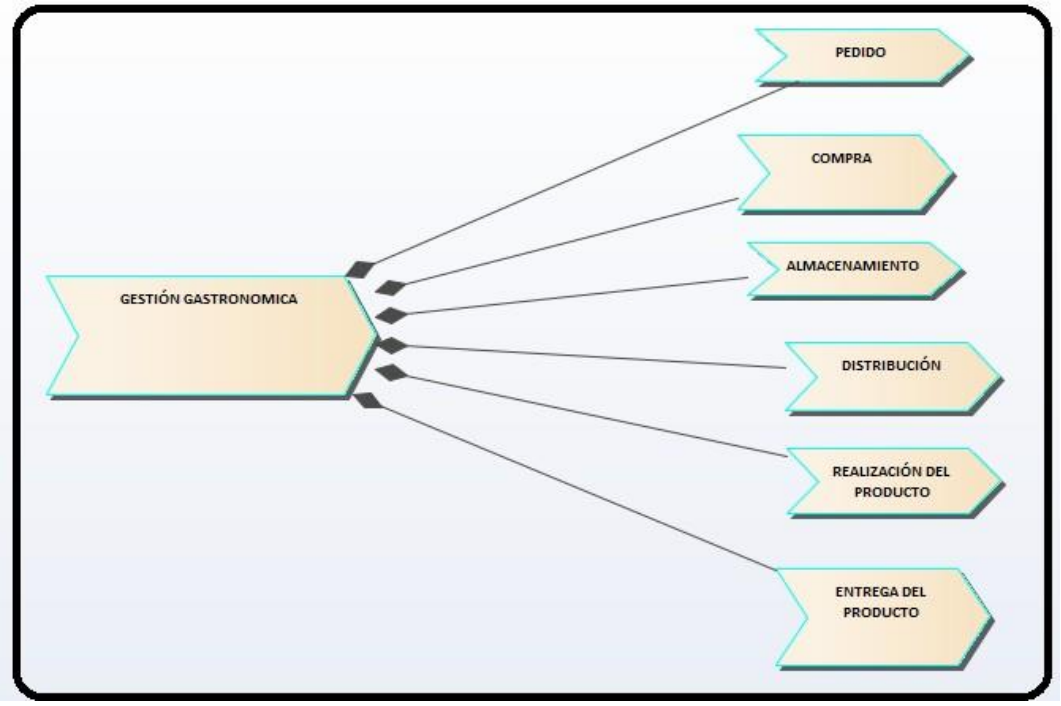


Figura 15. Descripción de Proceso de Gastronomía
Fuente. Autores del proyecto

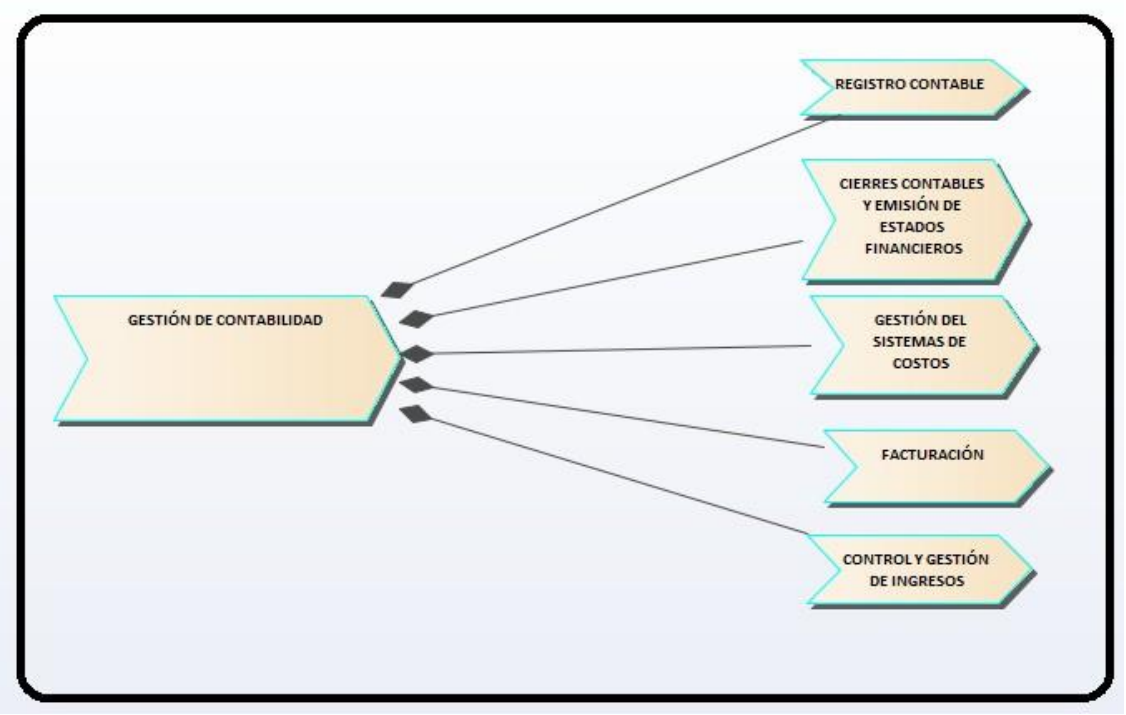


Figura 16. Descripción de Proceso de Gestión contabilidad
Fuente. Autores del proyecto

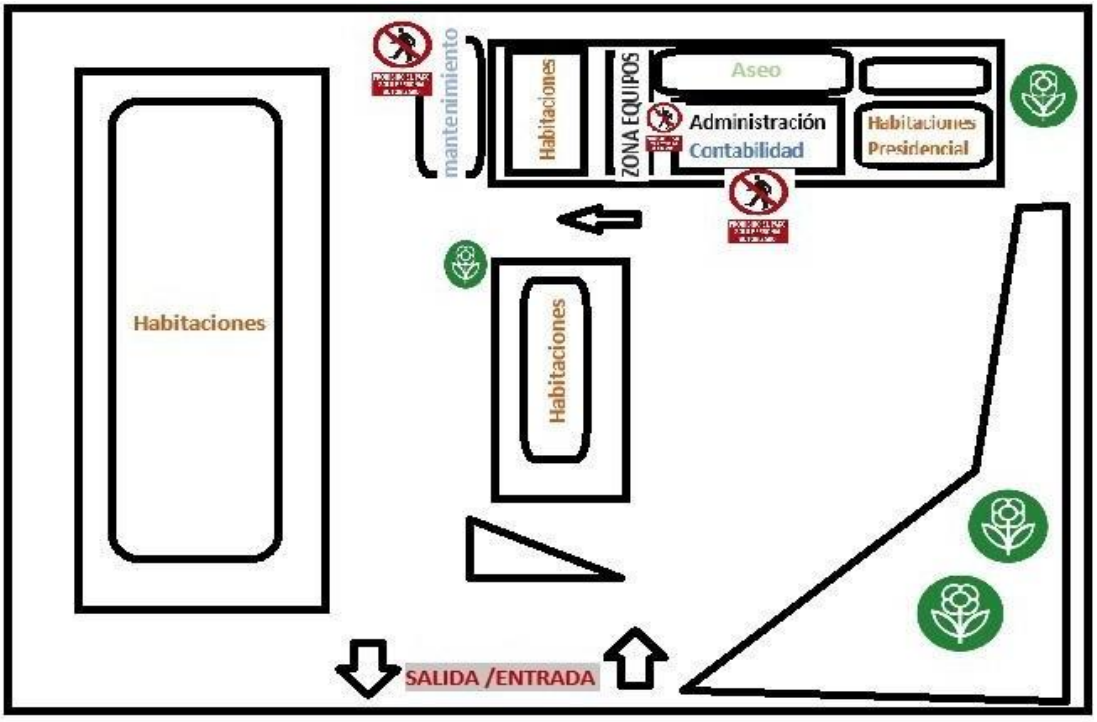


Figura 17. Estructura física de la empresa MOTEL DUBAI.
Fuente. Autores del proyecto

La empresa Motel Dubai. Está conformado en su planta física como lo muestra la Figura 8, en la entrada/ salida tiene un punto de acceso con buenas señalización, al costado derechos se encuentra un jardín, de frente a la entrada se encuentra la administración conformada (Gerencia, contabilidad y recepción), que tiene acceso restringido físicamente, detrás de ella está la zona Aseo y lavado de restringida señalizada la cual no cuenta con mecanismos de protección solo con cámara de vigilancia, su ubicación no es segura para el personal de la empresa para acceder al resto de las oficinas, luego sigue el área de Mantenimiento donde se realizan las reparaciones de los equipos y se ejecutan las órdenes de trabajo para realizar los mantenimientos de red. Continúa el área de la zona de equipos la cual

La zona de equipos ubicada en primer piso administración se encuentra con acceso restringido, pero sin controles efectivos, solo con contraseñas de usuario a equipo de recepción, enseguida se encuentran el área de facturación y contabilidad, esta última cuenta con acceso restringido sin controles eficientes. Las TIC usadas para contabilidad es software licenciado de desarrollo local llamado Manager, apoyando el proceso de comercialización con un sistema de Facturación, para administración de usuarios se usa plataforma de Windows.

Dentro de la Infraestructura Tecnológica, la empresa para el sistema de vigilancia cuenta con 20 cámaras de seguridad de HD y con VCR de grabación continuo. Por motivos de seguridad no se permitió más descripción de la infraestructura física de la empresa y algunos sistemas con sus especificaciones técnicas (radios, cámaras, controles de puertas, etc.)

Para el funcionamiento de las áreas de la empresa se cuenta con 3 computadores (Pc), los cuales 2 son portátiles y 1 es de mesa todo en uno, conectados con una pequeña LAN, un SWITCH de 8 puertos, existe conexión a internet brindada por un ISPP mediante un router Access Point WIFI que es el elemento que permite expansión de la red; además cuenta con una impresora de ticket mediante conexión directa, y una ups para soporte eléctrico de los equipos, un dispositivo para pagos electrónicos conectado a la red LAN por medio físico y Wifi.

Análisis de los activos y recursos. En el diagnóstico elaborado se hizo necesario identificar los activos y recursos con que cuenta la empresa, para definir con claridad la información y equipos existentes, se dejó constancia de los siguientes:

Tabla 8 ***Recursos físicos: Inventario de Hardware***

Inventario de Hardware					
No.	**Equipo**	**Marca**	**Núm. Inventario**	**Características**	**Observaciones**
1	Computador	Lenovo	RL-007	ALL ONE	Equipo de mesa, para facturación y administración de cámaras
2	Computador	HP	RL-008	Portátil	Utilizado por la contadora inventario y demás información confidencial
3	Computador	HP	RL-009	Portátil	Gerente
4	Impresora	SAT	RL-010	Impresora de ticket	Facturación
5	Conexión de red	-	RL-011	Red local	Red cableada de cámaras de vigilancia
6	UPS	2000	RL-012	Unidad interrumpida de poder	
7	Router	TPLink	Rl-013		ADL-DSL- 3 antenas
8	Datafono	Verifone	RI-014	VX-520	Dispositivos para pagos electrónicos

Fuente. Autores del proyecto

Tabla 9. ***Recursos físicos: Inventario de Software***

Inventario de Software							
REF	**Software**	**Versión**	**Número Inventario**	**Licencias**	**Presentación**	**Asignado a**	**Localización**
W01	Windows 8	Single language-64 bits 2012	RL-001	00179-40519-83-837-AAOEM(1)	CD-ROOM	Centro de Sistemas	Servidor 1
W02	Windows 8.1	Single language-64 bits 2013	RL-002	00262-30110-81048-AAOEM(1)	CD-ROOM	Área de contabilidad	Computador 1
W03	Windows 8.1	Single language-64 bits 2013	RL-003	00262-30308-9847-AAOEM(1)	CD-ROOM	Área de gerencia	Computador 2
SC	Manager	3.2	RL-004	1	Digital	Área de contabilidad	Servidor 1
PO	Office	16.0,10228.20080 2016	RL-005	3	Digital	Área de contabilidad, gerencia Centro de sistemas	Servidor 1 Computador 1 Computador 2
SV	CMS H264	264	RL-006	Software gratuito		Centro sistema	Servidor 1

Fuente. Autores del proyecto

4.1.3 Análisis de la gestión de activos**.** La gestión de activos permite a la empresa MOTEL DUBAI contar con las estrategias necesarias que controlen mejor sus activos.

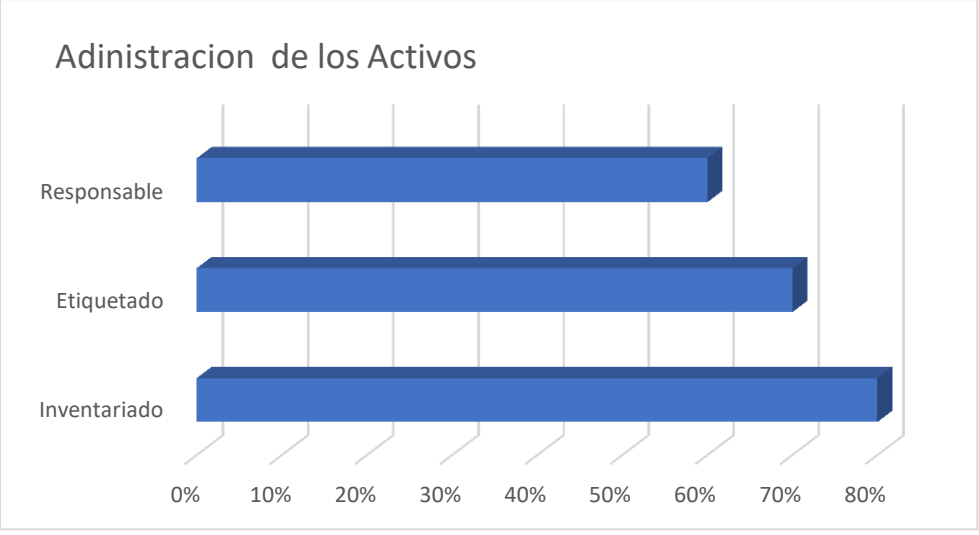


Figura 18. Análisis de la gestión de activos motel Dubai
Fuente. Autores del proyecto

Con la siguiente grafica se analiza que la empresa mote Dubai, cuenta con un aceptable y responsable manejo de sus activos, principal función que se encuentra a cargo del administrador/ gerente en apoyo con contabilidad , quien se, apoyándose estos en responsabilidades de los activos para las áreas vitales; a su vez se identifican todos los activos y se les asigna la responsabilidad por el mantenimiento y los controles apropiados, sin embargo existen activos que no cuentan con un propietario nombrado, es decir que están sin ninguna protección. Para el manejo de inventario lo realiza la contadora por medio de un software por el tema de facturación digital, se identificó y documento todos los activos con que cuenta la empresa con el fin de tener una protección efectiva sobre los mismos, se realiza por parte de la contadora y recepcionista el conteo e inventario de elementos diarios para uso, cabe mencionar que este inventario se realiza permanentemente todos los días, se tiene determinada como regla para el uso aceptable de los activos el registro y etiqueta de los mismos, permitiendo identificar cuales empleados usan o tienen acceso a los activos de la empresa y de esta manera conocer los responsables del uso que le den a los recursos; como se observa en la gráfica el porcentaje es interior al 20% lo que indica que este aspecto es poco controlado debido a que no todos los activos están etiquetados como debería ser.

4.1.4 Caracterización de la información de Motel Dubái. Como se dijo anteriormente la empresa maneja información de varios tipos la cual es administrada de acuerdo a su nivel de importancia, se puede identificar las siguientes**.**

Información Administrativa. Se dice de toda información de tipo administrativo que tiene que ver con el desarrollo de objetivos misionales propuestos, gerencia de la empresa, estrategias

de ventas y políticas; ésta es manejada estrictamente por dueño y gerencia con apoyo de confianza a través de la contadora.

Información contable. Es toda la información financiera y económica de la empresa la cual es manejada a través del software contable Manager, adicional a esto se maneja un software de facturación y uno de inventarios. Estos datos son administrados por la contadora de la empresa.

Información de usuarios. Contiene la información de los clientes de la empresa, pero esta es de registro privado el cual debe ser oculto para el resto de personal, la base de datos de usuarios es administrada por el área de contabilidad. Por motivos de riesgo y privacidad esta información solo es conocida por gerencia y contabilidad, nadie más tiene acceso.

Información de proveedores de insumos. Referente a la información de los proveedores de materias y servicios que necesita la empresa para prestar sus funciones. Se registran datos como teléfonos de contactos, privilegios otorgados a la empresa, promociones y valore, toda la información mencionada anteriormente es de estricta reserva teniendo en cuenta que es relevante para la competencia solo manejada por contabilidad y gerencia.

4.1.5 Auditoría realizada a la seguridad física de la empresa MOTEL DUBAI.

Realizada la auditoria para evaluar la seguridad física y del entorno de la empresa MOTEL DUBAI se obtuvieron los siguientes hallazgos: Para los procesos de administración y seguridad de la información los resultados obtenidos durante la evaluación, situaciones presentes:

Se evidencia que el Servidor 1 (principal), tiene instalado el Software de facturación (Manager V3.2), este equipo es usado también para otro tipo de actividades, a su vez diferentes usuarios realizan acciones que pueden colocar en riesgos la integridad de la información contable y financiera.

El Servidor 1, no cuenta con antivirus que evite ser afectado por amenazas internas o externas que podrían dañar la integridad de la información.

La red de cámaras de vigilancia, no cuenta con perfiles de usuario para categorizar la jerarquía de manejo de las mismas, y lograr evitar la intromisión al software de vigilancia e impedir alteraciones en los registros de seguridad. El software CMS H264 para la administración de cámaras es un software gratuito, se aclara que esta versión no es robusta y estable puede haber problemas con él y no cuenta con soporte técnico.

