DISEÑO DE CONTROLES Y POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA RED LAN EN EL HOTEL PIPATON

WILFRIDO ALFONSO TRUJILLO NIEBLES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BARRANCABERMEJA - SANTANDER

2020

DISEÑO DE CONTROLES Y POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA RED LAN EN EL HOTEL PIPATON

WILFRIDO ALFONSO TRUJILLO NIEBLES

Trabajo de grado presentado para optar por el título de:

Especialista en seguridad informática

Director de Proyecto:

Ing. Hernando José Peña Hidalgo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BARRANCABERMEJA - SANTANDER

2020

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Barrancabermeja, 01 de octubre de 2020

Este proyecto lo dedico primero que todo a papito Dios, porque me ha dado la posibilidad de cumplir una etapa más en mi vida, que con mucho esfuerzo me ha acompañado y fortaleciéndome en cada paso de esta especialización.

A mi madre que me dio la oportunidad de ser profesional y poderme abrir camino en el mundo laboral y de realizarme en lo personal. A mi hermana por el apoyo a seguir adelante teniendo la mirada en Dios. A mis hijos que son el motor que me impulsa a seguir día a día capacitándome y logrando mejores cosas.

De antemano agradecerle a las directivas del hotel y centro de convenciones Pipatón y su empresa propietaria Ibertur S.A.S., por permitirme la realización de este proyecto en sus instalaciones.

Al señor Oscar Castilla Alarcón, gerente operativo, por su disposición, colaboración y confianza para la realización de este proyecto que beneficiaría al hotel Pipatón.

A los funcionarios de las diferentes áreas involucradas en la realización del proyecto por la disposición ofrecida en la generación de información requerida.

Al ingeniero Hernando José Peña, por su orientación y dedicación a la culminación de este proyecto, compartiendo sus conocimientos y las recomendaciones para la culminación del proceso.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO INFORMÁTICO: recursos que tiene una empresa para la realización de sus procesos.

ADMINISTRACIÓN DEL RIESGO: son las tareas implementadas para realizar control de los riesgos en una empresa.

AMENAZAS: son las fallas que puede presentar una empresa y que a largo plazo se pueden convertir en un incidente.

ANÁLISIS DE RIESGO: son las diferentes técnicas para manipular la información y generar resultados para tomar decisiones que mejoren la situación actual.

COPIAS DE SEGURIDAD: son los duplicados de la información que se tienen para utilizar en algún momento crítico de la empresa.

DATACENTER: sitio destinado para albergar equipos de cómputo, dense se guarda la información privada de una empresa.

DATOS O INFORMACIÓN: son los datos recopilados por la organización para la manipulación en los diferentes procesos.

DEBILIDADES: son los posibles riesgos que pueden presentar una organización en el área informática.

HARDWARE. Son los dispositivos electrónicos que puede tener un sistema informático.

IMPACTO: es la situación presentada después de la ocurrencia de un riesgo.

MAGERIT: metodologías diseñadas para la reducción de los fallas en el uso de las tecnologías de la información.

METODOLOGÍA: son las diferentes actividades implementadas para la realización de un objetivo.

PROBABILIDAD: son las posibilidades que una falla pueda ocurrir en una empresa.

PYME: hace referencia a las medianas y pequeñas empresas.

RED: son los diferentes equipos de cómputo, conectados entre sí, por un medio físico.

RIESGO: son las posibles fallas que pueden presentar una organización en el área informática.

SEGURIDAD DE LA INFORMACIÓN: medidas para la protección informática tomadas en una empresa.

SEGURIDAD: medidas implementadas para blindar protección al interior de una empresa.

SERVIDOR: es el equipo de cómputo principal en una red, es donde se almacena la información principal de una empresa. A veces es el encargado de administrar algunos servicios de red.

SGSI: se refiere a los sistemas de gestión de seguridad de la información implementados en las diferentes empresas.

SOFTWARE: hace referencia a las aplicaciones que se manejan en una empresa, ya sean sistemas operativos, herramientas de diagnóstico y aplicaciones.

VULNERABILIDAD: hace referencia a las debilidades o fallas que presenta una empresa en su red o sistema de información, que pueden aprovechar para cometer delitos informáticos.

RESUMEN

El hotel Pipatón, para la protección de la información que recopila de sus clientes, huéspedes o proveedores que manipula en las diferentes áreas con que cuenta la organización para poder prestar y ofrecer sus servicios. Describiremos los diferentes pasos que se tomaron para la realización del diseño de los controles y políticas de calidad que servirán para minimizar las diferentes vulneraciones existentes en el hotel Pipatón con ayuda de la metodología Magerit. Se identificaron las diferentes fallas de seguridad de la información en las diferentes áreas con el apoyo de los funcionarios involucrados en el manejo de los sistemas de cómputo.

Después e lograron identificar los activos de información y se realizó el respectivo análisis para determinar el grado de vulnerabilidad existente y plasmarlo en el mapa de calor diseñado para este fin. Después de haber identificado los activos informáticos y su respectiva valoración, pasamos a plantear controles para poder minimizar las falencias o debilidades presentadas y por último se presentan unas políticas a tomar para que la empresa implemente con todos sus funcionarios. Los Controles y políticas de seguridad, tendrán éxito si concientizamos a los usuarios que ellos son los encargados de salvaguardar los datos en el hotel Pipatón.

Seguridad informática, seguridad de la información, seguridad en red LAN, Vulnerabilidades, controles y políticas de calidad.

INTRODUCCIÓN

La competitividad de los mercados en la actualidad, y la tendencia de cambio de los servicios, hacen que las empresas estén innovando constantemente. Como dice Alarcón[1], teniendo un desafío imponente día a día, productos y servicios más seguros, confiados y flexibles, llegando a los usuarios finales con un óptimo costo y de forma ágil, por todo esto las empresas requieren de una mayor investigación, tecnificar procesos y una constante labor de reingeniería.