No se realizan copias de seguridad de toda la información, solo la contadora realiza copias de seguridad de la información contable. No se cuenta con manuales de procedimientos y prácticas relacionados con el uso adecuado de la información y del software que se maneja en la empresa, lo cual puede provocar que los colaboradores de la entidad al no tener una guía no puedan desempeñar adecuadamente sus funciones y pérdida de información y de recursos como por ejemplo el tiempo. No se cuenta con un sistema de seguridad de prevención por robo, para las computadoras personales, con lo cual la información es susceptible de caer en manos que puedan perjudicar a la organización.

Estos hallazgos se presentan en las operaciones que realizan los empleados, al momento de cambios de turno, cada empleado no tiene un usuario específico creado para identificar y administrar de modo seguro sus funciones. Existe el riesgo de que personal ajeno a la empresa acceda al equipo principal ya que este se ubica en un lugar que no brinda seguridad física necesaria que evite esto, No existen políticas establecida para la confidencialidad de los datos de la empresa.

De acuerdo con las pruebas realizadas a los procesos de administración y seguridad de la información, y según los criterios de evaluación para las redes computacionales y sistemas de información, me permito dictar el resultado de la práctica de auditoria de sistemas y hacer las recomendaciones necesarias para corregir los hallazgos

4.1.6 Análisis y evaluación de riesgos. Se dice que los riesgos son eventos negativos tanto internos y externos que se pueden presentar afectando alcanzar los objetivos de la organización; su evaluación debe identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del mismo y los objetivos relevantes para la organización y los resultados deben guiar y determinar la acción de gestión apropiada para implementar los controles seleccionados y proteger la información contra riesgos.

En la empresa motel Dubai se evidencia que no existe la identificación y análisis de los riesgos, por lo que no cuentan con controles eficientes establecidos que les permita proteger sus activos de los eventos que pueden afectar en gran parte el cumplimiento de los objetivos.

Tabla 10. ***Matriz de Riesgos aplicada a la empresa motel Dubai***

CODIRIESGO	RIESGOS DEL PROCESO			ANALISIS DEL RIESGO						EVALUACIÓN DEL RIESGO (ZONA DE RIESGO)	CONTROLES	
	RIESGO	CAUSAS O AGENTE GENERADOR	CONSECUENCIAS	NIVEL	DESCRIPTOR	DESCRIPCIÓN DEL ANALISIS	FRECUENCIA	NIVEL	DESCRIPTOR	DESCRIPCIÓN DEL ANALISIS			
RM1	manejo de equipo sin autorización	exceso de confianza falta de controles de seguridad falta de equipos para más personal	pérdida y daños de información, daños en físico a los equipos por descargas no autorizadas, costos en reparación física de equipos Software y Hardware	3	Posible	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 2 años	4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad	Extrema	Crear usuarios y contraseñas, capacitar los empleados	mantenimiento y reparación Adquisición de nuevos equipos
RM2	manejo de las cámaras de seguridad	Exceso de confianza de los empleados Manipulación de terceros, no definir los roles de los empleados y funciones claras	fugas de información Manipulación de dispositivos de almacenamiento de información de las cámaras acceso de terceros sin previa autorización	3	Posible	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 2 años	4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad	Extrema	cambios de contraseñas y acceso al sistema de cámaras y software solo control de acceso gerencia y sistemas	cambios de claves periódicos validación y verificación por parte de sistemas
	copias de seguridad bacukp	falta de capacitación y concientización de sus funciones	perdida de información, gastos de reparación y obtención de datos recuperación costosa	3	Posible	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 2 años	3	Moderado	Si el hecho llegara a presentarse, tendría Medianas consecuencias o efectos	Alta	El Encargado de la administración debe asignar políticas de	Generas plan de contingencia, Recuperación de Bacukp, generar

			PQRSF						sobre la entidad.		elaboración de Backup y estructurar un manual de procedimientos de copias de seguridad	periódicamente
RM3	Suministrar información personal y/o sensible a terceros sin consentimiento del titular	Desconocimiento por parte de los funcionarios del área de la normatividad legal vigente aplicable a la protección de datos personales	Sanciones penales y/o disciplinarias: "Ley 1581 de 2012 Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales" PQRSF Afectación de la imagen institucional	3	Posible	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 2 años	3	Moderado	Si el hecho llegara a presentarse, tendría Medianas consecuencias o efectos sobre la entidad.	Alta	evitar y verificar eventos de posible pérdida información por parte de empleados. Suministrar información al solicitante sin autorización	llamados de atención contratación del personal, deja claro constancia de sus funciones

Fuente. Autores del proyecto

Tabla 11 ***Valores de Medición proceso probabilidad Matriz de Riesgos motel Dubai***

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

Fuente. Tomada fuente externa, ajustada por Autores del proyecto

Tabla 12 ***Valores de Medición Riesgo de proceso Matriz de Riesgos motel Dubai***

MEDICIÓN DEL RIESGO DE PROCESO IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse tendría consecuencia o efectos mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse tendría bajo impacto o efecto sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Fuente. Tomada fuente externa, ajustada por Autores del proyecto

Identificación y medición del riesgo. Con el cual se podrá realizar y trabajar de forma ajustada, permitiendo mayor control para así ser incluido en una base de datos de riesgos y generar informes más claros.

4.1.7 Resultados del diagnóstico de la seguridad física en la empresa motel Dubai. En relación con los datos obtenidos y las evidencias tomadas se puede identificar que el espacio físico tiene una distribución de elementos que no la adecuada, ya que se evidencia que a medida

que se iba necesitando se fue añadiendo por lo tanto no hubo planeación a futuro crecimiento empresarial.

Al ingresar a las áreas como por ejemplo Aseo se debe ingresar por la zona administrativa y de contabilidad la cual no tiene una demarcación y ni paneles que aíslen de forma física los accesos no autorizados, es decir que generen independencia de oficinas, exponiendo carpetas de la documentación y sus equipos; además se evidenció que existe solo una puertas en vidrio templado recubierto de papel oscuro por seguridad cuenta con cerradura mecánica de llave manual, que pueden ser manipuladas fácilmente, exponiendo la información a pérdida o robo por parte de personal de la empresa o agentes externos, solo existe un aviso físico de área restringida el cual no es un control tan efectivo, por otra parte el área de administración es fácil acceso por parte de cualquier persona ya que se encuentra ubicada en toda la entrada controlada por la puerta antes mencionada y un sistemas de 3 cámaras que registran 24/7 la evidencia del ingreso del personal, en teoría solo deben ingresar a esta área contador y recepción los cuales son responsables de estos equipos que están ubicados en la administración.

Se logra establecer que la seguridad física es causal de la posible pérdida de la información de la empresa, la vulnerabilidad se incrementa ante cualquier incidente afectando la integridad, disponibilidad y confidencialidad de los datos.

Hablar de integridad de la información y los datos se dice que no se deben realizar, afectar o modificar los datos e información con sus procesos por parte de personal autorizado o no autorizado, los cuales pueden ser conscientes de estas pérdidas o por omisión de conocimiento.

Para la integridad de la información decimos que puede ser afectada por accidente o sevicia se modifica, altera o más grave borrar los datos que son parte esencial de la información de la empresa, conociendo que el área de acceso es compartida y cualquier persona puede acceder al espacio físico y por ende verse afectada la toda la información. La información es disponible cuando se puede acceder a ella de manera confiable y oportuna, por parte del personal que la requiera; dicho esto al no contar con controles de acceso efectivos en la entrada adecuados la empresa corre gran riesgo de pérdida, manipulación y daño de equipos e información, ocasionando pérdidas que no se pueden cuantificar en la parte de la información.

La confidencialidad es la característica de la información supremamente importante para la empresa motel Dubai, donde se administra información contable y financiera, de seguridad por parte de las cámaras de vigilancia que es muy sensible y secreta para la gran mayoría de personal laboral y mucho aún más para el personal externo, por esto la empresa debe prevenir el ingreso y manipulación no autorizado de cualquier tipo a la información.

4.2 Identificación y análisis de los componentes que integran el plan de gestión de seguridad para la empresa motel Dubai de acuerdo a las normas ISO/IEC 27001 Y 27002.

El plan de gestión de seguridad de la información permite diseñar la estrategia para manejar, coordinar y controlar las acciones de la empresa en el periodo de tiempo establecido para el funcionamiento de sus servicios, esto incluye técnicas y estrategias que tengan en cuenta los aspectos fundamentales para una correcta administración de la información,

Es necesario aclarar que dicho plan de gestión define los puntos a seguir, cómo debe hacerse, estar elaborado racionalmente a las necesidades de la empresa, debe ser claro, conciso y puntual para evitar extravíos o malos entendidos en el cumplimiento del mismo.

Dicho esto, define una estructura lógica para el plan de gestión de seguridad de la información de la empresa MOTEL DUBAI que suministra su análisis y a la vez que es entendible para todo el personal que labora en la empresa.

4.2.1 Estructura del plan de gestión

Objetivo del plan de gestión, será claro e indicando específicamente que se logrará con la implementación de este, permitiendo identificar el resultado final que se busca.

Alcance. Establecerá las normas por las cuales que se producirá el plan de gestión de seguridad de la información, describirá los aspectos de estrategias y limitaciones, el tiempo y encargados de la implementación del plan.

Responsables. En este punto se concretarán los responsables de la elaboración del plan de gestión, nivelando quien será encargado de su implementación, precisando el responsable de la supervisión, actualización, evaluación del mismo, con el fin de asignar compromisos y cargos que permitan dar cumplimiento a lo propuesto.

Recursos. Conformar y definir los recursos necesarios para las necesidades de disponibilidad presupuestal a los requerimientos económicos, físicos y humanos que se estiman dentro del plan de gestión de seguridad de la información de la empresa.

Estrategias. Enumerar de forma clara las políticas para gestionar la seguridad de la información, como se debe realizar. Se indicará los lineamientos para que la empresa logre un nivel de seguridad apropiado, reduciendo riesgos y posibles amenazas de diferentes agentes.

Actividades. Se toma como base la norma de seguridad de la información ISO 27001:2013, para indicar la política que da cumplimiento a los indicadores establecidos en ella, realizando actividades relacionados con los requerimientos de la empresa,

4.2.2 Criterios normativos para el plan de gestión MOTEL DUBAI. Para el proyecto, se observó las normas existentes afines con la seguridad de la información, se determina que el desarrollo del proyecto debe realizarse con base en las normas ISO/IEC 27001: 2013 y complementando en la ISO/IEC 27002: 2013, las cuales son guías de buenas prácticas, que permiten definir los objetivos y principios generales. La ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) para cualquier organización sin importar su tipo o tamaño. (Instituto colombiano de normas técnicas y certificación. , 2007)

La norma ISO/IEC 27002: 2013, establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una

organización. Los objetivos de control y los controles son implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. La norma ISO/IEC 27001: 2013 cuenta 10 cláusulas, contiene 14 dominios, 35 objetivos de control y 114 controles de seguridad.

Figura 19. Contenido norma ISO/IEC 27002:2013
Fuente. ISO/IEC 27002:2013. Dominios, Objetivos de Control y Controles

En esta norma se tiene que cada dominio contiene un número de objetivos de control de seguridad principales. Los catorce dominios (acompañados por el número de objetivos de control incluidos en cada dominio) son:

Tabla 13 ***Dominio, Objetivos de Control, Controles, número de controles empleados en este proyecto***

Cantidad	Dominio	Objetivos de control	Controles
1	5. Políticas De Seguridad.	5.1 Directrices de la Dirección en seguridad de la información.	5.1.1 Conjunto de políticas para la seguridad de la información.
1	6. Aspectos organizativos de la seguridad de la información	6.1 Organización interna.	6.1.1 Asignación de responsabilidades para la segur de la información.
3	7. Seguridad Ligada A Los Recursos Humanos	7.2 Durante la contratación.	7.2.1Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información 7.2.3 Proceso disciplinario
3	8. Gestión De Activos.	8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos
		8.2 Clasificación de la información.	8.2.2 Etiquetado y manipulado de la información.
5	9. Control De Accesos.	9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos.
		9.2 Gestión de acceso de usuario.	9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.4 Gestión de información confidencial de autenticación de usuarios.
		9.4 Control de acceso a sistemas y aplicaciones.	9.4.1 Restricción del acceso a la información. 9.4.3 Gestión de contraseñas de usuario.
4	11. Seguridad Física Y Ambiental.	11.1 Áreas seguras.	11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos.
		11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
2	12. Seguridad En La Operativa.	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información.
		12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software.
2	13. Seguridad En Las Telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.
		13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.

4	14. Adquisición, Desarrollo Y Mantenimiento De Los Sistemas De Información.	14.1 Requisitos de seguridad de los sistemas de información.	14.1.3 Protección de las transacciones por redes telemáticas.
		14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
			14.2.5 Uso de principios de ingeniería en protección de sistemas.
		4.3 Datos de prueba.	14.3.1 Protección de los datos utilizados en pruebas.
4	16. Gestión De Incidentes En La Seguridad De La Información.	16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.1 Responsabilidades y procedimientos.
			16.1.5 Respuesta a los incidentes de seguridad.
			16.1.6 Aprendizaje de los incidentes de seguridad de la información.
			16.1.7 Recopilación de evidencias
2	17. Aspectos de Seguridad de La Información En La Gestión De La Continuidad Del Negocio.	17.1 Continuidad de la seguridad de la información.	17.1.1 Planificación de la continuidad de la seguridad de la información.
		17.2 Redundancias.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
5	18. Cumplimiento.	18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable.
			18.1.3 Protección de los registros de la organización.
			18.1.4 Protección de datos y privacidad de la información personal.
		18.2 Revisiones de la seguridad de la información.	18.2.1 Revisión independiente de la seguridad de la información.
			18.2.2 Cumplimiento de las políticas y normas de seguridad.

Fuente. Autores del proyecto. Basado en la ISO/IEC 27002:2013

Realizando un análisis más preciso de la norma ISO/IEC 27002 y aplicado a la empresa motel Dubái, teniendo en cuenta las condiciones y necesidades identificadas en la empresa, se

define el diseño del plan de gestión de seguridad para controlar el acceso a las áreas vitales de la empresa con base en lo siguiente:

- Generalidades
- Objetivos
- Alcance
- Políticas
- Domino
- Objetivos de control
- Controles

Teniendo en cuento los criterios de los dominios seleccionados para el plan de gestión de seguridad de la empresa motel Dubái, se seleccionan con base a las definiciones de estos en la guía, con respecto a su aplicabilidad al control del acceso físico para la empresa.

Política de seguridad. Sabiendo que la empresa no dispone de ninguna política de seguridad reconocida y que por parte los trabajadores existe la voluntad para mejorar los procesos, se establece el objetivo principal, que será la creación de una política adecuada que se ajuste a las condiciones de la empresa, esta marcará los puntos a seguir por los trabajadores para preservar la seguridad de la información, de la mano con la política de seguridad, se definirán las bases del que será el Sistema de Gestión de Seguridad de la Información. Será de vital importancia que por medio del plan de gestión de seguridad se dan los lineamientos para

proteger la información de posibles amenazas que afecten el normal funcionamiento y trabajo en la empresa.

Aspectos organizativos de la seguridad de la información. Permitir administrar la seguridad de la información de la empresa motel Dubái, estableciendo un modelo gerencial para vigilar su ejecución. Este dominio le ayuda a la empresa a que exista responsabilidad por parte de la gerencia en la asignación de roles y sus responsabilidades encaminadas a la seguridad de la información.

Gestión de Activos. La empresa no contaba con un inventario de activos, tampoco un detallado según su función o importancia dentro de la organización de la empresa, todo software utilizado disponga de las licencias pertinentes. Aquellos que no las tenían se realizó la anotación respectiva, se busca que la empresa motel Dubai tenga presente que debe lograr y a su vez mantener una adecuada protección de los activos físicos y lógicos, gestionando estrategias que alcancen estas metas, por eso la importancia de estar constantemente con el tema de inventarios de los activos, logrando controlar por parte de la administración estos recursos.

Seguridad ligada a los recursos humanos. Enfocado a minimizar los riesgos generados por equivocación de las personas, un mal uso de las instalaciones y equipos ya bien sea por falta de capacitación u otras, para la empresa es primordial ya que por medio del mismos se busca garantizar que los empleados conozcan y cumplan con sus responsabilidades o funciones, logrando así un óptimo desempeño y aprovechamiento de los recursos, generando disminución de los riesgos de hurto, estafa y uso indebido de la información.

Seguridad física y ambiental. Actualmente los activos de la empresa están clasificados en varios lugares. Se estableció que los elementos de oficina y hardware para el funcionamiento de los servicios están en el mismo lugar, otro son los dispositivos de seguridad como las cámaras y servidor principal los cuales se encuentran en la misma área física, no obstante, no existe o hay constancia de algún método de control de acceso donde éstos queden restringidos a personal ajeno a esta dependencia, el resto de activos de la empresa físicos, no se tiene ningún control de acceso ni registro de las personas que acceden a la áreas. Si existe cámaras y personal de seguridad, que busca impedir accesos no autorizados, daños e interferencia a las instalaciones e información de la empresa motel Dubái, pero su efectividad en el caso del factor humano es mínima y a veces poco funcional dado las cantidades de obligaciones puestas a este personal. Con las cámaras si existe aplicabilidad y permite identificar para posteriormente evitar el máximo riesgo de accesos físicos no autorizados

Gestión de incidentes en la seguridad de la información. Encaminado a la gestión de eventos que pueden llegar a afectar integridad, confidencialidad y disponibilidad de la información y los activos físicos de la empresa motel Dubái, de allí la importancia de usar una gestión de dominio de este tipo de características que permiten establecer las responsabilidades y los procedimientos a seguir con la finalidad de administrar de forma eficiente los sucesos y posibles vulnerabilidades de la seguridad de la información de la empresa.

Aspectos de Seguridad de la información en la gestión de la continuidad del negocio. Es importante siempre tener en cuenta que le permitirá a la empresa la implementación de una gestión de la continuidad del negocio que, para minimizar el impacto sobre la empresa,

posteriormente permitiéndole recuperarse de las posibles y eventuales pérdidas de activos de información hasta cierto punto, por medio de la combinación de controles preventivos y de recuperación de la información.

Cumplimiento. Este de vital importancia tener en cuenta esta misión, ya que gracias a la aplicación de estos controles permite evitar las transgresiones a cualquier estatuto o norma, reguladora o establecida; cualquier requerimiento de seguridad, de la misma manera la empresa motel Dubái regulada por varias secretarias municipales y entes territoriales debe practicar y acatar la normatividad que se dicta a diario en temas de este tipo de establecimientos.

Todos los dominios, objetivos de control y controles que establece la norma mencionada son ajustables a cualquier empresa, pero es de aclarar que para el caso práctico del motel Dubái se optaron sólo los citados anteriormente teniendo siempre presente las necesidades de diseñar un Plan de Gestión que genere los controles necesarios para impedir el acceso no autorizado a las áreas vitales de la empresa. Por tal motivo los dominios seleccionados son los relacionados con seguridad física y organizativa, no se tuvo en cuenta el demás dominio ya que su orientación es hacia la seguridad, pero de otro tipo y no aplican para el presente trabajo; además la empresa no permitió el acceso en algunos equipos e información por ser información empresarial interna.

4.2.3 Análisis diferencial del estado actual. Este análisis se realiza con respecto a la ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, lo cual nos permitirá conocer de forma global el estado de la empresa con respecto a los sistemas de gestión de la seguridad actuales.

Para poder revisar los distintos controles que están englobados dentro de la ISO/IEC 27002:2013 podemos revisar el siguiente:

Para poder cuantificar el estado de los diferentes controles realizaremos una estimación del estado de los mismos tal como se marca en el enunciado del TFM. Para ello emplearemos el Modelo de Madurez de la Capacidad o CMM

Tabla 14 *Modelo de Madurez de la Capacidad o CMM.*

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCION
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver
10%	L1	Inicial	Estadoinicialdondeeléxito de lasactividades de losprocesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivelcorporativo.
50%	L2	Reproducible pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cadaindividuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionable y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución delosprocesos. Sedispone de tecnologíaparaautomatizarelflujode trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Fuente. Modelo de Madurez de la capacidad

Tabla 15 ***Una vez definidos el distinto estado de madurez procedemos al análisis de los controles de la ISO/IEC 27001:2013.***

NOMBRE DE CONTROLES	CUMPLIDO
4.CONTEXTO DE LA ORGANIZACIÓN	
4.1 Comprensión de la organización y de su contexto	**L1**
4.2Comprensióndelasnecesidadesyexpectativasdelaspartesinteresadas	**L1**
4.3 Determinación del alcance del SGSI	**L0**
4.4 SGSI	**L0**
5. LIDERAZGO	
5.1 Liderazgo y compromiso	**L1**
5.2 Política	**L1**
5.3 Roles, responsabilidades y autoridades en la organización	**L2**
6. PLANIFICACIÓN	
6.1 Acciones para hacer frente a los riesgos y oportunidades	**L0**
6.1.1 General	**L0**
6.1.2 Valoración de los riesgos de seguridad de la información	**L0**
6.1.3 Tratamiento de los riesgos de seguridad de la información	**L1**
6.2Objetivosdeseguridaddelainformaciónyplanificaciónparaconseguirlos	**L1**
7. SOPORTE	
7.1 Recursos	**L1**
7.2 Competencia	**L1**
7.3 Concienciación	**L1**
7.4 Comunicación	**L1**
7.5 Información documentada	**L2**
7.5.1 General	**L1**
7.5.2 Creando y actualizando	**L1**
7.5.3 Control de la información documentada	**L0**
8. OPERACIÓN	
8.1 Planificación y control	**L1**
8.2 Valoración de los riesgos de la seguridad de la información	**L1**
8.3 Tratamiento de los riesgos de la seguridad de la información	**L1**
9. EVALUACIÓN DEL DESEMPEÑO	
9.1 Seguimiento, medición, análisis y evaluación	**L1**
9.2 Auditoría interna	**L0**
9.3 Revisión por la dirección	**L0**
10. MEJORA	
10.1 No conformidad y acciones correctivas	**L0**
10.2 Mejora continua	**L0**

Fuente. Autores del proyecto. Basado en la ISO/IEC 27001:2013

Si revisamos el estado actual con respecto a la norma ISOI/IEC 27001:2013 se observa la situación de la empresa con relación a la norma.

Como podemos apreciar los indicadores son muy bajos debido a que la empresa actualmente carece de un sistema de seguridad de la información implantado y la gestión del mismo actualmente está en un estado de inmadurez.

Al igual que en podemos observar que disponen de correctas medidas técnicas en muchas áreas y controles que nos dan buenas perspectivas de cara a la ISO/IEC 27002:2013, en el caso de la ISO/IEC 27001:2013 podemos apreciar que la Dirección y personal tienen un poco conocimiento de la seguridad de la información de la empresa.

4.3 Elaboración del plan de gestión de seguridad de la información mediante una serie de lineamientos que permiten controlar el acceso a las áreas restringidas a la empresa Motel Dubai

La información es considerado hoy en día un activo tan importante, ya que su característica intangible hace que sea valorado y resguardado de una forma más segura y comprometida con la integridad, de la misma forma existen otros activos comerciales importantes fundamentales para el negocio de toda empresa, es por esto que se ve la necesidad de proteger de forma adecuada estos activos, ya que en la actualidad debido a las conectividad cada vez más accesible ha permitido integrar diferentes sistemas a los activos de las empresas, provocando un resultado que para nadie es grato al cual la información ahora está expuesta a un número cada vez más amplio de amenazas y una lista de vulnerabilidades creciente por la masificación de los sistemas de información, equipos y conexiones a la red.

Debemos recordar que toda la información de hoy se halla en muchas formas, esta puede estar impresa, almacenada por medios electrónicos, esta a su vez puede ser transmitida por medio de correo electrónico, dispositivos móviles, conexiones bluetooth, expuesta en videos, conversada en audios o cualquier otro medio físico y digital que pueda contener y transmitir información, la cual debería estar debidamente protegida o resguardada

Habiendo conocido las necesidades esenciales en el tema de manejo de la información de la empresa motel Dubái, reconociendo la importancia de la seguridad de la información en las empresa en este caso la nuestra, se formula el documento de plan de gestión de seguridad de la información que permite establecer los controles necesarios que garanticen la protección, la disminución de los riesgos por de pérdida de información y activos, posibles daños irreparables a los equipos afectando la calidad de los servicios prestados por la empresa

4.3.1 Documento del plan de gestión de seguridad de la información Motel Dubai. El objetivo del presente plan de gestión de seguridad de la información es crear los lineamientos necesarios que garanticen la protección de los activos y recursos de almacenamiento de información de la empresa motel Dubai, resguardando la seguridad en las TIC utilizadas, las cuales se enfrentan a unas amenazas muy serias ya sean de tipo internas o externas, buscando de manera segura los criterios de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información de la empresa. El presente instrumento se establece en cumplimiento de las normas legales vigentes aplicadas a este tipo de activos, con el propósito de brindar y administrar apropiadamente la seguridad de la información, para el entorno físico y tecnológico de la empresa Motel Dubai se debe conocer y cumplir por parte de todo el personal

que labora en la empresa. El establecimiento de la etapa de implementación es compromiso de la gerencia y personal de la empresa.

La etapa de implementación del plan de seguridad de la información, así como las fases de revisión y actualización del plan, es compromiso o responsabilidad de la gerencia la cual debe apoyarse siempre en el comité de seguridad de la información de la empresa, para dicho comité se deberá crear y establecer en base a las políticas y acuerdos generados en vía de la seguridad de la información de la empresa, que se conforma en el presente plan de gestión de seguridad de la información. Dada la documentación del presente documento del plan de gestión de seguridad de la información con diseños de formatos especiales que son diferentes al cuerpo del presente trabajo, dicho documento está incluido como anexos, es importante tener en cuenta la asignación de roles y responsabilidades relativas a la seguridad de la información en DUBAI, por lo tanto, se diseñó el siguiente cuadro teniendo en cuenta el personal con que cuenta la empresa y sus funciones frente a la protección de la información y como quedaría conformado el comité de seguridad de la información.

Tabla 16 ***Asignación de roles y responsabilidades***

ROL	RESPONSABLE	RESPONSABILIDAD
Comité de seguridad de la información	Gerente	Coordinar el comité de seguridad de la información Implementar y cumplir la presente política
información	Jefe de área	Definir que usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
Área de recursos humanos	Contador publico	Notificar a todo el personal que ingrese las obligaciones del cumplimiento de la Política de Seguridad de la Información, los procedimientos y prácticas Implementar la suscripción de los acuerdos de confidencialidad y las tareas de capacitación en materia de seguridad de la información
usuarios	Personal de la empresa	Conocer y cumplir con la política de seguridad de la información

Fuente: Autores del proyecto

4.3.2 Propuesta de implementación del plan de gestión de seguridad de la información.

Luego de haber diseñado el plan de gestión de seguridad de la información para la empresa MOTEL DUBAI, se dejó elaborado una propuesta de posible implementación que puede ser usada por la empresa como herramienta para ello si así lo decide, sumado a esto se crea y describe un presupuesto para que Motel Dubai cuente con una estimación de la inversión que debe realizar para tal fin y estimando el tiempo que se requiere para llevar a cabo dicha implementación tal como se muestra a continuación.

Tabla 17 ***Propuesta de implementación***

ESTRATEGIA	RESPONSABLE	PRESUPUESTO
Generar un comité de gestión de la seguridad de la información que Autorice de la implementación, revisión y actualización de las políticas de seguridad.	Gerente	$ 0
Concretar actividades específicas que identifiquen las exigencias del plan de gestión de seguridad.	Comité de seguridad de la información	$ 300.000
Crear un cronograma para la realización de las actividades de las políticas de seguridad de la información.	Comité de seguridad de la información	$ 100.000
Asignar responsables para la ejecución de cada actividad de control en la política de seguridad de la información, de acuerdo al cargo dentro de la empresa.	Comité de seguridad de la información	$ 0
capacitación de la política de seguridad de la información de la empresa	Gerente	$ 500.000
Ejecución del Plan de Gestión de Seguridad	Comité de seguridad de la información	$ 1.000.000
Implementación del plan de gestión de seguridad de la información	Comité de seguridad de la información	$ 4.000.000
Elaboración de auditorías internas periódicas por parte del comité de seguridad de la información para evaluar el proceso de implementación del plan de gestión de seguridad de la información en la empresa.	Comité de seguridad de la información	$ 200.000
TOTAL, PRESUPUESTO		6.100.000

Fuente. Autores del proyecto

Tabla 18 ***Cronograma de elaboración del proyecto***

Actividades	Fecha Inicial	Fecha Final	Duración	Marzo 2019				Abril 2019			
				1° semana	2° semana	3° semana	4° semana	1° semana	2° semana	3° semana	4° semana
DIAGNOSTICO											
Determinar el estado actual en la gestión de seguridad	4 DE MARZO DE 2019	8 DE MARZO DE 2019									
Identificar vulnerabilidades (autoevaluación de controles)	4 DE MARZO DE 2019	8 DE MARZO DE 2019									
PLANEACIÓN											
Realizar análisis entorno a la seguridad de la información	11 DE MARZO DE 2019	15 DE MARZO DE 2019									
Definir el alcance del SGSI	11 DE MARZO DE 2019	15 DE MARZO DE 2019									
Definir roles y responsabilidades de seguridad de la información	11 DE MARZO DE 2019	22 DE MARZO DE 2019									
Elaborar políticas de seguridad de la empresa	11 DE MARZO DE 2019	29 DE MARZO DE 2019									
Identificar los activos de información	25 DE MARZO DE 2019	29 DE MARZO DE 2019									
Identificar los riesgos de seguridad de la información	4 DE MARZO DE 2019	29 DE MARZO DE 2019									
Definir plan de capacitación, comunicación y sensibilización	25 DE MARZO DE 2019	5 DE ABRIL DE 2019									
EVALUACIÓN DE DESEMPEÑ											

O							
Ejecución auditoria de seguridad de la información	25 DE MARZO DE 2019	5 DE ABRIL DE 2019					
MEJORA CONTINUA							
Diseñar plan de mejoramiento	25 DE MARZO DE 2019	12 DE ABRIL DE 2019					

Fuente. Autores del proyecto

Tabla 19 ***Evaluación Cumplimiento Controles ISO 27002:2013***

			RESPUESTA	VALOR	EVIDENCIA	OBSERVACION
ITEM	**DOMINIO**					
5	**POLITICA DE SEGURIDAD**				1	
5.1	Politica de Seguridad de la Información	Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.				
5.1.1	Documento de la política de seguridad de la información	¿Se tiene una Política de seguridad de la información desarrollada y documentada?	NO CUMPLE	1		No implementado/ inexistente
		¿El documento de políticas de seguridad de la información se encuentra publicado?	NO CUMPLE	1		No implementado/ inexistente
5.1.2	Revisión de la política de seguridad de la información	¿Este es revisado por la dirección constantemente?				
6	**ORGANIZACIÓN DE SEGURIDAD**				1,083333333	
6.1	**Organización de la SI**	**Se debería establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro**				

		de la organización.			
6.1.1	Compromiso de la dirección con la seguridad de la información	¿Se evidencia el compromiso demostrado de la dirección frente a la seguridad de la información en la organización?, Con una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información?	NO CUMPLE	1	por no contar con las políticas de seguridad de la información , no hay responsable de la seguridad
6.1.2	Coordinación de la seguridad de la información	¿Ha sido establecido un proceso para coordinar la implementación o puesta en práctica de las medidas de seguridad de la información?	NO SABE	0	
6.1.3	Asignación de responsabilidades para la seguridad de la información	¿Las responsabilidades de la realización de los requisitos/requerimientos/responsabilidades de la seguridad de la información se definen claramente? ¿Han sido definidos?	NO CUMPLE	1	por no contar con las políticas de seguridad de la información, no hay responsable de la seguridad
6.1.4	Proceso de autorización para los servicios de procesamiento de información	¿Se ha establecido un proceso de autorización de la dirección para nuevos servicios de procesamiento de información? (Punto de vista del negocio y técnico)	NO CUMPLE	1	
6.1.5	Acuerdos sobre confidencialidad	¿Se ha definido un procedimiento de identificación y revisión de los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información?	NO CUMPLE	1	aunque no hay políticas establecidas se evidencia que cuando se contratan se les hace énfasis en la confidencialidad de la información

6.1.6	Contacto con las autoridades / contactos con grupos de interés especial	¿Existe un acuerdo o contactos con personal externo y/o organizaciones que maneje el tema de la seguridad de la información? incluyendo especialistas de la seguridad de la industria y/o de gobierno; autoridades de ley; Proveedores de servicio TI; autoridades de telecomunicaciones?	NO CUMPLE	1	no hay ningún acuerdo con personal externo
6.1.7	Revisión independiente de la seguridad de la información		CUMPLE PARCIALMENTE	2	cuenta con proveedor de servicio
6.2	**Partes Externas**	**Mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso terceras partes o que son procesados, comunicados o dirigidos por éstas.**			
6.2.1	Identificación de los riesgos relacionados con las partes externas	¿Una revisión independiente de las prácticas de la seguridad de la información se ha conducido para asegurar viabilidad, eficacia, y conformidad con políticas escritas? ¿Esta establecida la revisión a intervalos de tiempo planificados?	NO CUMPLE	1	no hay un cronograma para la revision de la politicas de seguridad
6.2.2	Riesgos conexiones con terceros	¿Se han analizado los riesgos para la información y los servicios de procesamiento de información en los procesos de negocio que incluyen o involucran a partes externas?	NO CUMPLE	1	no se cuenta con el analisis de los riesgos externos para la seguridad en la informacion
6.2.3	Abordaje de la seguridad cuando se trata con los clientes	¿Se han identificado las medidas de seguridad específicas	NO CUMPLE	1	no han identifiacado los riesgos por conexión

		de combatir riesgos de la conexión de los terceros?				
6.2.4	Abordaje de la seguridad en los acuerdos con terceras partes	¿Se han identificado los requisitos de seguridad antes de dar acceso a los clientes a los activos o la información de la organización?	CUMPLE PARCIALMENTE	2		no se brinda informacion a terceros de los activos de la empresa
6.3	Partes Externas (outsourcing)	¿Los requisitos de la seguridad se incluyen en contratos formales con terceras partes?	NO CUMPLE	1		no se cuenta con un contratos para terceros
7	**CONTROL DE ACTIVOS**				1,4	
7.1	**Responsabilidad por los activos**	**Lograr y mantener la protección adecuada de los activos de la organización. Todos los activos se deben incluir y deben tener un dueño designado**				
7.1.1	Inventario de activos	¿Los inventarios de activos importantes asociados a cada sistema de información se han creado?	CUMPLE PARCIALMENTE	2		si cuenta con los inventarios
7.1.2	Propiedad de los activos	¿La información y los activos asociados con los servicios de procesamiento de información tienen asignado un propietario parte de la organización?	CUMPLE PARCIALMENTE	2		porque se realiza una asignacion vervalmente pero no por escrito
7.1.3	Uso aceptable de los activos	¿Se han identificado, documentado e implementado reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información?	NO CUMPLE	1		falta la documentacion de las reglas para los activos y la informacion
7.2	**Clasificación de la información**	**Asegurar que la información recibe el nivel de protección adecuado**				