Por tal razón, es Así mismo, son incuestionables los beneficios y generosidades obtenidos que admite el firme avance en comunicaciones y tecnologías de la información en el ambiente de una empresa, con un mayor alcance y siendo efectivos alcanzando una amplia cobertura, costos bajos en los servicios son algunos prototipos que enmarcan los beneficios que se generan con el aprovechamiento de la revolución de las TIC.

En la conformación de los controles y las políticas de seguridad de la información, el proceso de análisis y diseño en la red LAN del Hotel Pipatón. El objetivo de los controles y políticas es la de defender la confidencialidad e integridad, de cada y

[1] ALARCÓN, Javier Orlando. Aspectos de la investigación. En: Diseño e implementación de políticas de seguridad informática, red y virtualización apoyadas con software libre en la compañía tecnología y redes S.A.S. 2016. p.16.

uno de los activos de la organización. El objetivo se alcanzará primordialmente con un robusto análisis de riesgos que constantemente soporte la información obtenida en el hotel, y posteriormente realizar la máxima protección de los activos de la empresa, implementando las salvaguardas requeridas.

Como dice Suarez[2], en el mundo actual, las empresas medianas y pequeñas enfrentan grandes peligros, por el motivo que la mayoría de las organizaciones, invierten pocos recursos en la seguridad. Y mucho menos invierten en mitigar los riesgos que se le pueden generar a los activos asociados a la información, lo que en gran parte de se deriva en pérdidas de la información y riesgos económicos.

Con todo lo expuesto anteriormente, y evitando ser víctima de algún tipo de vulnerabilidad, es que el hotel y centro de convenciones Pipatón, realiza el proceso de establecer controles y políticas para salvaguardar la información en los sistemas y la red LAN existente, y de esta forma garantizar que todos los funcionarios que ingresen a la información para su visualización o manipulación, estén debidamente autorizados y logrando de esta manera que los funcionarios tomen conciencia de la implementación de la seguridad informática, y así mismo el uso de medidas específicas claras que conlleven a obtener beneficios para la organización.

[2] SUAREZ, Sandra Yomay. Justificación del proyecto. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.15

1. DEFINICIÓN DEL PROBLEMA

1.1 PRESENTACIÓN

Como dice Suarez[3], actualmente los sistemas de información y las empresas, afrontan, un incremento de inseguridades y riesgos informáticos, derivados de una amplia diversidad de fuentes, en los que se tienen los delitos relacionados a la informática, sabotajes, espionajes, perjuicios que ocasionan los virus informáticos y agresiones de intrusión o de servicios de navegación, que se han vuelto cada día más comunes de las empresas.

El Hotel y centro de convenciones Pipatón, recibe información de sus proveedores y clientes por multiplex medios y canales (personal, redes de datos, sistemas en línea, telefónico, empresas de mensajería, electrónicos, entre otros); información financiera y personal. Esta gran cantidad de información y datos forman la principal materia prima para los procesos del hotel, convirtiéndolo en el activo más importante que se debe proteger desde el ingreso hasta su disposición final.

[3] SUAREZ, Sandra Yomay. Justificación del proyecto. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.17.

“Los datos son para las organizaciones lo que significa el corazón para el cuerpo humano”[4], en este pasaje se puede afirmar a los datos pasan a ser el activo con un alto valorado que conserva una empresa, debido a que estos datos se ya que se proporcionan a los demás procesos de servicios que ofrece el hotel, la información se vuelve el todo, de tal forma, resguardarla de personas extrañas, conservarla segura y es de importante en el entorno laboral.

Como dice Alarcón[5], el Hotel Pipatón, dentro de su infraestructura no tiene una arquitectura tecnológica con diseños de gran disponibilidad para las aplicaciones de la empresa, es decir, un suceso catastrófico, sería la parálisis general de los procesos. El Hotel Pipatón no tiene un equipo servidor alterno para una replicación (Datacenter)[6], conllevando un gran peligro en la evolución del hotel Pipatón.

Se debe contar con una conveniente protección, independiente de la forma como esta información se manipule (ingrese, almacene y comparta), sin embargo, la seguridad de la información que el hotel Pipatón tiene en estos momentos es muy limitada, por este motivo se eligió realizar un estudio minucioso de la realidad actual,

---

[4] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Justificación. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p.5.

[5] ALARCÓN, Javier Orlando. Descripción del problema. En: Diseño e implementación de políticas de seguridad informática, red y virtualización apoyadas con software libre en la compañía tecnología y redes S.A.S. 2016. p.17.

[6] Un data center es un centro de procesamiento de datos, una instalación empleada para albergar un sistema de información, como telecomunicaciones y los sistemas de almacenamientos.

como primera fase, y con los resultados obtenidos, edificar controles y políticas para la seguridad de la información en la LAN en el hotel Pipatón, para ser incorporada por el administrador informático encargado para proteger la información en el hotel y centro de convenciones Pipatón.

Como dice Suarez[7]; comprometiendo a todos sus funcionarios como una pieza para la creación activa del proyecto, para que con esto se pueda garantizar y minimizar en buen porcentaje las debilidades enfrentadas en la organización en términos de seguridad informática, podrán ser de conocimiento de la dirección, con el fin de establecer si, son: gestionados, asumidos, minimizados, accediendo a la formalización de un ambiente seguro para la información, aplicaciones y sistemas de gestión.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué puede hacer el Hotel Pipatón en la red LAN, para minimizar los factores de vulneración y riesgo a los que exponen día a día, la información de la organización, y así poder contribuir con el mejoramiento de la seguridad?

[7] SUAREZ, Sandra Yomay. Formulación del problema. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.17.

2. JUSTIFICACIÓN

En muchos países del mundo al igual que en Colombia, las personas y organizaciones, todavía no han tomado conciencia de la gran variedad de vulnerabilidades o riesgos que poseen en la parte de sistemas. El área de informática en los últimos días ha presentado un crecimiento, por tal razón, la información almacenada dentro de nuestros sistemas de información, está quedando más expuesta a los ataques los Crackers o Hackers, aprovechando las falencias de seguridad[8] y por tal razón, es muy viable que estas personas secuestren o roben la valiosa información de la organización.

Como dice Pulido[9] , el continuo aumento de las amenazas a la información, buscando robar la información de las organizaciones, sacar beneficios de los delitos financieros, realizando ataques al servicio como el de cómo es visualizado en los informes, por las organizaciones de seguridad, las autorizadas en el tema de seguridad. Este tema ha obligado a dar prioridad a las empresas en cuanto a la seguridad informática, ya que los procesos, la información realizan procedimientos con los activos más valiosos.

---

[8] Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño.

[9] SUAREZ, Sandra Yomay. Justificación del proyecto. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.18.

Como dice Alarcón[10], la necesidad de perfeccionar los procedimientos tecnológicos, seguridad de la información, definiendo planes de continuidad en el ejercicio, controles y políticas de seguridad de la información, mejorando la administración de los recursos financieros, hacen fundamental que se implemente un plan de investigación.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles. En la organización diligenciar la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes. También se puede requerir asesoría especializada de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño[11].

En la actualidad asegurar la integridad, confidencialidad y disponer de la información más sensible, se vuelven fundamentales en beneficio de la consecución y mantenimiento de los estándares de competitividad, economía, imagen de la

[10] ALARCÓN, Javier Orlando. Justificación del proyecto de implementación. En: Diseño e implementación de políticas de seguridad informática, red y virtualización apoyadas con software libre en la compañía tecnología y redes S.A.S. 2016. p.19.
[11] Norma Técnica Colombiana NTC ISO 17799, Tecnología de la Información, ICONTEC, 2006. Citado por PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Justificación. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p.8.

organización, para conseguir objetivos de la empresa, obteniendo beneficios económicos.

Como dice Pulido[12], el sitio de inicio para encaminar la seguridad de la información al interior de una organización se ubica las políticas de seguridad, que se diseñen. Estas contienen una lista de objetivos, implementando una serie de procedimientos requeridos para obtener un nivel adecuado de seguridad, apropiado para lo que se requiera al interior de la organización.

Como dice Pulido[13], cada país para ofertar esta competitividad la primera mediad que tiene que seguir es brindar sistemas de alta seguridad y confiabilidad, en donde la vulneración del sistema de información sea muy difícil. Los diferentes controles y políticas de seguridad son comprados a un alto costo económico. En cuanto a las empresas pequeñas no cuentan con los recursos necesarios para la adquisición de ellos, por ende, la mayor parte de las empresas son vulnerables a los ataques realizados desde el exterior de la organización.

---

[12] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Justificación. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p.8.

[13] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Justificación. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p.9.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar el análisis de la situación actual del Hotel Pipatón, diseñar controles y políticas de seguridad de la información en el sistema de información, red LAN, ofreciendo a la infraestructura tecnológica una apropiada protección en seguridad informática a la organización.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar el diagnóstico actual de la situación de la seguridad de la información del Hotel Pipatón.
- Identificar por medio del análisis de riesgo los activos de información, las amenazas y vulnerabilidades a las que está expuesto el sistema de información, a través de cuestionarios, entrevistas a los funcionarios, responsables.
- Elegir los controles más importantes de la seguridad de la información, que garanticen la integridad, disponibilidad y confidencialidad de la información.
- Establecer unas políticas de seguridad conforme a los patrones universales, buscando establecer una manipulación aceptable para los activos de información.

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

Como dice Perafán[14], para toda empresa es claro que el activo más significativo es la información, por tal razón, se requieren tener políticas viables que la salvaguarden sin excluir la seguridad de los equipos de cómputo donde se guarda la información. Estas políticas o normas se tienen que estructurar en los estándares universales de seguridad física y lógica que conlleven a la unificación de defensas y procedimientos que protejan la información, permitiendo el ingreso, manipulación únicamente a los funcionarios acreditados.

En la actualidad podemos encontrar en el comercio electrónico diversos equipos de electrónicos como los equipos portátiles, tabletas, celulares, etc., que actualmente se han convertido en el objetivo de los ataques y averiguaciones de vulnerabilidades existentes en ellas, y diversos delitos informáticos. Las actividades de contingencia, normas, controles y políticas de seguridad, deben contemplar las áreas lógicas como físicas en la administración de la seguridad de la información.

Particularidad de los Sistemas Seguros:

[14] PERAFAN, Jhon Jairo and CAICEDO Cuchimba Mildred. Conclusiones. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. 2014. p.24-28

Confidencialidad: La información guardada en el sistema de información solo tendrán acceso a ellas los funcionarios autorizados.

Integridad: La información guardada en el sistema de información solo podrá ser manipulada por los funcionarios autorizados.

Disponibilidad: Los funcionarios de la organización deberán tener a su disposición el sistema de información para manipulación en cualquier momento. La información que no se puede ingresar, no sirve tenerla en el sistema, de manera ilesa. Por disponibilidad igualmente se piensa en el procedimiento de recuperar la información almacenada en un sistema de información de forma rápida. A continuación se detallaran conceptos que son relacionados con la seguridad de la información:

Auditoría: Procedimientos con los cuales se puede establecer que fallas o debilidades presenta un sistema, los movimientos de los funcionarios, las fechas y horas de los ingresos.

Control de ingreso a recursos: Es la norma por la cual un sistema de información se regula en su utilización de servicios ofrecidos.

Metodología para auditar: Consiste en la presentación de normas o procedimientos correctos, para la realización de actividades, labores, pasos para implementar procedimientos preliminares de investigación, diagnósticos de controles, paralelos actualizados de seguridad, y terminando con la presentación de informes con los efectos de la implementación de la metodología.

Magerit: La metodología está fundamentada en pasos para implementar procesos analíticos en riesgos y de igual manera proporciona normas la administración de debilidades de sistemas de información, teniendo en cuenta los puntos que tengan finalidad en las empresas para alcanzar la mayoría de los objetivos trazados cumpliendo con los alcances de la organización. Este proyecto se fundamentó en Megerit para desarrollar el análisis de riesgos alcanzando varios logros: identificar activos, amenazas, estableciendo los riesgos, las debilidades potenciales y realizando recomendaciones, como los controles y políticas de seguridad.