7.2.1	Directrices de clasificación	¿Las pautas de la clasificación de seguridad se han establecido para indicar la necesidad , y las prioridades, de la protección de la seguridad?	NO CUMPLE	1		no se ha implementado
7.2.2	Etiquetado y manejo de la información	¿Se ha implementado un procedimiento para el etiquetado y manejo de la información?	NO CUMPLE	1		la empresa no cuenta con ningun procedimiento de manejo y etiquetiado de la informacion
8	**SEGURIDAD DE LOS RECURSOS HUMANOS**				1,2222 22222	
8.1	**Antes de la Relación Laboral**	**Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.**				
8.1.1	Roles y responsabilidades	¿Las responsabilidades de la seguridad se incluyen en descripciones de las funciones del empleado?	NO CUMPLE	1		la emprresa no cuenta con un reglamento de funciones de manejo de la seguridad de la informacion
8.1.2	Selección	Son las aplicaciones de empleados para un trabajo revisadas de acuerdo al tipo de trabajo (Cargo) a realizar y los niveles de acceso a información sensible acorde con el cargo a cumplir?	NO CUMPLE	1		
8.1.3	Términos y Condiciones laborales	¿Los términos y las condiciones del empleo incluyen la responsabilidad del empleado de la seguridad de la información, incluyendo la duración después del empleo y	NO CUMPLE	1		no se cuenta en los termino y condiciones de los empleados ´por faltas la divulgacion de la informacion

		consecuencias de la falta de satisfacer estos términos?			
8.2	**Durante la Relación Laboral**	**Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respectos a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano**			
8.2.1	Responsabilidad de la dirección	Se evidencia una exigencia de la dirección para que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización?	NO CUMPLE	1	no hay ninguna exigencia por la organizacion para la aplicación de las politicas y procedimientos de seguridad
8.2.2	Educación, formación y concientización sobre la SI	Existe un programa de capacitación a empleados, contratistas, etc. de concientización de seguridad, políticas y procedimientos de seguridad , según sea pertinente para sus funciones laborales?	NO CUMPLE	1	no se cuenta con ningun documento de capacitacion a empleados y contratistas para la seguridad de la informacion
8.2.3	Proceso disciplinario	¿Existe definido un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la	NO CUMPLE	1	No implementado/ inexistente

		seguridad?			
8.3	**Terminación o cambio**	**Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.**			
8.3.1	Responsabilidades en la terminación	¿Existe un proceso de terminación donde estén claramente definidas las responsabilidades para llevar a cabo la terminación o el cambio de la relación laboral con empleados?	NO CUMPLE	1	Se ha hecho algo, manifestamente insuficiente
8.3.2	Devolución de activos	¿Existe establecido un procedimiento aplicado a los empleados, contratistas u usuarios de terceras partes donde se establezca como parte del mismo la devolución todos los activos de la organización que estén en su poder al finalizar su relación laboral, contrato o acuerdo?	CUMPLE PARCIALMENTE	2	lo realizan de forma verval pero no esta esyablecido por escrito
8.3.3	Retiro de los derechos de acceso	¿Existe un procedimiento (Documentado) de retiro de acceso a los sistemas de procesamiento de información a empleados, contratistas o terceras partes al finalizar la relación laboral, contrato o acuerdo?	CUMPLE PARCIALMENTE	2	al realizar el retiro se realiza el retiro de los derechos
9	**SEGURIDAD FISICA DEL ENTORNO**	**SEGURIDAD FÍSICA DEL ENTORNO**		1,076923077	
9.1	**Areas seguras**	**Evitar el acceso físico no autorizado, el daño e**			

		interferencia a las instalaciones y a la información de la organización.			
9.1.1	Perímetro de seguridad física	¿Existen elementos de seguridad física para proteger las áreas que contienen información y servicios de procesamiento?	CUMPLE PARCIALMENTE	2	solo ingresa el personal autorizado
9.1.2	Controles de acceso físico	¿Se emplean los controles de la entrada en áreas seguras para asegurar ingreso solamente a personal autorizado?	NO CUMPLE	1	pero no hay controles para el ingreso
9.1.3	Seguridad de oficinas, recintos y servicios	¿Es la seguridad física para los centros de datos y las salas de cómputo conmensurada con amenazas? (Documentada)	NO SABE	0	
9.1.4	Protección contra amenzas externas y ambientales	¿Existen mecanismos de protección física contra daño por incendio, inundación, terremoto, explosión, malestar social y otras formas de desastre natural o artificial?	NO SABE	0	
9.1.5	Trabajo en áreas seguras	¿Se utilizan controles adicionales para el personal o los terceros que trabajan en el área segura?	NO SABE	0	
9.1.6	Áreas de carga, despaho y acceso	¿Existen controles en los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones? Estos puntos se encuentran aislados de los servicios de procesamiento de información?	NO CUMPLE	1	no cuenta con los controles en los puntos de acceso
9.2	**Seguridad de los equipos**	**Evitar pérdida, daño, robo o puesta en peligro de los activos y la**			

		interrupción de las actividades de la organización			
9.2.1	Ubicación y protección de los equipos	¿El equipo se localiza para reducir riesgos de peligros ambientales y del acceso no autorizado?	CUMPLE PARCIALMENTE	2	
9.2.2	Servicios de soporte	¿El equipo electrónico se protege contra apagones y otras anomalías eléctricas?	CUMPLE PARCIALMENTE	2	cuentan con ups
9.2.3	Seguridad del cableado	¿El cable de la energía y de las telecomunicaciones se protege contra la interceptación o daño?	CUMPLE PARCIALMENTE	2	
9.2.4	Mantenimiento de los equipos	¿Se han establecido procedimientos para correcto mantenimiento de equipos y de esta forma asegurar su disponibilidad e integridad de manera continua?	NO CUMPLE	1	no se han establecido procedimientos para mantenimiento de los equipos
9.2.5	Seguridad de los equipos fuera de las instalaciones	¿Se aplica la misma seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización?	NO CUMPLE	1	no cuenta con la seguridad para los equipos fuera de la instalacion
9.2.6	Seguridad en la reutilización o eliminación de los equipos	¿Existe algún mecanismo para tratamiento de equipos una vez estos se reutilizan o eliminan? (Procedimiento)	NO CUMPLE	1	
9.2.7	Retiro de propiedad	¿Existe un procedimiento definido para retiro de equipos, información o software bajo previa autorización de la gerencia?	NO CUMPLE	1	no existe ningun procedimiento establecido
10	**GESTION DE LAS COMUNICACIONES Y OPERACIONES**	**GESTIÓN DE COMUNICACIONES Y**		1,2333333333	

		OPERACIONES			
10.1	**Procedimientos de Op. y Resp.**	**Asegurar la operación correcta y segura de los servicios de procesamiento de información.**			
10.1.1	Procedimientos de operación documentados	¿Se documentan los procedimientos de operación (funcionamiento) para que todos los sistemas informáticos aseguren su operación correcta y segura?	NO CUMPLE	1	no se documenta los procesos de operación
10.1.2	Gestión del cambio	¿Hay un proceso para el control de los cambios a las instalaciones de IT y los sistemas para asegurar el control satisfactorio de los equipos, software o a los procedimientos?	NO CUMPLE	1	
10.1.3	Distribución de funciones	¿Están establecidas separaciones entre las funciones y las áreas de responsabilidad para reducir las oportunidades de la modificación no autorizada o el mal uso de datos o de servicios? Especifique.	NO CUMPLE	1	no estan separadas las funciones en las areas de responsabilidad
10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	¿Las instalaciones de desarrollo, ensayo(Prueba) y producción (Operación) se separan para reducir el riesgo de cambios accidentales o del acceso no autorizado al software operacional y a los datos de negocio?	NO CUMPLE	1	no esta separado las instalaciones de desarrollo
10.2	**Gestión servicios de terceros**	**Implementar y mantener un grado adecuado de seguridad de la información y de la**			

		prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes			
10.2.1	Prestación del servicio	¿Los controles de seguridad, las definiciones del servicio y los niveles de prestación incluidos en el acuerdo de prestación del servicio por terceras partes, están siendo implementados, mantenidos y operados por las terceras partes?	NO CUMPLE	1	
10.2.1	Monitoreo y revisión de los servicios por terceras partes	¿Se controlan y revisan los servicios, reportes y registros suministrados por terceras partes?	CUMPLE PARCIALMENTE	2	se revisan los informes por terceros
10.2.3	Gestión de los cambios en los servicios por terceras partes	¿Se posee un procedimiento de gestión de cambios en la prestación de servicios con terceras partes? Incluir mantenimiento, mejoras de políticas existentes de seguridad, procedimientos, sistemas, etc.	NO CUMPLE	1	
10.3	**Planificación y aceptación del sistema**	**Minimizar el riesgo de fallas en los sistemas**			
10.3.1	Gestión de la capacidad	¿Se supervisan o hacen seguimiento los requisitos de la capacidad, y se proyectan los requisitos futuros, para reducir el riesgo de la sobrecarga del sistema?	NO CUMPLE	1	no se le hace verificacion a los sistemas de almacenamiento
10.3.2	Aceptación del sistema	¿Los criterios de la aceptación para los nuevos sistemas se han establecido?, y las pruebas convenientes se han	NO CUMPLE	1	no hay criterios para loss nuevos sistemas y no se realizan prueban

		realizado antes de la aceptación?			
10.4	**Protección contra códigos móviles y maliciosos**	**Proteger la integridad del software y de la información**			
10.4.1	Controles contra código maliciosos	¿Se han implementado las medidas preventivas de detección y prevención de virus y los procedimientos del concientización de usuarios?	NO CUMPLE	1	no cuentan con antivirus licenciados y los ususarios no tienen ninguna restriccion
10.4.2	Controles contra códigos moviles	¿Existe una política de seguridad definida para la autorización y tratamiento de código móvil ?	NO CUMPLE	1	no hay tratamiento de codigo movil
10.5	**Respaldo**	**Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.**			
10.5.1	Respaldo de información	¿Se ha establecido un procedimiento para hacer copias de respaldo de los datos y del software esenciales de negocio para asegurarse de que puede ser recuperado después de un desastre de sistema de cómputo o de una falta de los medios?	CUMPLE PARCIALMENTE	2	se realizan las copias de seguridad todos los dias
10.6	**Gestión de Seguridad de las redes**	**Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.**			
10.6.1	Controles de las redes	¿Existen controles apropiados que aseguran la seguridad de datos en redes, y la protección de servicios conectados contra el acceso no	CUMPLE PARCIALMENTE	2	Se ha hecho algo, manifestamente insuficiente

		autorizado?			
10.6.2	Seguridad de los servicios de red	Se tiene claro que en cualquier acuerdo sobre servicios de red se deberían identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red? ¿Se sigue esta práctica?	NO CUMPLE	1	Se ha hecho algo, manifestamente insuficiente
10.7	**Manejo de los medios**	**Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada y la interrupción en las actividades de negocio**			
10.7.1	Gestión de los medios removibles	¿Existen procedimientos para la gestión de los medios removibles de las computadoras tales como cintas, discos, cassettes, e informes impresos?	NO CUMPLE	1	No implementado/ inexistente
10.7.2	Eliminación de los medios	¿Existe un proceso implementado para asegurarse que los medios de la computadora son eliminados con seguridad cuando estos no se necesitan más?	NO CUMPLE	1	No implementado/ inexistete
10.7.3	Procedimientos para el manejo de la información	¿Existen procedimientos para manejar datos sensibles y para proteger tales datos contra acceso no autorizado o divulgación?	NO CUMPLE	1	No implementado/ inexistente
10.7.4	Seguridad de la documentación del sistema	¿La documentación del sistema se protege contra el acceso no autorizado?	NO CUMPLE	1	No implementado/ inlate
10.	**Intercambio de Información**	**Mantener la**			

8.		**seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.**			
10.8.1	Políticas y procedimientos para el intercambio de información	¿Existen establecidas políticas, procedimientos y controles formales de intercambio para proteger el intercambio de información a través del uso de todos los tipos de servicio de comunicación?	NO CUMPLE	1	No implementado/ inexistente
10.8.2	Acuerdos para el intercambio	¿Existen acuerdos para el intercambio de información y software entre la organización y partes externas?	NO CUMPLE	1	no cuentan intercambio de informacion
10.8.3	Medios Físicos en Tránsito	¿Se aplican controles para salvaguardar a los medios de la computadora que son transportados entre sitios para reducir al mínimo su vulnerabilidad al acceso no autorizado, al mal uso, o a la corrupción durante el transporte?	NO CUMPLE	1	No implementado/ insete
10.8.4	Mensajería electrónica	¿Se aplican controles cuando sea necesario reducir los riesgos de negocio y de seguridad asociados con el correo electrónico para dar frente a la interceptación, la modificación y errores?	NO CUMPLE	1	No implementado/ insete
10.8.5	Sistemas de información del negocio	¿Existen desarrolladas e implementadas políticas y procedimientos para proteger la información asociada con la interconexión	NO CUMPLE	1	No implementado/ inexistente

		de los sistemas de información del negocio?			
10. 9.	**Servicios de Comercio Electrónico**	**Garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.**			
10. 9.1	Comercio Electrónico	¿Se aplican controles de la seguridad para proteger comercio electrónico (los datos electrónicos intercambian, correo electrónico, y las transacciones en línea a través de una red pública tal como el Internet) contra la interceptación o la modificación desautorizada?	CUMPLE PARCIALMENTE	2	cuentan con controles de seguridad en ciertas cuentas
10. 9.2	Transacciones en línea	¿Se implementan mecanismos de protección de información en transacciones en línea para evitar transmisión incompleta, enrutamiento inadecuado, alteración no autorizada del mensaje, divulgación no autorizada, duplicación o repetición no autorizada del mensaje?	NO SABE	0	
10. 9.3	Información disponible al público	¿Hay un proceso formal de la autorización antes de que la información se haga disponible al público?	CUMPLE SATISFACTORIAMENTE	3	se cuenta con un documento formal donde se autoricee la entrega de informacion para que se haga disponible al publico
10. 10.	**Monitoreo**	**Detectar actividades de procesamiento de información no autorizada**			

10.10.1	Registro para auditoría	¿Existe procedimiento o disposición para mantener y elaboran durante un periodo acordado la grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.?	NO CUMPLE	1	no hay ningun procedimiento establecido
10.10.2	Monitoreo del uso del sistema	¿Existen procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo y se revisan con regularidad.?	NO CUMPLE	1	no se cuenta con ningun documento para el procesamiento de la informacion
10.10.3	Protección de la información del registro	¿Existen controles (Procedimientos) para el manejo y almacenamiento de la información con el fin de protegerla contra divulgación no autorizada o uso inadecuado?	CUMPLE PARCIALMENTE	2	Cumple implementado/ inexistente
10.10.4	Registros de administrador y de operador	¿Se mantiene un registro de las actividades tanto del operador como del administrador del sistema?	CUMPLE PARCIALMENTE	2	Cumple implementado/ insete
10.10.5	Registro de fallas	¿Existe cultura o reglas definidas para el registro para posterior análisis sobre fallas? Y basado en estas tomar las acciones adecuadas?	NO CUMPLE	1	no cuentan con reglas establecidas para el analisis de las fallas

10.6	Sincronización de relojes	¿Se han fijado a un estándar para asegurar la exactitud de los registros de la auditoria respecto al tiempo, donde se mantengan sincronizados los relojes de los sistemas o dispositivos de comunicaciones?	NO CUMPLE	1		no hay un estandar para asegurar la exactitiud de los registros
11.	**CONTROL DE ACCESO**	**CONTROL DE ACCESO**			0,88	
11.1.	**Requisitos del negocio para el control de acceso**	**Controlar el acceso a la información**				
11.1.1	Política de control del acceso	¿Los requisitos del negocio se definen y se documentan para el control de acceso?	CUMPLE PARCIALMENTE	2		lo tienen establecido vervalmente, pero no la han realizzado por escrito
11.2.	**Gestión de Acceso de Usuarios**	**Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información**				
11.2.1	Registro de usuarios	¿Hay un procedimiento formal del registro y de la cancelación de registro del usuario para el acceso a todos los servicios de información?	CUMPLE PARCIALMENTE	2		no hay un proceso formal, pero si vervalmente
11.2.2	Gestión de privilegios	¿Hay restricciones y controles sobre la asignación y uso de privilegios de los usuarios en los sistemas de información (Multiusuario)? ¿Existe un proceso formal para esto?	CUMPLE PARCIALMENTE	2		si cuentan con privilegios para ingresar al sistema de informacion
11.2.3	Gestión de contraseñas para usuarios	¿Se ha establecido un proceso formal de gestión de las contraseñas?	NO SABE	0		No implementado/ insete
11.2.4	Revisión de los derechos de acceso de los usuarios	¿Existe un proceso formal para la revisión periódica de los derechos de acceso de usuarios?	NO SABE	0		No implementado/ inexistente