Formatos de Trabajo: se refiere a las evidencias físicas que el personal encargado de realizar la auditoria manipula, para el levantamiento de información de cada uno de los puestos laborales, se emplea el manejo de formatos.

SGSI: el sistema de gestión de seguridad de la información es el encargado de suministrar diversidad de procedimientos y herramientas fundamentadas en la norma ISO27001, la cual permitirá identificar en una organización que debilidades puede tener la seguridad de la información, especificando como administrar los riesgos, convirtiéndose en estándares de la organización para ser socializados a todos los funcionarios involucrados, siendo de constante revisión y constantemente mejorado.

Para diseñar las políticas y procedimientos de una empresa se deberán tener en cuenta las anteriores pautas tratando de no obviar los puntos más importantes y se

puedan efectuar los procesos de excelente manera para usuarios y sistema, teniendo en cuenta los deberes de usuarios y administradores. Para no crear un entorno de tensión en la empresa, se deben dar a conocer a los funcionarios los controles y políticas de seguridad, garantizando los servicios prestados.

Para vigilar y salvaguardar los activos informáticos de una empresa, fue establecida la seguridad informática, garantizando la integridad, disponibilidad y confidencialidad de la información sin importar su capacidad, tipo o naturaleza.

La información: al interior de las organizaciones sea convertido en el elemento principal. La seguridad de la información deberá contar con pautas determinadas por el administrador del sistema y funcionarios capacitados, contemplando que personal no autorizado o externo consigan ingresar sin ser autorizados. Impidiendo que la información sea manipulada de manera maliciosa logrando sacar beneficios de ella.

La seguridad de la información tiene como función la accesibilidad y disponibilidad que nos garantizan el ingreso a la información y la disposición inmediata en cualquier momento, incorporando las copias de seguridad, si dado el tema de presentarse fallas o daños de información, por accidentes, desastres naturales, se logre utilizar una copia de seguridad impidiendo parálisis en la empresa o interrupción de los servicios, que conlleva costos y perdidas.

La infraestructura tecnológica: dentro del día a día de las organizaciones se ha convertido en una parte imprescindible para realizar gestión, administración y almacenamiento. La seguridad informática ejerce el papel de vigilar el correcto trabajo del hardware logrando impedir robos, fallas eléctricas, incendios, calamidades naturales, que consigan perturbar en forma directa la infraestructura tecnológica.

Usuarios: los funcionarios que están de forma directa en constante interactuación con el sistema de información, manipulación de la información y comunicaciones. La seguridad informática contemplará pautas que ayuden a minimizar las vulnerabilidades de la información y de su infraestructura, en esas pautas se deberá contemplar, horas de ingreso, limitaciones lógicas y físicas, autorizaciones, prohibiciones, perfiles, métodos de emergencia, con forme a estándares internacionales, que ayuden a minimizar las vulnerabilidades y el impacto en presencia de la ocurrencia de una catástrofe.

4.2 MARCO TEÓRICO

Desde años atrás se viene entendiendo lo importante que es realizar la administración recursos primordiales con la los sistemas, y el pensar en informática está directamente ligado a hablar de tecnología de punta, tanto en hardware, software y diferentes maneras de manipular la información, buscando la forma que

sea más permanente, pero nunca se consideró el camino que nos acercara a la informática, omitiendo que los datos forman la base de la informática[15].

Las empresas deberán encaminar la información al igual como lo ejercen con los otros recursos, de manera organizada, correcta, clara y eficiente, buscando que agrandar las utilidades. Los funcionarios administradores son conocedores que existen costos afines con el almacenamiento, seguridad, producción, distribución de la información que se manipula al interior de las empresas. Entendiendo que la información posee un costo monetario y que con la manipulación optima se conseguirá progresos significativos que le posibilitará a la empresa convertirse en competitiva y eficiente.

Como dice Suarez[16], hoy en día se debe tener en cuanta como un elemento crítico de las tácticas del servicio para una empresa, además se deberá manipular en métodos integrales, para poder garantizar la “defensa” en cualquier aspecto. En nuestro país las empresas han venido visionando en el ambiente privado y público, salvaguardar sus infraestructuras de tecnología de cualquier medio de las amenace,

---

[15] SALAZAR, Jacqueline. La Informática y Su Impacto Social. Universidad de Pinar del Río. Hnos. Cuba, Citado por PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 13.

[16] SUAREZ, Sandra Yomay. Marco teórico. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.23.

buscando la resguardar la infraestructura vulnerable y de una vez sus procesos esenciales. Con esta forma de ver la situación se vienen fomentando estudios, averiguaciones y tesis, que tienen relación con la seguridad informática.

Como dice Pulido[17], los sistemas de información (SI), realizan procesos desarrollados con la información son evaluados y salvaguardados, interactuando con los siguientes puntos: capital informático, físicos y de telecomunicaciones, políticas y medidas de trabajo, técnicas laborales, actividades, personal idóneo, datos fuentes. En un sistema de información, se efectúan cuatro acciones primordiales:

Ingreso de información (INPUT): es la manera por el cual el sistema recopila la información para la manipulación de los datos, se realiza por medio de ratones, teclados, medios magnéticos, códigos de barra, etc.

Almacenare de información: Tarea con alto grado de jerarquía que se realiza, porque por medio de este proceso los sistemas obtienen la recopilación de los datos utilizados en técnicas preliminares.

[17] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco teórico – conceptual. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 13.

Procesamiento de información: Facultad de los sistemas para posibilitar el desarrollo de la información para rápidamente ser manipulada para ejecutar proyecciones, con la información recopilada en el proceso y volver una empresa más competitiva y eficiente.

Salida de información (OUTPUT): Proceso que nos retorna la información manipulada, por medio de medios magnéticos, impresiones, etc. La gestión apropiada de los sistemas de información (SI) se ha convertido en un gran reto característico para los administradores empresariales, ya que al progresar al campo de la informática se pude llegar al fracaso, por motivos de las amenazas existentes en el comercio y la dura competencias.

Seguridad de la información:

Los sistemas de información para las empresas resultan de gran ayuda para la seguridad de su elemento principal (información) deberá ser resguardado de forma apropiada, el desarrollo de una empresa está basado en la seguridad de la información, minimizando las fallas y maximizando las inversiones. La información se pude obtener en diferentes maneras, física o impresa en hojas, digitalmente, enviada por correo, visualizada en pantallas y en audios de diálogos.

De cualquier manera, que se recopile la información, o la forma como se desplace o se guarde, rutinariamente deberá ser salvaguardada de manera adecuada. La seguridad de la información se define como la preservación de los siguientes rasgos:

- Confidencialidad: certifica que la información sea visualizada solo por funcionarios con ingreso autorizados.
- Integridad: la protección total de la información y técnicas de procesamiento.
- Disponibilidad: certificara que los funcionarios autorizados puedan ingresar a la información y recursos afines, en todo momento.

Política de seguridad

Haciendo un conjunto apropiado de controles se obtendrá una buena seguridad de la información, estos controles contienen, funciones de software[18], procedimientos, experiencias, estructuras de la organización, y actas en las cuales quede registrado las responsabilidades de la dirección de la empresa con la seguridad de la información, que deberá quedar plasmado el concepto de seguridad de la información dentro de los lineamientos de la organización.

El progreso de la política de seguridad se puede dividir en tres etapas:

Como primer punto se definió la planificación, la redacción e investigación de la política. Crear una política se tiene que identificar para que se requiere, ejemplo, aspectos legales, contratos operacionales, se deberá establecer el alcance y aplicación, roles y los responsables de la utilización de la política garantizando la

[18] Instituto Argentino de Normalización. Esquema 1 de Norma ISO IEC 17799. Tecnología de la Información. Citado por PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 15.

posibilidad de su ejecución. La realización de una política deberá contener una investigación que establecerá las obligaciones de la empresa para la creación de las normas, las áreas que deben aprobarlas. En esta etapa se conocerá el documento con la política acorde con los estándares de la empresa.

El segundo punto de la política es la revisión, después de haber concebido la documentación y se ha comenzado la coordinación, se deberá llevar a una persona independiente para revisión y aprobación. Una revisión independiente conlleva varios beneficios: una política más factible por medio de la revisión de una persona que tiene un punto de vista diferente a el funcionario que creo la norma, se obtendrá un soporte extenso para la norma por medio del aumento en el número de personal inmerso, ampliación de la credibilidad por el aporte realizado por los especialistas que la revisaron.

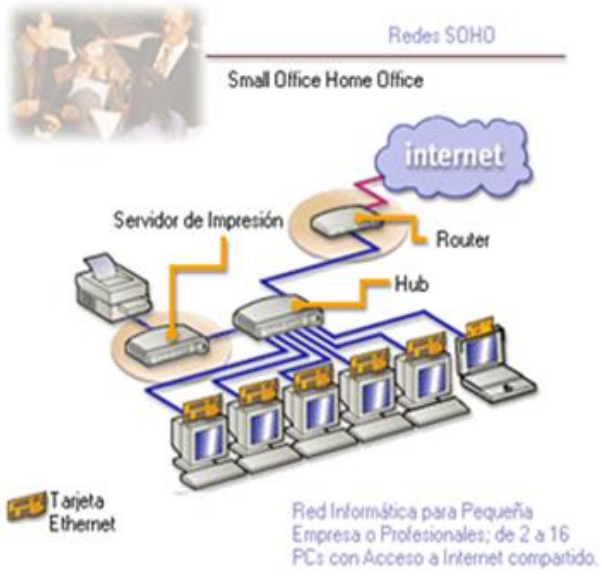
En este nivel se hace la socialización de la política al personal que la revisara, sea carácter formal o informal, dando a conocer cualquier tema de importancia en la revisión, exponiendo el objetivo, el argumento y los potenciales servicios de la norma, demostrando su necesidad. Como objetivo de esta sección, se busca que la persona que implemento la política recoja las observaciones efectuando cambios, desarrollando los arreglos y estudios requeridos para conseguir la versión actual de la política y aprobación de la administración.

El último punto en la evolución de las políticas, es la aprobación. El objeto fundamental de esta fase es conseguir el apoyo de las directivas de la empresa, respaldada en la firma de un funcionario de perfil administrativo y con autoridad.

Red SOHO (Small Office, Home Office)

Este tipo de red LAN, está enfocada a entidades que tienen un tope de equipos de cómputo inferior a dieciséis computadores, con su respectivo ingresos a la red WAN o internet compartido, como se muestra en la figura No. 1, que se estipula para mencionar a los dispositivos dispuestos para manejo profesional, que en comparación con otras marcas, no fueron diseñados para un grandes usos de trabajo.

Figura 1. Red para empresas pequeñas



Fuente: PANAFONIC.COM. [Sitio web]. España: PANAFONIC, Redes SOHO. [Consulta: 11 mayo 2020]. Disponible en: http://www.panafonic.com/netquote.htm

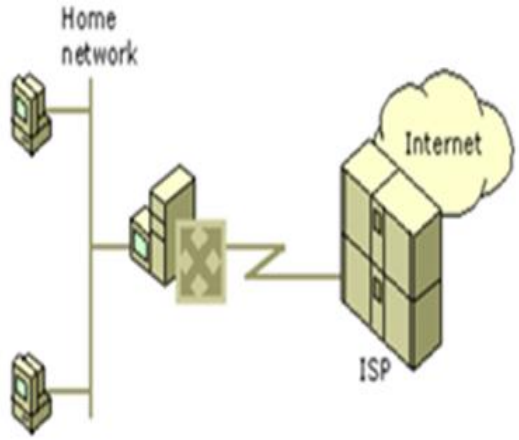
Conexión enrutada

Como dice Microsoft[19], para este tipo de conexión, el equipo servidor es el encargado de realizar el enrutamiento y el ingreso remoto trabaja como un enrutador IP, que es el encargado de reenviar los paquetes los dispositivos host SOHO y el host de la WAN. La red SOHO se caracteriza por:

- Red segmentada
- Manejo de un solo protocolo (TCP/IP)
- Posee conexión de vínculo dedicado con cualquier proveedor de internet (ISP).