11.3.	**Responsabilidades de los usuarios**	**Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información**			
11.3.1	Uso de contraseñas	¿Se han enseñado los usuarios buenos prácticas de la seguridad en la selección y el uso de contraseñas?	NO SABE	0	No implementado/ inexistente
11.3.2	Equipo de usuario desatendido	¿Se concientiza a todos los usuarios y contratistas de los requisitos y de los procedimientos de la seguridad para proteger equipo desatendido? ¿Están todos los usuarios y contratistas concientizados de sus responsabilidades de poner tal protección en ejecución?	NO CUMPLE	1	no han realizo capacitaciones para concientizar a los usuarios sobre los procedimientos de seguridad
11.3.3	Política de escritorio despejado y de Pantalla despejada	¿Se tiene adoptada una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información?	NO CUMPLE	1	no cuenta con políticas de escritorio despejada
11.4.	**Control de Acceso a redes**	**Evitar el acceso no autorizado a servicios en red**			
11.4.1	Política del uso de los servicios en red	¿Un proceso existe para asegurarse de que la red y los servicios informáticos que se pueden alcanzar por un usuario individual o de una Terminal particular son consistentes con la política del control	NO CUMPLE	1	no hay control de acceso establecidas por escrito todo se realiza de forma verval

		de acceso del negocio?			
11.4.2	Autenticación de usuarios para conexiones externas	¿Las conexiones de los usuarios remotos vía redes públicas o no pertenecientes a la organización se autentican para prevenir el acceso no autorizado a las aplicaciones del negocio?	NO SABE	0	No implementado/ inlaste
11.4.3	Identificación de los equipos en las redes	¿Existe un mecanismo de identificación automática de los equipos que sirva para autenticar conexiones de equipos y lugares específicos? ¿Qué métodos se utilizan para dicha identificación?	NO SABE	0	No implementado/ inexistente
11.4.4	Protección de los puertos de configuración y diagnóstico remoto	¿Existe un proceso para controlar el acceso a los puertos de diagnóstico diseñados para el uso remoto por personal autorizado?	NO SABE	0	No implementado/ inexistente
11.4.5	Separación en las redes	¿Las redes grandes se han dividido en dominios separados para atenuar el riesgo del acceso no autorizado a los sistemas informáticos existentes que utilizan la red?	NO SABE	0	No implementado/ inlaste
11.4.6	Control de las conexiones en red	¿Se han incorporado controles para restringir la capacidad de la conexión de usuarios en aquellas redes que se extienden mas allá de las fronteras de la organización? (Dando cumplimiento a la política de acceso y	NO SABE	0	No implementado/ insete

		requisitos de aplicación del negocio)			
11.4.7	Control del enrutamiento en la red	¿Se han incorporado controles de enrutamiento a través de los límites de organización para asegurarse de que las conexiones de los sistemas de cómputo y la información fluye de acuerdo con la política del acceso de las unidades de negocio?	NO SABE	0	No implementado/ insete
11.5.	**Control de Acceso al sistema Operativo**	**Evitar el acceso no autorizado a los sistemas operativos**			
11.5.1	Procedimientos de ingreso seguros	¿Existe un procedimiento de registro de inicio seguro en los sistemas operativos?	NO CUMPLE	1	No implementado/ inexistente
11.5.2	Identificación y autenticación del usuario	¿Todos los usuarios tienen un identificador único (userID) para su uso personal y único, para asegurarse de que sus actividades se pueden rastrear?	CUMPLE PARCIALMENTE	2	solo en algunos casos se cumplen
11.5.3	Sistema de gestión de contraseñas	¿Un sistema de gestión eficaz de la contraseña se emplea para autenticar a usuarios?	CUMPLE PARCIALMENTE	2	hay contraseñas en la información contable
11.5.4	Uso de las utilidades del sistema	¿Se restringen los programas utilitarios de sistema que se podrían utilizar para pasar los controles de sistema y aplicaciones? Su uso es restringido?	NO SABE	0	
11.5.5	Tiempo de inactividad de la sesión	¿Las terminales en localizaciones de riesgo elevado se les configurada bloqueo cuando son inactivos por cierto tiempo a fin de prevenir el acceso por personas no autorizadas?	CUMPLE PARCIALMENTE	2	Cumple implementado/ inseguro

11.5.6	Limitación del tiempo de conexión	¿Se ha fijado un límite en el período durante el cual los terminales se pueden conectar con los sistemas de uso sensibles?	NO CUMPLE		No implementado/ inseguro
11.6.	**Control de Acceso a las Aplicaciones y a la Información**	**Evitar el acceso no autorizado a la información contenida en los sistemas de información**			
11.6.1	Restricción del acceso a la información	¿El acceso a los datos y a las funciones del sistema de aplicaciones se restringe de acuerdo con la política de acceso definida y esta se basa en requisitos individuales?	NO CUMPLE	1	no hay políticas establecidas
11.6.2	Aislamiento de sistemas sensibles	¿Según riesgos identificados, los sistemas de aplicaciones sensibles funcionan en un ambiente de proceso aislado?	NO SABE	0	No implementado/ inseguro
11.7.	**Computación Móvil y Trabajo Remoto**	**Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto**			
11.7.1	Computación y comunicaciones móviles	¿Se ha desarrollado una política formal que trata los riesgos del trabajo con las instalaciones de computación móvil, que incluyan los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, el respaldo, y la protección de virus?	CUMPLE PARCIALMENTE	2	solo la contadora puede trabajar remotamente, el programa que sutiliza es TeamViewer version14

11.7.2	Trabajo remoto	¿Las políticas y los procedimientos se han desarrollado para controlar teleworking, las instalaciones existentes que abarcaban, el ambiente teleworking propuesto, requisitos de la seguridad de comunicaciones, y la amenaza del acceso no autorizado al equipo o a la red?	CUMPLE PARCIALMENTE	2		solo la contadora puede trabajar remotamente, el programa que seutliza es teamviewer version14
12.	**ADQUISICIÓN, DESARROLLO y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	**ADQUISICIÓN, DESARROLLO y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**			1	
12.1.	**Requisitos de seguridad de los sistemas de información**	**Garantizar que la seguridad es parte integral de los sistemas de información**				
12.1.1	Análisis y especificación de los requisitos de seguridad	¿Se realiza un análisis de los requisitos de la seguridad como parte de la etapa del análisis de requisitos de cada proyecto del desarrollo?	NO CUMPLE	1		no se realiza el análisis de la seguridad
12.2.	**Procesamiento correcto de las aplicaciones**	**Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones**				
12.2.1	Validación de los datos de entrada	¿Los Datos que se ingresan en sistemas de aplicaciones se validan para asegurarse de que son correctos y apropiados?	CUMPLE PARCIALMENTE	2		al ingresar pide un usuario y contraseña
12.2.2	Control del procesamiento interno	¿Chequeos de validación se han incorporado en sistemas para detectar la corrupción causada por errores de	NO CUMPLE	1		no se realizan chequeos de validación

		proceso o por actos deliberados?			
12.2.3	Integridad del mensaje	¿La autentificación del mensaje se ha considerado para las aplicaciones que implican la transmisión de datos sensibles?	NO SABE	0	No implementado/ inlate
12.2.4	Validación de los datos de salida	¿Los datos de salida de los sistemas de aplicación se validan para asegurarse de que son correctos y apropiados?	NO SABE	0	No implementado/ inloste
12.3.	**Controles Criptográficos**	**Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos**			
12.3.1	Política sobre el uso de controles criptográficos	¿La gerencia ha desarrollado una política en el uso de controles criptográficos, incluyendo la gerencia de las llaves del cifrado, y se implementación eficaz?	NO SABE	0	No implementado/ inlate
12.3.2	Gestión de llaves	¿Es un sistema de administración implementado para soportar el uso en la organización de lleves publicas y llevas privadas?	NO SABE	0	No implementado/ ineste
12.4.	**Seguridad de los archivos del sistema**	**Garantizar la seguridad de los archivos del sistema**			
12.4.1	Control del software operativo	¿Se tiene un estricto control sobre la implementación de software en sistemas operacionales?	CUMPLE PARCIALMENTE	2	Cumple implementado/ insete
12.4.2	Protección de los datos de prueba del sistema	¿Se protegen y se controlan todos los datos de la prueba de los sistemas de aplicación?	CUMPLE PARCIALMENTE	2	Cumple implementado/ insete

12. 4.3	Control del acceso al código fuente de programas	¿Para reducir el potencial para la corrupción de los programas de computadora, el acceso a las bibliotecas fuente del programa es estrictamente controlado?	CUMPLE PARCIALMENTE		Cumple implementado/ inparate
12. 5.	**Seguridad en los procesos de desarrollo y soporte**	**Mantener la seguridad del software y de la información del sistema de aplicaciones**			
12. 5.1	Procedimientos de control de cambios	¿Se ha implementado un procedimiento formal de control de cambios?	CUMPLE PARCIALMENTE	2	Cumple implementado/ insete
12. 5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	¿Se revisan los sistemas de aplicaciones cuando ocurren cambios a nivel de los sistemas operativos?	CUMPLE PARCIALMENTE	2	Cumple implementado/ insete
12. 5.3	Restricciones en los cambios a los paquetes de software	¿Se desalienta la realización de modificaciones a los paquetes de software? ¿Se limitan a los cambios necesarios, y todos los cambios se controlan estrictamente?	NO SABE	0	No implementado/ insete
12. 5.4	Fuga de Información (Canales Encubiertos y Código Troyano)	¿Se consideran los siguientes aspectos para limitar el riesgo de fuga de información, por ejemplo, mediante el uso y explotación de los canales encubiertos?	NO SABE	0	
		a) exploración de los medios y comunicaciones de salida para determinar la información oculta;	NO CUMPLE	1	
		b) comportamiento de las comunicaciones y del sistema de modulación y	NO CUMPLE	1	No implementado/ insete

		enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento;			
		c) utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados (véase la norma ISO/IEC 15408);	NO CUMPLE	1	No implementado/ insete
		d) monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes;	NO CUMPLE	1	No implementado/ insete
		e) monitoreo del uso de los recursos en los sistemas de computador	NO CUMPLE	1	No implementado/ insete
12. 5.5	Desarrollo de software contratado externamente	¿Cuando desarrollo del software es por outsourcing, se definen los detalles para proteger, supervisar y monitorear el desarrollo?	NO CUMPLE	1	No implementado/ insete
12. 6.	**Gestion de las Vulnerabilidades**	**Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.**			
12. 6.1	Control de las vulnerabilidades técnicas	¿Se obtiene información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso? ¿Se evaluar la exposición de la organización a dichas vulnerabilidades y se toman las acciones apropiadas para tratar los riesgos	NO CUMPLE	1	se no se tiene en cuenta las vulnerabilidades en el sistema de información

		asociados?			
13.	**GESTIÓN DE INCIDENTES - MONITOREO**			0,6	
13.1.	**Reporte sobre los eventos y las debilidades de seguridad de la información**	**Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente**			
13.1.1	Reporte sobre los eventos de seguridad de la información	¿Existen procedimientos formales de reportes y respuesta a incidentes para identificar las acciones a ser tomadas frente a la recepción de un reporte de incidentes?	NO CUMPLE	1	no hay procedimientos para los reportes de incidendencias
13.1.2	Reporte sobre las debilidades en la seguridad	¿Son los usuarios requeridos observar y reportar todas las debilidades de seguridad observadas o sospechadas o amenazas a los sistemas o a los servicios?	NO CUMPLE	1	no hay reporte de las debilidades en la seguridad
13.2.	**Gestión de los incidentes y las mejoras en la seguridad de la información**	**Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.**			
13.2.1	Responsabilidades y procedimientos	¿Se ha establecido las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la	NO CUMPLE	1	no se han establecido responsabilidades y procedimientos de la gestion

		información?			
13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Existen implementados mecanismos para monitorear los tipos, los volúmenes, y los costos de incidentes y de malfuncionamientos?	NO SABE	0	
13.2.3	Recolección de evidencias	¿Existen definidos procedimientos para se debería recolectar, retener y presentar evidencia para cumplir las reglas de la evidencia establecidas en la jurisdicción pertinente?	NO SABE	0	
14.	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		1	
14.1.	**Aspectos de seguridad de la información en la Gestión de la Continuidad de Negocios**	**Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.**			
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	¿Se ha desarrollado y mantenido un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización?	NO CUMPLE	1	No implementado/ insete
14.1.2	Continuidad del negocio y evaluación de riesgos	¿Se han identificado los eventos que pueden ocasionar interrupciones en los	NO CUMPLE	1	No implementado/ insete

		procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información?				
14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	¿En el proceso del planeamiento de la continuidad del negocio ha incluido la identificación y el acuerdo de todas las responsabilidades y procedimientos de emergencia?	NO CUMPLE	1		No implementado/ insete
14.1.4	Estructura para la planificación de la continuidad del negocio	¿Se mantiene un único marco (framework) del plan de la continuidad del negocio para asegurarse de que todos los niveles del plan son consistentes?	NO CUMPLE	1		No implementado/ insete
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	¿Los planes de la continuidad del negocio se prueban regularmente para asegurarse de que son actuales y eficaces?	NO CUMPLE	1		No implementado/ insete
15.	**CUMPLIMIENTO**	**CUMPLIMIENTO**			1,2	
15.1.	**Cumplimiento de los requisitos legales**	**Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad**				
15.1.1	Identificación de la legislación aplicable	¿Todos los requisitos estatutarios, reguladores, y contractuales relevantes son específicamente definidos y se documentan para cada sistema de información?	CUMPLE PARCIALMENTE	2		

15.1.2	Derechos de propiedad intelectual (DPI)	¿Hay conformidad con restricciones legales en el uso de material con copyright asegurándose que solamente el software se desarrolló en la organización, o licenciado o proporcionado por el desarrollador a la organización, es utilizado?	CUMPLE PARCIALMENTE	2	el software contable es licenciadoManager 3.2
15.1.3	Protección de los registros de la organización	¿Los registros de la organización importantes se mantienen con seguridad para dar cumplimiento a requisitos estatutarios, así como para apoyar actividades económicas esenciales?	CUMPLE PARCIALMENTE	2	se puede evidenciar que unas aplicaciones no cumplen con la proteccion de los datos del negocio
15.1.4	Protección de los datos y privacidad de la información personal	¿Las aplicaciones que procesan datos personales dan cumplimiento a la legislación aplicable de la protección de los datos?	CUMPLE PARCIALMENTE	2	se puede evidenciar que unas aplicaciones no cumplen con la proteccion de los datos del negocio
15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	¿Las instalaciones de IT se utilizan solamente para los propósitos del negocio?	CUMPLE PARCIALMENTE	2	se puede evidenciar q las ITse usan para otros propositos fuera del negocio
15.1.6	Reglamentación de los controles criptográficos	¿El asesoramiento jurídico se ha buscado en la conformidad de la organización con leyes nacionales e internacionales sobre controles criptográficos?	NO SABE	0	
15.2.	**Cumplimiento de las Políticas y las normas de seguridad y cumplimiento técnico**	**Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización**			

15.2.1	Cumplimiento con las políticas y las normas de seguridad	¿Todas las áreas dentro de la organización son consideradas para revisiones con regularidad que asegure conformidad con políticas y estándares de la seguridad?	NO CUMPLE	1	no hay politicas y estandares de seguridad
15.2.2	Verificación del cumplimiento técnico	¿Las instalaciones de IT se comprueban regularmente para saber si hay conformidad con los estándares seguridad implementados?	NO CUMPLE	1	no hay estandares de seguridad establecidas
15.3.	**Consideraciones de la Auditoría de los sistemas de Información**	**Maximizar la eficacia de los procesos de auditoría de los sistemas de información y maximizar su interferencia**			
15.3.1	Controles de auditoría de los sistemas de información	¿Las auditorias y las actividades que implican chequeos en sistemas operacionales se planean y se arreglan cuidadosamente?	NO SABE	0	
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	¿El acceso a las herramientas de auditoria del sistema es controlado?	NO SABE	0	
		GRADO O NIVEL DE CUMPLIMIENTO NORMA ISO27001		**35 %**	

Fuente. Autores del proyecto

5. Conclusiones

Logramos desarrollar una serie de acciones que nos permitieron entender el estado actual del funcionamiento de la empresa, como es el manejo y manipulación de la información, aplicando una serie de herramientas a los empleados que nos permitió recolectar datos y obtener valores, para cuantificar los resultados. Se realizó un análisis a la gestión de los activos, el estado en que se encuentra, la ubicación y distribución, la identificación de la información logrando realizar la aplicación de una matriz de riesgos a la empresa.

Se alcanzó los objetivos propuestos, inicialmente se planteó diagnosticar el estado actual y si tenía conocimiento de que es un plan de gestión de la información, posterior a eso se utilizó la normativa ISO 27000 como modelo para la creación del plan, y luego la ejecución o diseño de este para ser evaluada e implementado por la empresa.

La empresa no cuenta con controles de seguridad definidos para evitar el acceso físico no autorizado; todas estas falencias son consecuencia de no planear ni implementar políticas de seguridad que orienten a la empresa para la aplicación de buenas prácticas en la gestión de la información. Se elaboró el Plan de Gestión de Seguridad de la Información como documento que establece los lineamientos para proteger los recursos de almacenamiento de información y la tecnología utilizada de la empresa.

Este proyecto nos deja una gran enseñanza como personas y profesionales, mostrándonos que las empresas y personas estamos expuesta constantemente a los peligros de ser afectado en

nuestra información, que debemos tener controles y seguimiento a las actividades para que estas no sean afectadas y no suframos de pérdidas irreparables de cualquier índole.

6. Recomendaciones

Como primera medida de recomendación se hace a la gerencia del motel Dubái para que gestione, apruebe e implemente el Plan de Gestión de Seguridad de la Información, este a su vez sea informado a todo el personal laboral de la empresa, con la intención de dar cumplimiento y efectividad de los controles señalados en el plan de seguridad y así garantizar la confidencialidad, integridad y disponibilidad de la información.

Tener en cuenta la propuesta de implementación planteada en este proyecto como guía para que la empresa se oriente en las estrategias y recursos financieros necesarios para la puesta en marcha del plan de gestión de seguridad de la información.

Se debe hacer por parte del comité de seguridad y empleados un control a las políticas y verificación de cumplimiento de las políticas de seguridad de la información expresadas en el plan de gestión, adicional corroborar su efectividad.

Se aconseja efectuar auditorías internas periódicas que permitan evaluar, mejorar los controles antes propuestos, siempre apoyándose de los instrumentos de recolección de información y análisis de datos planteados en la auditoría realizada por el equipo de trabajo del proyecto. Así disminuirá la afectación de perdida de información, protegiendo los procesos y actividades de la empresa.

Referencias

Angarita, L. L., Suarez, D. M., & Rodriguez, P. H. (2014). *Diseño del plan de gestión de seguridad de la información para controlar el acceso a las areas restringidas de la empresa ingepec ltda en la ciudad de ocaña.* OCAÑA.

Arévalo, A. J., Bayona, T. R., & Rico, B. D. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Revista Tecnura*.

Instituto colombiano de normas técnicas y certificación. . (2007). *Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.* . Bogotá: ICONTEC. NTC ISO/IEC 27002.

Muñoz, J. (2017). *Diseño de un plan estratégico para la seguridad* . Bogota: Universidad nacional abierta y a distancia.

Oliveros, C. D., & Martínez, G. (2017). *Efecto de las TIC sobre la gestión de las empresas hoteleras afiliadas a Cotelco de Bucaramanga (Santander, Colombia).* Bucaramanga : Revista EAN.

Pérez, U. M. (2008). *Características y problemas. Cuadernos de Investigación.* Tolima: La pyme.

Rodríguez, P. C. (2010). *Seguridad de la información: estrategia para fortalecer el gobierno corporativo.* Obtenido de https://www.redalyc.org/pdf/3600/360033192006.pdf

Ugas, M. L. (2002). *Seguridad en organizaciones con tecnologías de la tecnologias de informacion.* Telematique.

Apéndices

Apéndice A. Entrevista No 1 Administración y procesamiento de la información MOTEL DUBÁI.

JG Auditoria & consultoria	PERIODO: Marzo-Abril	EMPRESA: MOTEL DUBÁI
	FECHA: 4 al 8 de marzo 2019	AUDITOR: Gina Paola Claro Ropero Jesús Eduardo Espinel Blanco
	ENTREVISTA No 1	AREA AUDITADA: Centro de sistemas
PREGUNTAS		**RESPUESTAS**
¿Considera usted que el lugar donde se encuentra ubicado los equipos de procesamiento de datos es el adecuado para estar seguro de inundaciones, robo cualquier otra situación que pueda poner en peligro los equipos?		Considero que debe realizarse varias adecuaciones, para evitar el ingreso de personal no autorizado.
¿Conociendo que dentro de las empresas los empleados deben conocer sus funciones y saber realizar su labor, cuáles son sus obligaciones y responsabilidades como empleado?		Debo registrar los clientes e ingresar el horario de entrada y salida, verificar las ventas o consumo, ofrecer servicios extras y que la información de los clientes sea reservada.
¿Todas las empresas deben manejar un nivel de seguridad y privilegios para acceder a la información de la misma, usted tiene acceso al equipo principal, cámaras y contraseñas del sistema de información de la empresa?		Inicialmente todos los empleados teníamos acceso a las contraseñas y cámaras de la empresa, luego de la sugerencia del contador público se modificaron y solo el gerente y contador tienen acceso a esa información.
¿Se entiende que en todo lugar de trabajo o donde se maneja información esencial para el funcionamiento de las empresas se debería hacer copias con el fin de evitar pérdidas u otros eventos, en su caso usted cuenta con copias de los archivos e información en un lugar distinto al de la computadora principal (Backup)?		En mi cargo como recepcionista solo realizo los ingresos, salida de los clientes y las ventas, no realizo copias de seguridad.
¿Actualmente los programas o software deben contar con sus respectivas licencias y actualizaciones que garanticen un buen funcionamiento de los mismos, sabe usted si los programas que maneja para su trabajo cuentan con licencias?		No tengo conocimiento
¿En las empresas hoy se maneja gran cantidad y variedad de información la cual puede verse afectada por diferentes razones, sabe usted si existen o se cuenta con programas y procedimientos de detección de virus que garanticen la integridad de los datos?		No se tiene un anti virus, que yo tenga conocimiento

Apéndice B. Entrevista No 2

JG Auditoria & consultoria	PERIODO: Marzo-Abril	EMPRESA: MOTEL DUBÁI.
	FECHA: 4 al 8 de marzo 2019	AUDITOR: Jesús Eduardo Espinel Blanco
	ENTREVISTA No 2	AREA AUDITADA: Centro de sistemas
PREGUNTAS		**RESPUESTAS**
¿Considera usted que el lugar donde se encuentra ubicado los equipos de procesamiento de datos es el adecuado para estar seguro de inundaciones, robo cualquier otra situación que pueda poner en peligro los equipos?		Estoy consciente que dicho lugar debe realizarse unas mejoras, pero estamos en el proceso de culminación del hotel donde será trasladada el centro de cómputo y unas nuevas oficinas.
¿Conociendo que dentro de las empresas los empleados deben conocer sus funciones y saber realizar su labor, cuáles son sus obligaciones y responsabilidades como empleado?		Planificar, organizar y coordinar todo el funcionamiento del motel (incluyendo los servicios al cliente, la gestión del personal y la administración del motel). Dirigir, supervisar y formar al personal y a los aprendices. Contratar y destinar a los nuevos miembros del personal
¿Todas las empresas deben manejar un nivel de seguridad y privilegios para acceder a la información de la misma, usted tiene acceso al equipo principal, cámaras y contraseñas del sistema de información de la empresa?		Se realizaron cambios sugeridos por el contador público porque anteriormente todos los empleados tenían acceso a esa información, en el momento solo personal seleccionado tenemos acceso a contraseñas y cámaras.
¿Se entiende que en todo lugar de trabajo o donde se maneja información esencial para el funcionamiento de las empresas se debería hacer copias con el fin de evitar pérdidas u otros eventos, en su caso usted cuenta con copias de los archivos e información en un lugar distinto al de la computadora principal (backup)?		No se realizó copias de seguridad
¿Actualmente los programas o software deben contar con sus respectivas licencias y actualizaciones que garanticen un buen funcionamiento de los mismos, sabe usted si los programas que maneja para su trabajo cuentan con licencias?		Los programas y software con los que cuenta la empresa cuentan con sus respectivas licencias.
¿En las empresas hoy se maneja gran cantidad y variedad de información la cual puede verse afectada por diferentes razones, sabe usted si existen o se cuenta con programas y procedimientos de detección de virus que garanticen la integridad de los datos?		No se cuenta con anti virus, porque no había visto la necesidad de adquirirlos.

Apéndice C. Entrevista No 3

	PERIODO: Marzo-Abril	EMPRESA: MOTEL DUBÁI.
	FECHA: 4 al 8 de marzo 2019	AUDITOR: Gina Paola Claro Ropero
	ENTREVISTA No 3	AREA AUDITADA: Centro de sistemas
PREGUNTAS		RESPUESTAS
¿Considera usted que el lugar donde se encuentra ubicado los equipos de procesamiento de datos es el adecuado para estar seguro de inundaciones, robo cualquier otra situación que pueda poner en peligro los equipos?		Considero que debe realizarse varias adecuaciones, ya que no hay paso restringido para personal no autorizado y esto puede permitir robos y se ponga en peligro la información que allí se guarda.
¿Conociendo que dentro de las empresas los empleados deben conocer sus funciones y saber realizar su labor, cuáles son sus obligaciones y responsabilidades como empleado?		Procesar, codificar y contabilizar los diferentes comprobantes por concepto de activos, pasivos, ingresos y egresos, dan lugar a los balances y demás reportes financieros. Llevar mensualmente los libros generales de Compras y Ventas, mediante el registro de facturas emitidas y recibidas a fin de realizar la declaración de IVA Mantener actualizado el software contable de la empresa y demás actividades que requiera mi cargo.
¿Todas las empresas deben manejar un nivel de seguridad y privilegios para acceder a la información de la misma, usted tiene acceso al equipo principal, cámaras y contraseñas del sistema de información de la empresa?		Gracias a que el gerente recibió mi sugerencia de cambiar las claves de las cámaras y por el momento solo el gerente y el contador tenemos acceso a esa información y para el acceso al software contable solo yo tengo acceso.
¿Se entiende que en todo lugar de trabajo o donde se maneja información esencial para el funcionamiento de las empresas se debería hacer copias con el fin de evitar pérdidas u otros eventos, en su caso usted cuenta con copias de los archivos e información en un lugar distinto al de la computadora principal (backup)?		Si, realizo copias de seguridad de la información del software contable semanalmente y las subo al Dropbox. Y la información del personal de la empresa hay una copia guarda en un lugar diferente de la empresa.
¿Actualmente los programas o software deben contar con sus respectivas licencias y actualizaciones que garanticen un buen funcionamiento de los mismos, sabe usted si los programas que maneja para su trabajo cuentan con licencias?		Si cuentan con las licencias respectivas
¿En las empresas hoy se maneja gran cantidad y variedad de información la cual puede verse afectada por diferentes razones, sabe usted si existen o se cuenta con programas y procedimientos de detección de virus que garanticen la integridad de los datos?		Por el momento no cuentan con anti virus

Apéndice D. ENCUESTA, Encuesta numero 1

Objetivo: Conocer como es la administración, aplicación y el uso de dispositivos hardware de almacenamiento y procesamiento de la información MOTEL DUBÁI

Encuesta No 1.

	PERIODO: Marzo-Abril	EMPRESA: MOTEL DUBÁI.		
	FECHA: 4 al 8 de marzo 2019	AUDITOR: Gina Paola Claro Ropero Jesús Eduardo Espinel Blanco		
	ENCUESTA No 1	AREA AUDITADA:		
CONCEPTO		**SI**	**NO**	**Observación**
¿Realiza algún tipo de mantenimiento preventivo o correctivo a los equipos de sistemas?			X	
¿Cuentan con manuales para cada programa que se maneja en la empresa?			X	
¿Conoce usted del contenido de estos manuales o tuvo la oportunidad de revisarlos?			X	
¿Se tienen identificados los archivos con información confidencial y se cuenta conclaves de acceso?			X	
¿Existe un control preciso de las copias de estos archivos?			X	
¿Se restringe el acceso a los lugares para guardar los dispositivos de almacenamiento, solo al personal autorizado le es permitido acceder?			X	
¿Le es permitido el acceso a los programas, archivos y datos a los empleados que no pertenezcan al área de sistemas?			X	
¿El lugar donde se ubica el servidor o computador principal se encuentra a salvo?		X		

Apéndice E. Encuesta No 2

Auditoria & consultoria	PERIODO: Marzo-Abril	EMPRESA: MOTEL DUBÁI.
	FECHA: 4 al 8 de marzo 2019	AUDITOR: Gina Paola Claro Ropero Jesús Eduardo Espinel Blanco
	ENCUESTA No 2	AREA AUDITADA:

CONCEPTO	**SI**	**NO**	**Observación**
¿Realiza algún tipo de mantenimiento preventivo o correctivo a los equipos de sistemas?		X	
¿Cuentan con manuales para cada programa que se maneja en la empresa?		X	Los manuales se extraviaron
¿Conoce usted del contenido de estos manuales o tuvo la oportunidad de revisarlos?	X		
¿Se tienen identificados los archivos con información confidencial y se cuenta conclaves de acceso?	X		
¿Existe un control preciso de las copias de estos archivos?	X		
¿Se restringe el acceso a los lugares para guardar los dispositivos de almacenamiento, solo al personal autorizado le es permitido acceder?		X	
¿Le es permitido el acceso a los programas, archivos y datos a los empleados que no pertenezcan al área de sistemas?		X	Se restringió el acceso y ahora solo personal autorizado puede acceder
¿El lugar donde se ubica el servidor o computador principal se encuentra a salvo?		x	Está entrando personal no autorizado

Apéndice F. Encuesta No 3

Auditoria & consultoria	PERIODO: Marzo-Abril	EMPRESA: MOTEL DUBÁI.
	FECHA: 4 al 8 de marzo 2019	AUDITOR: Gina Paola Claro Ropero Jesús Eduardo Espinel Blanco
	ENCUESTA No 3	AREA AUDITADA:

CONCEPTO	SI	NO	Observación
¿Realiza algún tipo de mantenimiento preventivo o correctivo a los equipos de sistemas?		X	
¿Cuentan con manuales para cada programa que se maneja en la empresa?		X	
¿Conoce usted del contenido de estos manuales o tuvo la oportunidad de revisarlos?		X	
¿Se tienen identificados los archivos con información confidencial y se cuenta conclaves de acceso?	X		
¿Existe un control preciso de las copias de estos archivos?	X		
¿Se restringe el acceso a los lugares para guardar los dispositivos de almacenamiento, solo al personal autorizado le es permitido acceder?		X	
¿Le es permitido el acceso a los programas, archivos y datos a los empleados que no pertenezcan al área de sistemas?		X	
¿El lugar donde se ubica el servidor o computador principal se encuentra a salvo?		X	Considero que debe realizarse unas modificaciones

Apéndice G. Lista De Chequeo: Chek List No 1

Objetivo: Con el propósito de tener un mejoramiento continuo del procesamiento de la información y datos del motel Dubai, de Auditoría Interna desea conocer su opinión sobre esta actividad.

A continuación, encontrará una serie de preguntas cuya respuesta se debe señalar con una (X), con observaciones dadas el caso que sea necesario realizar.

	EMPRESA: MOTEL DUBÁI	AREA AUDITADA:		
	PERIODO: Marzo-Abril	Fecha: 4 al 8 de marzo		
	AUDITOR: Gina Paola Claro Jesús Eduardo Espinel			
CONCEPTO		SI	NO	OBSERVACION
¿Se encuentran separadas las funciones dentro del área?		X		
¿Están establecidas las líneas de autoridad y responsabilidad dentro del área?		X		
¿Usted como empleado tiene acceso al sistema de información de la empresa?			X	
¿Muestra la gerencia interés por la integridad y los valores éticos de los empleados?		X		
¿Los funcionarios responden adecuadamente a la integridad y valores éticos propiciados por la empresa?		X		
¿Existe una cultura de rendición de cuentas con características de integridad, confiabilidad y oportunidad?		X		
¿Existen procedimientos para inducir a todos los funcionarios sobre el comportamiento ético pretendido, independientemente de su jerarquía?			X	
¿Los funcionarios tienen conocimiento de los reglamentos específicos y el manual de procesos?			X	

Apéndice H. Lista De Chequeo: Chek List No 2

	EMPRESA: MOTEL DUBÁI PERIODO: Marzo-Abril AUDITOR:	AREA AUDITADA: Fecha: 4 al 8 de marzo		
CONCEPTO		SI	NO	OBSERVACION
¿Los empleados que utilizan el sistema de información están conformes con respecto a la confiabilidad y oportunidad de los informes que emiten dichos sistemas?		X		
¿existen usuarios o perfiles para cada empelado y así acceder al sistema de información de forma confiable?			X	El software contable solo puede acceder el contador y las cámaras solo el gerente y contador tienen acceso.
¿Conocen los usuarios el nivel de confiabilidad de la información financiera y operativa que utilizan?			X	
¿Existen resguardos apropiados de la información contra alteraciones, pérdidas y falta de confidencialidad?		X		
¿Se protegen adecuadamente con copias de seguridad los programas de aplicación y los archivos informáticos generados durante el procesamiento diario de las operaciones?		X		
¿Los componentes de la red tienen todo el hardware necesario un correcto funcionamiento?			X	
¿Los softwares utilizados tienen todas sus características de licencias y actualizaciones para un correcto funcionamiento?		X		

Apéndice I. Prueba No 1

MOTEL DUBAI	
Prueba	Ingreso a los equipos de la empresa para validar credenciales de acceso
Objetivo	Determinar nivel de privilegios que manejan los usuarios
Técnica	Pruebas de cumplimiento de los controles generales de sistemas de información.
Tipo de prueba	S_X C_ DF_
Procedimiento	1. solicitud de ingreso al servidor principal 2. validar si existe controles de seguridad para el ingreso al sistema
Recursos	
RESULTADOS DE LA PRUEBA	
Hallazgos	Se evidencia que no cuenta con perfiles y calves de acceso para los empleados, se evidencia que todos tiene acceso a la información sin ningún tipo de restricción
Causa	No existen perfiles de usuario creados en los equipos
Situación de riesgo que genera	la probabilidad de ocurrencia está clasificada en alto, en cuanto al impacto pedirá ser prepucial para la empresa
Recomendaciones de auditoria	El Encargado de la administración debe asignar perfiles y contraseñas para los usuarios que verdaderamente usen el equipo.
Fecha	08 de marzo 2019
Elaborado por:	Gina Paola Claro Ropero
Revisado por:	Jesús Eduardo Espinel Blanco

Apéndice J. Prueba N0 2

JG Auditoria & consultoria	***MOTEL DUBAI***
Prueba	Elaboración de copias de seguridad
Objetivo	Seguridad de la información
Técnica	Pruebas de cumplimiento de los controles generales de sistemas de información y seguridad
Tipo de prueba	S_ C_ DF_X
Procedimiento	1. solicitarles a varios empleados como hacen el proceso de guardado de la información 2. presenten la evidencia física y lógica del guardado de la información
Recursos	
RESULTADOS DE LA PRUEBA	
Hallazgos	Se logro evidenciar que no realizan copias de seguridad, solo el área de contabilidad realiza dicho backup y lo guarda en Dropbox
Causa	No cuentan con políticas de elaboración de backup
Situación de riesgo que genera	la probabilidad de ocurrencia está clasificada en alto, en cuanto al impacto que puede presentar porque se puede perder la base de datos y no cuentan con un respaldo
Recomendaciones de auditoria	El Encargado de la administración debe asignar políticas de elaboración de backup y estructurar un manual de procedimientos de copias de seguridad
Fecha	08 de marzo 2019
Elaborado por:	Gina Paola Claro Ropero
Revisado por:	Jesús Eduardo Espinel Blanco