A continuación, mostraremos una red SOHO enrutada.

Figura 2. Conexión Enrutada



Fuente: MICROSOFT.COM. [Sitio web]. USA: MICROSOFT, Conexión enrutada a Internet. [Consulta: 11 mayo 2020]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780147(v%3dws.10)

[19] MICROSOFT. Documentación. En:. Estados Unidos. 2020. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc736774(v%3dws.10)

El encargado de realizar el enrutamiento e ingreso remoto, es el servidor, que se configura con un dispositivo de red muy utilizado en las redes domésticas, como las redes Ethernet, y un dispositivo modem análogo. Se podrá manejar una conexión de trazo concedida o una tecnología de conexión duradera, como puede ser la ADSL y modem, pero aquí mostraremos el tipo de configuración más actualizada, que requiere para la conexión un ingreso por teléfono ISP.

Conexión traducida

Como dice Microsoft[20], para este tipo de conexión, el equipo de encargado de realizar enrutamiento e ingreso remoto y NAT trabajo como intérprete de direcciones, el enrutador IP que convierte las direcciones enviadas entre los dispositivos host SOHO y los del servicio de internet. Para realizar la configuración tan solo se requiere un protocolo de enrutamiento que descifre las direcciones, tal como el Network Address Translation, encargado de descifrar las direcciones, direccionamiento e identificación de nombres de equipos en la red SOHO.

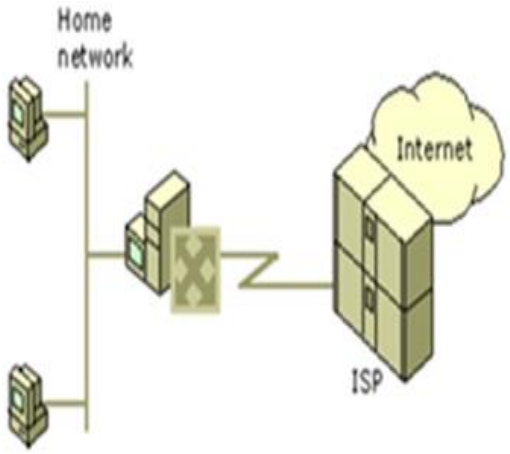
Este tipo de red se caracteriza por:

- Realiza segmentación de red
- Manejo de un solo protocolo (TCP/IP)
- Posee conexión de vínculo dedicado con cualquier proveedor de internet (ISP).

[20] MICROSOFT. Documentación. En: Conexión traducida a Internet. Estados Unidos. 2020. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780147(v%3dws.10)

A continuación, mostraremos una red SOHO traducida.

Figura 3. Conexión Traducida



Fuente: MICROSOFT.COM. [Sitio web]. USA: MICROSOFT, Conexión enrutada a Internet. [Consulta: 11 mayo 2020]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780147(v%3dws.10)

Para poder realizar el intercambio de datos, como se mostró anteriormente, los equipos requieren una ubicación cercana, facilitando que los funcionarios encargados de la manipulación de la información se relacionen y conozcan, convirtiéndose en un alto peligro para la red SOHO y teniendo una ventaja para el ingreso desde el exterior a la información. Por tal razón, mediante el uso de equipos se deberá controlar el ingreso a la información resguardada.

Sistemas biométricos

Son dispositivos que nos facilitan el poder identificar a las personas por medio de particularidades personales, efectuándolo de forma sistematizada. Esta técnica

biométrica permite realizar la identificación con gran exactitud a personas, logrando gran seguridad en el momento de realizar la validación de la identidad.

Encriptación o Cifrado

Habitualmente las redes LAN están configuradas para controlar el ingreso de personas no autorizadas a la información privada, desde el exterior de la red de la empresa por medio de encriptación a los datos. Esta práctica está ligada al proceso para evitar que la información vital sea visible a los intrusos. Desencriptar[21] a información solo se realizará empleando una clave. Pero en la actualidad la gran parte de las redes LAN manipulan los movimientos de información entre host, como archivos planos. El personal no autorizado podrá tener ingreso a la información, con solo el ingreso y un indagador de protocolos.

Firma digital

Como dice Pulido[22], Firma electrónica que se utiliza para realizar la verificación o identificación de la persona que remite un correo o un documento, garantizando que el contexto del documento no ha sido reformado. Las firmas digitales son fácil transferencia, no se consiguen copiar, y se logran sellar con la hora y la fecha de

[21] Foro de internet. Alegsa.com: Diccionario de informática y tecnología [consultado el 11 de mayo de 2020, 18:28]. Disponible en: http://www.alegsa.com.ar/Dic/encriptaci%C3%B3n.php

[22] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco de referencia. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 20.

forma automática. Garantizar que el correo firmado llegue completo, representa que el que envía, no podrá negar que lo envío. La firma digital la podemos trabajar con todo tipo de documento, con seguridad o no, y quien recibe sepa la identidad de quien lo envía y que el documento llego ileso.

Así mismo asegurando los ingresos a los datos, colocando un filtro para controlar la circulación de la información de una red LAN a otra, evitando que personas externas puedan ingresar a la información privada. Esta manera de defensa de la información, se logra por medio de los llamados Firewall. La mayoría de delitos informáticos corresponden al robo, daño de información, como gusanos, virus, que se encargan de encontrar vulnerabilidades, es decir, puertos disponibles por donde pueden ingresar a la red.

4.3 MARCO LEGAL

Con el transcurrir de los días, el Internet se ha ido situando a nivel mundial como una herramienta de gran importancia. Las tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios. La evolución de la criminalidad informática y de las nuevas tecnologías, tanto en los métodos utilizados y las herramientas son contrarrestadas o minimizadas con las leyes existentes en los diferentes países. Debido a la proliferación de violaciones por delitos informáticos se los países han adoptado medidas disciplinarias para frenar los diferentes métodos de ataques y delitos existentes.

La parte jurídica juega un papel fundamental en el control de los delitos informáticos, en Colombia la ley 1273 de enero de 2009, sancionada por el presidente Álvaro Uribe, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico denominado 'De la protección de la información y de los datos. La cual contempla multas de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
Como dice Pulido[23], Normatividad 1273 de enero de 2009, declara la salvaguardia de los datos e información.

Esta normatividad implementa nuevos defensas de orden penal, creados para la defensa de la información y hechos de violaciones informáticas, y con castigos monetarios y penas de cárcel. Se tuvo en cuenta para estructurar esta ley las administraciones ilegales de los datos ajenos, quedando visible que las organizaciones se deben defender jurídicamente para defensa de algún tipo de delito.

En el tema de las amenazas informáticas, esta legislación divisa los progresos tecnológicos y la manipulación de ellos para sustraer el patrimonio de personas,

[23] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 23.

como ejemplo la clonación de medios electrónicos, variación de los equipos de cómputo para realizar transferencias por medio de aplicaciones y manipulación de cajeros, siendo estas prácticas cada día más frecuentes en nuestro país.

Como dice[24], en Colombia se ha normalizado la ley para el manejo de información personal, tal como lo dice el artículo cuarto de la ley estatutaria 1581 del año 2012, la cual fue acogida en parte por el decreto de la nación 1377 del año 2013, y que a continuación se mencionan:

Principio de legalidad: la manipulación de la información de las personas se considera como actividad regulada y deberá estar sujeta a las normas o leyes actuales.

Principio de finalidad: la manipulación de la información de las personas será bajo finalidad justificada en conformidad con la ley y por ende con la constitución, informando al propietario de la información.

Principio de libertad: para la manipulación de la información de personas, solo se podrá efectuar con una aprobación anticipada, por tal razón la información personal no se debe captar o socializar sin consentimiento.

Principio de autenticidad o calidad: la información será cierta, puntual, renovada, completa, probada y clara. Es un error manipular información incompleta.

---

[24] SUAREZ, Sandra Yomay. Justificación del proyecto. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.43, 44.

Principio de transparencia: este punto deberá certificar al propietario la verificación sin limitaciones la presencia de información personal en cualquier sistema.

Principio de ingreso y circulación restringida: la manipulación de la información se acoge a las limitaciones que resulten de la naturaleza, este principio solo podrá realizarse con personas que el titular autorice, por esta razón no debe ser socializada en internet o en otras formas de comunicación, exceptuando los medios públicos.

Principio de seguridad: la información se deberá manipular con procesos técnicos por la persona delegada para otorgar protección a la información, sin ningún tipo de manipulación y sin autoridad.

Principio de confiabilidad: está enfocado a todo el personal que administre la información siendo obligadas a ser discretas en la manipulación, y no liberar información a terceras personas o empresas.

4.4 ANTECEDENTES

a. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano. Autor: Carmen Elizabeth Fajardo Díaz

Como dice Fajardo[25], en este proyecto se enfoca a efectuar una investigación de las debilidades de la seguridad informática de una aplicación de gestión documental, estableciendo las debilidades de seguridad en los que se halla la información en la manipulación diaria de la aplicación de gestión documental, construyendo pautas para el procedimiento apropiado de las debilidades ejerciendo un control y minimizando a niveles admisibles.

En cualquier empresa, la documentación que manipulas diariamente se convierte en la seguridad que se realizaron las labores encomendadas, manipulando el documento sensible, por tal motivo la seguridad de la información se convierte en punto vital de las empresas que quieren efectuar un sistema documental, entre otros puntos el crecimiento productivo, reducción de costos y tiempo en los procesos.

En la actualidad la información tiene un valor para el desarrollo del negocio y desempeño de los objetivos de la empresa, la empresa dueña del software ha manifestado la necesidad de instaurar acciones de mejora identificando las vulnerabilidades que muestra el aplicativo en la defensa de la seguridad de la información. Por escenarios que han sufrido baja de confidencialidad y disponibilidad en la información que se manipula a través del aplicativo, y también

[25] FAJARDO, Carmen Elizabeth. Introducción. En: Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano. 2017. p.7.

fallas en el código fuente por falta de procedimientos para establecer metas para la gerencia y almacenamiento de datos de la evolución del software.

Como dice Fajardo[26] , en el mundo actual las organizaciones privadas como públicas han preferido por efectuar soluciones de gestión documental para tener la documentación centralizada, organizada digitalmente poder manipularla tanto en el interior y exterior de la empresa, convirtiéndose esta información en el activo informático más preciado, por tanto es requisito que estas aplicaciones salvaguarden la integridad, disponibilidad y confidencialidad de la información, características que hacen que una empresa sea competitiva. Link: http://repository.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%C3%B3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y

b. Diseño del sistema de gestión de seguridad de la información para la empresa SEREXCEL servicios funerarios. Autores: William Andrés Núñez Vergara y Edinson Andrés chacón Umaña.

   Como dice Núñez[27], en todos los ambientes de trabajo se presentan vulnerabilidades que pueden traer como consecuencias perdidas a la empresa

[26] FAJARDO, Carmen Elizabeth. Justificación. En: Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano. 2017. p.11.
[27] NUÑEZ, William Andrés and CHACÓN, Edinson Andrés. Resumen. En: Diseño del sistema de gestión de seguridad de la información para la empresa SEREXCEL servicios funerarios. 2017. p.11.

cuando no se manejan a tiempo y de manera adecuada. Para este tipo de inconvenientes hay métodos como es el tema de la gestión de las fallas tecnológicas enfocadas en salvaguardar la información, describiendo las fortalezas y debilidades que lograsen perturbar el servicio en su periodo productivo.

El presente proyecto mencionara temas concernientes a la gestión de las debilidades de la seguridad de la información, metodologías, estándares y herramientas que facilitan las pautas requerida para minimizar el nivel de debilidad que poseen los activos informáticos frente a una amenaza. Es de mucho valor que las empresas, que ofrecen algún tipo de servicios tecnológicos y conservar el respaldo de un gran volumen de información confidencial de manera segura, deberá tener un plan de trabajo de riesgos asegurando el contante desarrollo del negocio.