Apéndice K. Prueba N0 3

	MOTEL DUBAI
Prueba	Red de vigilancia
Objetivo	Seguridad de la información
Técnica	Pruebas de cumplimiento de los controles generales de sistemas de información y seguridad
Tipo de prueba	S_ C_ DF_X
Procedimiento	1. solicitarles a los empleados que accedieran a las cámaras
Recursos	
RESULTADOS DE LA PRUEBA	
Hallazgos	Los empleados conocen los el usuario y contraseña al software de las cámaras
Causa	
Situación de riesgo que genera	la probabilidad de ocurrencia está clasificada es alto, ya que puede presentarse fuga de información y se puede presentar inconvenientes por el mal uso de los empleados
Recomendaciones de auditoria	El Encargado de la administración debe asignar perfile y contraseña, que solo lo tenga una personal seleccionado y calificado e implantar un software con licencia
Fecha	11 de marzo 2019
Elaborado por:	Jesús Eduardo espinel blanco
Revisado por:	Gina Paola claro ropero

Apéndice L. Prueba N0 4

	MOTEL DUBAI
prueba	Manuales de procedimientos
Objetivo	Seguridad de la información
Técnica	Pruebas de cumplimiento de los controles generales de sistemas de información y seguridad
Tipo de prueba	S_ C_X DF_
Procedimiento	1. Solicitar los manuales de procedimientos y practicas de la información del software que maneja la empresa
Recursos	
RESULTADOS DE LA PRUEBA	
Hallazgos	No cuentan con manuales de procedimientos del uso de los sistemas de información
Causa	Desconocimiento
Situación de riesgo que genera	la probabilidad de ocurrencia está clasificada es media, ya que puede no tienen definido los parámetros y pueden cometer errores
Recomendaciones de auditoria	El Encargado de la administración debe implementar los procedimientos del manejó de la información
Fecha	11 de marzo 2019
Elaborado por:	Jesús Eduardo espinel blanco
Revisado por:	Gina Paola claro ropero

Apéndice M. Prueba N0 5

	**MOTEL DUBAI**
prueba	Seguridad contra robo de equipos informáticos
Objetivo	Seguridad de la información
Técnica	Pruebas de cumplimiento de los controles generales de sistemas de información y seguridad
Tipo de prueba	S_ X C_ DF_
Procedimiento	1. verificar si los equipos de la empresa cuentan con sistemas de protección contra robos
Recursos	
RESULTADOS DE LA PRUEBA	
Hallazgos	Se logra evidenciar que no tienen implementado ningún método de seguridad ante robos
Causa	
Situación de riesgo que genera	la probabilidad de ocurrencia está clasificada es alta, ya que puede ocurrir un robo, puede perderse la información de la empresa y caer en manos que puedan perjudicar a la organización
Recomendaciones de auditoria	El Encargado de la administración debe implementar métodos correctivos
Fecha	12 de marzo 2019
Elaborado por:	Gina Paola claro ropero
Revisado por:	Jesús Eduardo espinel blanco

Apéndice N. Introducción del informe de auditoría de sistemas

El presente informe de auditoría, es el resultado de la solicitud realizada por a la gerencia de le empresa para el área de centro de sistemas, con la colaboración de la entidad auditada, se estableció la necesidad de evaluar la existencia de riesgos potenciales para la protección y respaldo de los archivos de información, así como la evaluación de los sistemas, equipos, instalaciones y componentes.

Como auditores externos de la administración y procesamiento de la información MOTEL DUBAI, efectuamos la auditoría correspondiente del 04 de marzo al 12 abril de 2019, nuestra responsabilidad está dada por lo siguiente

Objetivo. Evaluar la existencia de registros de información del sistema, acorde con su funcionamiento y copias de resguardo de sus archivos, así como la seguridad de su software y hardware.

Alcance. La auditoría se realizará sobre los sistemas informáticos, sobre el hardware de las computadoras que estén conectados a la red interna de la empresa.

Apéndice O. Presentación del dictamen

AUDITORIA Y CONSULTORÍA DE SISTEMAS INFORMATICOS
Expertos en Integridad, calidad y confianza

Ocaña N. de S. 15 de abril 2019

Señor:
(POR SEGURIDAD)
Gerente Propietario

En relación a la solicitud realizada por usted, me permito enviarle el dictamen de la auditoría practicada al centro de sistemas, para los procesos de administración y seguridad de la información, misma que se llevó a cabo del 04 de marzo al 12 abril de 2019

Para los resultados obtenidos durante la evaluación, me permito informarle a usted las siguientes observaciones:

Situaciones presentes:

Se evidencia que el Servidor 1 (principal), tiene instalado el Software de facturación (Manager V3.2), este equipo es usado también para otro tipo de actividades, a su vez diferentes usuarios realizan acciones que pueden colocar en riesgos la integridad de la información contable y financiera.

El Servidor 1, no cuenta con antivirus que evite ser afectado por amenazas internas o externas que podrían dañar la integridad de la información.

La red de cámaras de vigilancia, no cuenta con perfiles de usuario para categorizar la jerarquía de manejo de las mismas, y lograr evitar la intromisión al software de vigilancia e impedir alteraciones en los registros de seguridad.

El software CMS H264 para la administración de cámaras es un software gratuito, se aclara que esta versión no es robusta y estable puede haber problemas con él y no cuenta con soporte técnico.

No se realizan copias de seguridad de toda la información, solo la contadora realiza copias de seguridad de la información contable.

No se cuenta con manuales de procedimientos y prácticas relacionados con el uso adecuado de la información y del software que se maneja en la empresa, lo cual puede provocar que los colaboradores de la entidad al no tener una guía no puedan desempeñar adecuadamente sus funciones y pérdida de información y de recursos como por ejemplo el tiempo.

No se cuenta con un sistema de seguridad de prevención por robo, para las computadoras

personales, con lo cual la información es susceptible de caer en manos que puedan perjudicar a la organización.

Estos hallazgos se presentan en las operaciones que realizan los empleados, al momento de cambios de turno, cada empleado no tiene un usuario específico creado para identificar y administrar de modo seguro sus funciones.

Existe el riesgo de que personal ajeno a la empresa acceda al equipo principal ya que este se ubica en un lugar que no brinda seguridad física necesaria que evite esto, No existen políticas establecida para la confidencialidad de los datos de la empresa.

De acuerdo con las pruebas realizadas a los procesos de administración y seguridad de la información, y según los criterios de evaluación para las redes computacionales y sistemas de información, me permito dictar el resultado de la práctica de auditoria de sistemas y hacer las recomendaciones necesarias para corregir los hallazgos

IS Esp. Jesús Eduardo Espinel Blanco.
Auditor Líder
Celular: xxxxxxxxxxxxxxxxx

Apéndice P. Formato de situaciones encontradas

Auditoria & consultoria	***EMPRESA:*** *MOTEL DUBAI*	***HOJA*** *No 01*
	AREA AUDITADA: *Centre de sistemas*	***FECHA: DD / MM / AA*** *20-03-2019*

SITUACIONES ENCONTRADAS

REF	Situación	Causas	Solución	Fecha de solución	Responsable
AE-01	Ninguno de los computadores cuenta con password de usuario individual	Por el tamaño de la Empresa y la confianza que se le tiene al personal no se ha considerado necesario implementar un sistema de contraseñas.	Que la administración juntamente con el encargado de la programación elabore un sistema con la finalidad de crear cuentas de usuarios individuales para los colaboradores de la empresa.	15-03-2019	Personal de centro de sistemas
AE-02	En la empresa no se cuenta con la política de elaboración de Back-ups.	Debido a la falta de la elaboración de una política de resguardo de la información.	La administración debe estructurar un manual de políticas y procedimientos para la elaboración de Back-Ups.	20-03-2019	Personal de centro de sistemas Personal de cada área
AE-03	En el área auditada no se cuenta con un lugar específico para almacenar componentes magnéticos para las copias de seguridad	Debido a la falta de políticas de Backup y al volumen de información que se tendría para guardar no se cuenta con el espacio físico, pero si se tiene previsto.	Que al momento de necesitar almacenar la información la administración tome en cuenta las condiciones y el espacio para el almacenamiento de la misma.	18-03-2019	gerencia

	AE-04	No se cuenta con manuales de procedimientos y practicas relacionados con el uso adecuado de la información y del software que se maneja en la empresa.	Por tener un sistema de cómputo nuevo y la reciente capacitación del personal en relación al nuevo sistema aún no se ha previsto una manual sobre el uso del software y resguardo de la información.	Que la administración ejecute un plan para elaborar manuales de políticas y procedimientos en cuanto al uso de los sistemas y el resguardo de la información	30-03-2019	Área administrativa	
	AE-05	Se observo que las computadoras personales no cuentan con un sistema de seguridad contra robo.	Debido a la confianza que se tiene con el personal y que el acceso solo es permitido al mismo no se ha implementado.	Colocar a las computadoras candados de seguridad.	15-03-2019	Gerencia	
	AE-06	La red de cámaras de vigilancia, no cuenta con perfiles de usuario y todos los empleados tienen acceso a la información.	Los empleados conocen el usuario y contraseña principal del software de las cámaras	Adquirir un software con licencia que le permita crear usuarios con el fin de administrar las cámaras con nivel de privilegios	17-03-2019	Gerencia	

Elaboró (nombre y firma) GINA PAOLA CLARO ROPERO	Aprobó (nombre y firma) JESUS EDURDO ESPINEL BLANCO

Formato de situaciones relevantes

Auditoria & consultoria	***EMPRESA:*** *MOTEL DUBAI*	***HOJA*** *No 01*
	AREA AUDITADA: *Centro de sistemas*	***FECHA: DD / MM / AA*** *25-03-2019*

SITUACIONES RELEVANTES

REF	Situaciones	Causas	Solución
AE-02	En la empresa no se cuenta con la política de elaboración de Backup	Debido a la falta de la elaboración de una política de resguardo de la información.	La administración debe estructurar un manual de políticas y procedimientos para la elaboración de Backup
AE-03	En el área auditada no se cuenta con un lugar específico para almacenar componentes magnéticos para las copias de seguridad	Debido a la falta de políticas de Backups y al volumen de información que se tendría para guardar no se cuenta con el espacio físico, pero si se tiene previsto.	Que al momento de necesitar almacenar la información la administración tome en cuenta las condiciones y el espacio para el almacenamiento de la misma.
AE-04	No se cuenta con manuales de procedimientos y practicas relacionados con el uso adecuado de la información y del software que se maneja en la empresa.	Por tener un sistema de cómputo nuevo y la reciente capacitación del personal en relación al nuevo sistema aún no se ha previsto una manual sobre el uso del software y resguardo de la información.	Que la administración ejecute un plan para elaborar manuales de políticas y procedimientos en cuanto al uso de los sistemas y el resguardo de la información
AE-06	La red de cámaras de vigilancia, no cuenta con perfiles de usuario y todos los empleados tienen acceso a la información.	Los empleados conocen el usuario y contraseña principal del software de las cámaras	Adquirir un software con licencia que le permita crear usuarios con el fin de administrar las cámaras con nivel de privilegios

Elaboró (nombre y firma) GINA PAOLA CLARO ROPERO	Aprobó (nombre y firma) GINA PAOLA CLARO ROPERO

Apéndice Q. Guía de auditoria

Auditoria & consultoria	***EMPRESA:*** *MOTEL EL DUBAI*	***HOJA*** *No 01*
	AREA AUDITADA: *CENTRO DE SISTEMAS*	
	RESPONSABLE: Jesús Eduardo Espinel Blanco	
	PERIODO: 04 de marzo al 12 de abril 2019	***FECHA: DD / MM / AA*** 18 / 03 / 2019

Guía de Auditoria

REF	Actividad o función a evaluar	Procedimiento de auditoria	Herramientas utilizadas	Observación
EV01	Evaluar la seguridad en el acceso de usuarios, validar de sus perfiles	Se solicita acceso e ingreso a los equipos para ver la información, manipular datos, bases de datos, instrucciones y programas, hasta donde lo permite los sistemas. Ingresar al administrador y cambiar privilegios, atributos y contraseñas	Observación Pruebas Prueba en la seguridad del sistema	El sistema debe validar el ingreso, no permitir accesos no autorizados Documentar los accesos o y cambios que se realicen al sistema
EV02	Revisar los procedimientos de copias de seguridad o backup	Requerir el procedimiento para almacenar la información, las condiciones y el espacio para el almacenamiento de la misma	Observación Pruebas Listas de chequeo entrevistas	Debe existir un procedimiento para el guardado de toda información Deben existir protocolos establecidos para evitar pérdidas de datos
EV03	Evaluar el procedimiento para la administración de las cámaras de seguridad de la información	Verificar como es el manejo de este sistema de vigilancia	Entrevistas Pruebas Listas de chequeo	Documentar los accesos al sistema de vigilancia, realizar las copias y guardado de información.

Apéndice R. Plan de seguridad de la información

PLAN DE SEGURIDAD DE LA INFORMACIÓN

Elaborado	Revisado	Aprobado
Jesús Eduardo Espinel Blanco Ing. De Sistemas Gina Paola Claro Ropero Contador Publico	Gerente motel Dubai	Gerente propietario motel Dubai

INTRODUCCIÓN

La información es el activo más importante hoy en día para las empresas como se da a conocer, es por ende que las Tecnologías de Información y Comunicación (TIC) como se les conoce en la actualidad, por si solas no garantizan la seguridad y deben apoyarse en estrategias que permitan y garanticen su idoneidad generando una mayor conciencia y a su vez está cambiando ese paradigma donde la seguridad, confiabilidad, disponibilidad de la información juegan un papel fundamental para protección de los activos de las empresas, permitiéndoles obtener buenos resultados salvaguardando mediante estrategias y lineamientos que son reconocidos mundialmente de posibles amenazas internas y externas que se enfrentan las organizaciones.

Es necesaria la implementación de un Plan de seguridad de la información que formen parte de la cultura organizacional, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

Como consecuencia de lo expuesto, el motel Dubai se diseñó la meta de proponer e implementar el plan de seguridad de la información, basándose en las características de la norma ISO 27001

Así mismo, con el propósito de que dicha implementación pueda realizarse en forma ordenada y gradual, la entidad ha encomendado a su Comité de Gestión de seguridad de la información, cuya tarea es coordinar y supervisar la ejecución de actividades propias de estas políticas.

PLANTEAMIENTO DE LOS OBJETIVOS DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO GENERAL

Proponer el plan de gestión de seguridad de la información para el Motel Dubai

OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual de la seguridad de la información de la empresa.

- Identificar los componentes que integraran el plan de gestión de seguridad de información de la empresa de acuerdo a las Normas ISO/IEC 27001:2013.
- Establecer el plan de gestión de seguridad de la información mediante un procedimiento que brinde el control necesario a las áreas principales de la empresa.

JUSTIFICACIÓN

Las empresas que logran generar una estructura organizada permiten garantizar que sus procesos y/o servicios se elaboren de forma eficiente y de forma controlada que les permite seguir generando productividad; El establecer un plan de seguridad de la información, aplicarlos y hacerles seguimientos producen resultados beneficiosos para la empresa.

Aplicar este plan cimienta la responsabilidad de resguardar los activos y toda la información generada en los procesos de la empresa, de la misma forma es la evidencia de una administración y organización empresarial bien desempeñada, ya que gran porcentaje de las empresas afirman esto.

La seguridad información y el cumplimiento de sus objetivos de negocio son la principal meta de la organización, a pesar de esto no definen claramente las infraestructuras de seguridad que hoy en día existen y manejan, teniendo en cuenta que estas necesitan de un tiempo de reacción, debido que los ataques a la seguridad se efectúan con mayor porcentaje que cada día crece en sus modalidades.

REQUISITOS GENERALES

La empresa motel Dubai comprometida con el mejoramiento de los procesos de protección de la información y demás activos, avanza en el diseño del plan de Seguridad de la información, cumplimiento a las normas que se sirven de apoyo para la seguridad de la información ISO 27001:2013.

Para formular el plan de seguridad se adelantan las siguientes etapas; primera medida realizar el diagnóstico usando las herramientas de a la norma para la evaluación, alineación de los objetivos, guia de seguridad de la información, para terminar en la definición del plan de seguridad de la información donde se analiza el estado actual y se construye el plan de seguridad de la información.

Todo esto con el fin de plantear la propuesta y salvaguardar la información de la empresa

ALCANCES Y LIMITES DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

ALCANCES

- Tener claridad de la situación actual de la empresa y el tipo de seguridad que se brinda a los activos de información.
- Establecer un plan de seguridad de la información alineado con los objetivos estratégicos de la empresa.

- Establecer los controles que se aplicarán a los procesos de forma adecuada.
- Crear las políticas convenientes para proteger la información de la información, resaltadas en la prevención y disminución del impacto de los incidentes de seguridad.
- Garantizar la seguridad, continuidad de los activos de información que soportan los procesos y actividades de la empresa.
- Incentivar el talento generando huella y participación en el personal que labora, fomentando el uso y apropiación de las nuevas tecnologías para mejorar la atención a los usuarios.
- Mantener la seguridad de la información de sus clientes, proveedores y activos como prioritaria.

LIMITES

Teniendo en cuenta que hay información de la empresa la cual se debe proteger algunos datos no serán tenidos en cuenta en el siguiente plan de seguridad,

El cumplimiento de algunos de los objetivos del plan de seguridad de la información tiene costos de inversión que estarán sujetos al rubro presupuestal para financiar.
Falta de participación y compromiso del personal que labora en la entidad.

MARCO JURIDICO

La empresa por medio de su plan de Seguridad de la Información con el ánimo de mejorar la estrategia corporativa, dará cumplimiento al primero de los requisitos y lineamientos, que tienen como objetivo, gestionar adecuadamente la seguridad de la información, la organización e identificación de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos.

Dichos requisitos y lineamientos serán aplicados a todos los procesos de la empresa deberán ser conocidos y cumplidos por todo el personal incluyendo empleados y proveedores, que tengan acceso a los sistemas de información e instalaciones físicas de la empresa.

El plan de Gestión de Seguridad de la Información, se encuentra basado en el marco de lo establecido, en la norma internacional NTC-ISO-IEC 27001:2013 y las buenas prácticas contenidas en el componente Seguridad de la información de la estrategia, apoyándose en la NTC-ISO-IEC 27002:2013 para los controles.

DIRECCIONAMIENTO ESTRATÉGICO DE MOTEL DUBAI.

El Motel Dubái nace a partir de un estudio de mercadeo que les permitió identificar algunas de los factores más demandantes en las personas, la empresa busca cubrir las necesidades del ser humano para comodidad, seguridad, descanso y otros servicios que aprueben disfrutar momentos agradables en el ambiente de hospedaje.

Es así como en el año 2013 con la idea original nace el primer motel temático de la ciudad es un lugar perfecto para todos los habitantes de la ciudad Ocaña y sus alrededores que quieran vivir

momentos inolvidables y placenteros, con absoluta privacidad y fácil acceso. Ofrecemos 8 suites temáticas y 31 sencillas, todas inspiradas en culturas, países, personajes y situaciones de la vida cotidiana, convirtiéndonos en un referente turístico para todos aquellos que visitan nuestra hermosa ciudad.

Confortables y con un diseño vanguardista perfecto para disfrutar los mejores momentos de la vida, con una diversidad de habitaciones que se adaptan al presupuesto de todos nuestros clientes. en la actualidad funciona con una nómina de catorce (14) empleados;

La oferta del Motel Dubai es la siguiente:

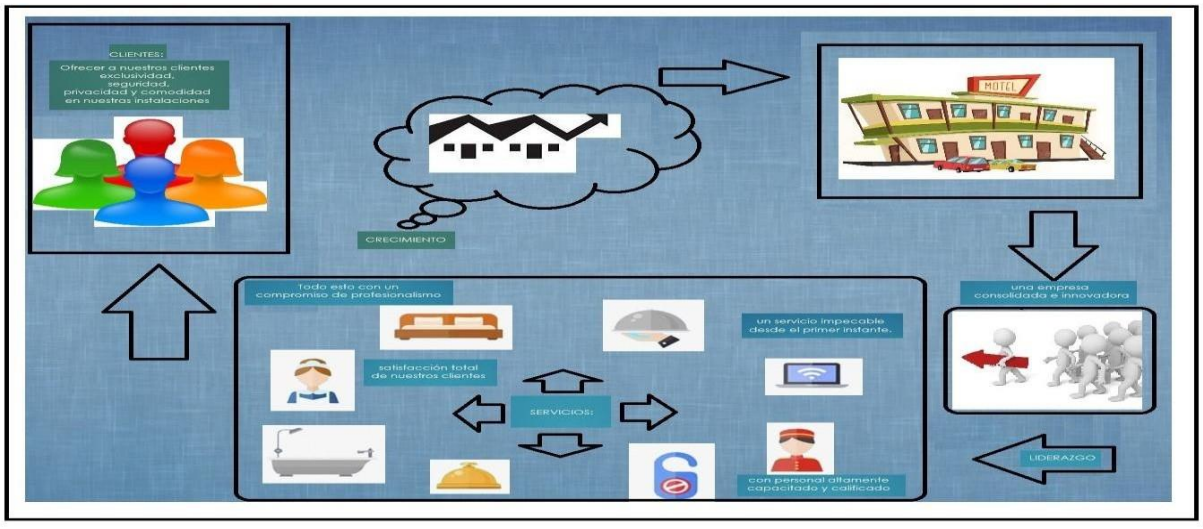
Precio asequible.
Confort Limpieza y pulcritud.
Rapidez del servicio
Disponibilidad 24 horas
Privacidad absoluta
Variedad de productos y servicios

Modelo de Objetivos. La empresa motel Dubai este articulado con el objetivo principal con la misión y visión de la empresa. (Figura 1.)

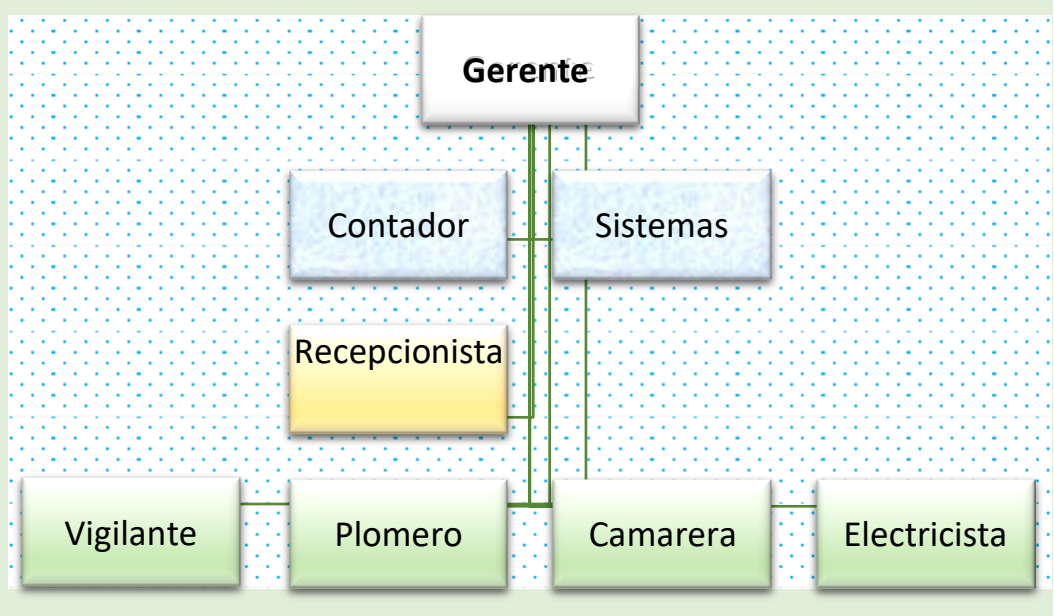
Misión. Ofrecer a nuestros clientes una experiencia de armonía, exclusividad, seguridad, privacidad y comodidad en nuestras instalaciones, con un servicio impecable desde el primer instante. Todo esto con un compromiso de profesionalismo, con personal altamente capacitado y calificado; promoviendo al desarrollo integral de los colaboradores internos y logrando la satisfacción total de nuestros clientes.

Visión. Mantener el liderazgo en la línea motelera, siendo una empresa consolidada e innovadora que responda a las más estrictas exigencias, buscando exceder las necesidades y expectativas de nuestros clientes.

OBJETIVOS DE LA EMPRESA MOTEL DUBAI

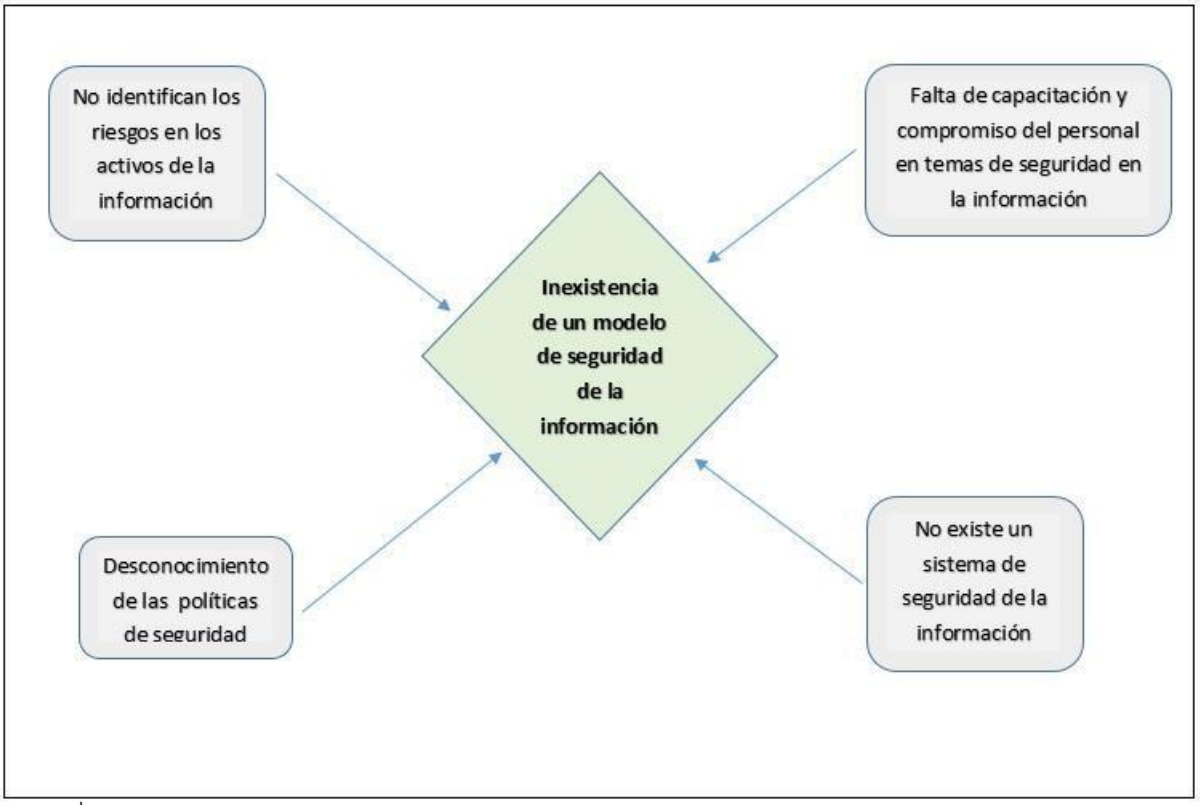


Estructura Organizacional Estructura Orgánica Motel Dubai



IDENTIFICACION DE AMENAZAS Y CAUSAS DEL PROBLEMA ACTUAL

Causas de vulnerabilidades en la seguridad de la Información de la empresa



GESTION DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

Realizar la gestión de los riesgos de seguridad de la información evitará pérdidas y brindará protección de la información, permitiendo conocer las debilidades que afectan durante todos los servicios ofrecidos por la empresa.

Es muy importante para la empresa contar con un plan de gestión de seguridad de la información que garantice la continuidad del negocio. Lo que lleva a la necesidad de desarrollar el diagnóstico de seguridad de la información y creación del plan de seguridad de la información que resguarde las áreas vitales de la empresa.

Antes de iniciar con este plan de gestión se ha revisado el documento con el diagnóstico del sistema actual de la empresa, donde se conoce la situación actual de la organización y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

ROLES Y FUNCIONES DEL PERSONAL A CARGO DE LA SEGURIDAD

Documento del plan de gestión de seguridad de la información Motel Dubai tendrá como objetivo del presente plan de gestión de seguridad de la información es crear los lineamientos necesarios que garanticen la protección de los activos y recursos de almacenamiento de información de la empresa motel Dubai, resguardando la seguridad en las TIC utilizadas, las cuales se enfrentan a unas amenazas muy serias ya sean de tipo internas o externas, buscando de manera segura los criterios de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información de la empresa.

El presente instrumento se establece en cumplimiento de las normas legales vigentes aplicadas a este tipo de activos, con el propósito de brindar y administrar apropiadamente la seguridad de la información, para el entorno físico y tecnológico de la empresa Motel Dubai se debe conocer y cumplir por parte de todo el personal que labora en la empresa. El establecimiento de la etapa de implementación es compromiso de la gerencia y personal de la empresa.

La etapa de implementación del plan de seguridad de la información, así como las fases de revisión y actualización del plan, es compromiso o responsabilidad de la gerencia la cual debe apoyarse siempre en el comité de seguridad de la información de la empresa, para dicho comité se deberá crear y establecer en base a las políticas y acuerdos generados en vía de la seguridad de la información de la empresa, que se conforma en el presente plan de gestión de seguridad de la información.

Dada la documentación del presente documento del plan de gestión de seguridad de la información con diseños de formatos especiales que son diferentes al cuerpo del presente trabajo,

dicho documento está incluido como anexos, es importante tener en cuenta la asignación de roles y responsabilidades relativas a la seguridad de la información en DUBAI, por lo tanto, se diseñó el siguiente cuadro teniendo en cuenta el personal con que cuenta la empresa y sus funciones frente a la protección de la información y como quedaría conformado el comité de seguridad de la información.

Asignación de roles y responsabilidades

ROL	RESPONSABLE	RESPONSABILIDAD
Comité de seguridad de la información	Gerente	Coordinar el comité de seguridad de la información
		Implementar y cumplir la presente política
información	Jefe de área	Definir que usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
Área de recursos humanos	Contador publico	Notificar a todo el personal que ingrese las obligaciones del cumplimiento de la Política de Seguridad de la Información, los procedimientos y prácticas
		Implementar la suscripción de los acuerdos de confidencialidad y las tareas de capacitación en materia de seguridad de la información
usuarios	Personal de la empresa	Conocer y cumplir con la política de seguridad de la información

El comité de Seguridad de la información de la empresa motel Dubái, será la dependencia encargada de recibir los informes trimestrales que el gerente, área de sistemas y contador elabore teniendo en cuenta las novedades y el seguimiento de control.

CRITERIOS PARA PRIORIZACIÓN DEL PROYECTO

- Elaboración del Plan de Seguridad de la Información
- Iniciativas que soportan la implementación de la estrategia de seguridad
- Mitigación de riesgos de seguridad de la información que garanticen la custodia de la información en su confidencialidad, disponibilidad e integridad.
- Identificar los procesos que respaldan el cumplimiento de la estrategia.
- Contar con soluciones para mejorar los indicadores de gestión de algunos procesos.

IDENTIFICACIÓN DEL RIESGO

1. Riesgo Estratégico: Se asocia con la forma en que se administra la empresa.
El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
2. Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de los clientes y personal hacia la empresa.
3. Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información, de la definición de los procesos, de la estructura de la empresa y de la articulación entre dependencias.
4. Riesgos Financieros: Se relacionan con el manejo de los recursos de la empresa que incluyen; la ejecución de balances, la elaboración de los estados financieros, los pagos y manejo sobre los bienes.
5. Riesgos de Cumplimiento: Se asocian con la capacidad de la empresa para cumplir con los requisitos legales, contractuales y en general con su compromiso ante los usuarios, en relación con su misión.
6. Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la empresa para satisfacer sus necesidades actuales y futuras en el cumplimiento de la misión empresarial.

SITUACION NO DESEADA

- ✓ Robo de información vital o de equipos informáticos.
- ✓ Pérdida o borrado de la información
- ✓ Hurto de información durante el cumplimiento de las funciones laborales
- ✓ Incendio en las instalaciones de la empresa por desastre natural o de manera premeditada.
- ✓ Alteración de claves de sistemas y/ manipulación de la información.
- ✓ Daño de equipos y de información Atrasos en la entrega de información
- ✓ Fuga de información Manipulación indebida de información.

PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- ➢ Dar soporte al plan de seguridad de la información conformes a las normas y controles establecidos
- ➢ Preparación de un procedimiento de respuesta a incidentes.
- ➢ Descripción de los requisitos de seguridad de la información para un producto un servicio
- ➢ Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

ANALISIS DE VULNERABILIDADES.

Descripción de vulnerabilidades. Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, En la empresa motel Dubai se encontraron otras amenazas como las siguientes:

1. La infraestructura física es amplia, pero las áreas vitales donde se encuentran los equipos TI es pequeña limitando en algunos casos puntuales las labores de los empleados.

2. Se evidencia que los usuarios y contraseñas al sistema de cámara de vigilancia en las áreas de la empresa no deben ser manipuladas por todo el personal solo deben tener acceso a estos recursos tecnológicos el personal capacitado y destinado para tal fin.

3. El sistema eléctrico está cerca a los escritorios, no existe distancia segura de los dispositivos electrónicos, la cantidad de equipos que tiene cada oficina son reorganizados para mayor eficiencia, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el empleado no alcanza a ser guardada.

4. Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento, el cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y equipos
- En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
- los equipos de cómputo insuficientes para el uso de la totalidad de su personal.
- Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.
- sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, debidamente demarcados y mejorando en los procesos.
- La información es llevada un solo equipo principal.
- No hay control para el uso de memorias portátiles en los equipos exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
- Descarga de música, videos y otros tipos de archivos generando posibles amenazas y perdida de información.
- desconocimiento del tema de seguridad y privacidad de la información en el personal de la empresa
- No existe un historial de reportes de los procesos de mitigación de vulnerabilidades realizados por el personal de sistemas en la empresa.
- Los documentos físicos manejados en la empresa algunos no se han digitalizado en su totalidad, por lo tanto, están expuestos a pérdidas y daños.
- No existen procesos de copias de seguridad establecidos, solo la contadora de la empresa realiza copias en su equipo personal.
- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones
- Se cuentan con los tipos de extintores adecuados para cada emergencia.

INFORMES

Realizado el diagnóstico y verificación de los resultados obtenidos se logró identificar las fallas de seguridad que tiene la Empresa, señalando que existen amenazas reales que pueden afectar los activos e información de la empresa motel Dubai

- Con base en el diagnóstico elaborado a la infraestructura tecnológica del motel Duabi, se identificó las vulnerabilidades que pueden generar riesgo a los activos e información.
- Se estableció el riesgo existente en los recursos como redes sistemas de vigilancia, sistemas informáticos, también sumado a la posible manipulación de la información.
- Se debe crear un plan de gestión de seguridad de la información, junto con un manual de normas y políticas de seguridad informática que se debe dar a conocer a los empleados, que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad.
- Es necesario actualizar y mejorar las políticas de seguridad en la empresa con el fin de llevar un tratamiento continuo de los riesgos.
- Diseñar e implementar el plan de seguridad que permita la continuidad del negocio, generación de backup, documentar todos los procesos que el personal cumple en la empresa en temas de seguridad de la información, reportes o controles para estructurar mejoras de un plan de gestión de riesgos de seguridad de la información.
- Realizar capacitación a personal nuevo y existente en las normas, controles y procedimientos a seguir para el bueno manejo de la información
- No dar tanta confianza a empleados en el manejo de sistemas de información con datos críticos.