Por etas razones, se ha contemplado la necesidad de implementar un sistema de gestión de seguridad de la información SGSI cuidadoso a los diferentes procesos que conforman la entidad SEREXCEL servicios funerarios, enmarcada en la metodología Megerit. El primer paso es realizar una descripción del contexto presente de la empresa, paso siguiente realizar la identificación de los activos y las amenazas referentes, para después efectuar la medición de las vulnerabilidades encontradas formarían parte del proyecto de implantación.

Para finalizar el proyecto, la contribución de este trabajo es la de establecer los niveles de vulnerabilidad que tienen los activos informáticos basados en el nivel de perfección de la seguridad utilizada y con el objetivo de estimular a los funcionarios a acatar las normas pertinentes y procedimientos concernientes a la seguridad de los recursos e información. Link: http://repository.udistrital.edu.co/bitstream/11349/8323/1/Edinson%20Andres%20Chacon%20Uma%C3%B1a%20-%20William%20Andres%20Nu%C3%B1ez%20Vergara%202017.pdf

c. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Autor: Sandra Yomay Suarez Padilla.

Como dice Suarez[28], en el día a día las pymes presentan problemas ya que la mayoría de estas empresas no aportan rubros para enfrentar las fallas de seguridad, ni advertir las debilidades de sus activos informáticos, teniendo en cuenta que en la mayoría de los casos presentados se han registrado pérdidas de datos y económicas. Con base en lo anteriormente explicado y para no ser objeto de esas fallas la empresa Suárez Padilla & Cía. Ltda., siendo consciente

[28] SUAREZ, Sandra Yomay. Introducción. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.15.

de la problemática ha decidido comenzar con el proceso de elaborar un Sistema de Gestión de Seguridad Informático para poder garantizar e ingresen al sistema.

Como dice Suarez[29], en este trabajo se detallan los objetivos, alcance, sistema de gestión de seguridad de la información (SGSI) y la metodología definida, la planeación e identificación y el diseño estándar de seguridad de la información que será implementado en la empresa Suárez Padilla & Cía. Ltda.

Modelo estructurado en la norma ISO 27001:2013, el cual principia con el análisis actual del ambiente de la empresa desde el punto de vista de procedimientos críticos del movimiento documental, seguido de la realización de análisis de seguridad de los datos, visualizando las vulnerabilidades y debilidades vitales, empleando una técnica metodológica de gestión del riesgo para la mitigación de las debilidades de la seguridad informática, además de la estructuración de las actividades del tratamiento de los riesgos y promoción del documento enmarcado en el SGSI para la empresa Suárez Padilla & Cía. Ltda.

Establecer la situación real, realizar el estudio de riesgos, identificar y valorar los activos informáticos como inicio del análisis, identificar, evaluar y clasificar las

[29] SUAREZ, Sandra Yomay. Resumen. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. p.14.

debilidades, valoración de los niveles de desempeño de ISO/IEC 27002:2005 en la empresa, representación con documentos del sistema de administración de seguridad informático, establecimiento de políticas, elección de los objetivos de vigilancia de la norma ISO 27001; implantando tácticas de contingencia. Link: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3777/1/20904541.pdf

d. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca Autor: John Jairo Perafán Ruiz y Mildred Caicedo Cuchimba.

   Como dice Perafán[30], la Institución Universitaria Colegio Mayor del Cauca, es una organización en desarrollo que requiere incorporar dentro de sus normas de defensa de la información, por tal razón se implementara el análisis de vulnerabilidades a la seguridad de la información, enfocada en los activos informáticos.

   La realización de los análisis de vulnerabilidades admite efectuar una observación para evidenciar las debilidades y fortalezas para la implementación de los controles, normas y políticas de seguridad adecuadas para la

[30] PERAFAN, Jhon Jairo and CAICEDO Cuchimba Mildred. Introducción. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. 2014. p.13.

incorporación en un Sistema de Gestión de Seguridad de la Información (SGSI), facilitando el constante monitoreo mediante auditorias y la mejora continua.

Como dice Perafán[31], la Institución Universitaria Colegio Mayor del Cauca, actualmente no cuenta con un sistema de seguridad de la información, que administre las debilidades, fallas, amenazas que se ven expuestas diariamente la información en la manipulación realizada por los procesos. Igualmente los procesos, controles no están acorde a los estándares internacionales para minimizar los posibles delitos informáticos, implicando la integridad, confidencialidad y disponibilidad de la información.

La institución en la actualidad presenta varios inconvenientes con la manipulación de la información, ya que hay un aumento el volumen de los datos y los funcionarios no son conscientes de lo importante de salvaguardar los datos existentes. Conforme al crecimiento es vital crear controles y políticas que establezcan un orden en los procesos afines con la información siendo indispensable la implementación de un análisis de debilidades de la seguridad de la información, teniendo en cuenta los activos como lo especifica la metodología Magerit.

[31] PERAFAN, Jhon Jairo and CAICEDO Cuchimba Mildred. Planteamiento del Problema. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. 2014. p.14.

Para la institución la no utilización en los sistemas las recomendaciones de seguridad, en un futuro les podrían ocasionar caer en delitos informáticos ocasionando el mal funcionamiento de los servicios, por robo de información, secuestro, y otros delitos informáticos. Link: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

e. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. Autores: Andrea Marcela Pulido Chadid, Paulo César Rincón Albarracín y Óscar Mauricio Velásquez Acosta.

Como dice Pulido[32], la realización de este proyecto procede de un macroproyecto, que fue implementado en la universidad de San Buenaventura, NEOBYTE, en la cual se fragmentaron las organizaciones del sector. El proyecto se centraliza en el diseño de controles y políticas para entidades del área de transporte basándose en el diseño de redes SOHO, en Bogotá. Como dice Pulido[33], estudios de diferentes universidades en Colombia en los diversos

[32] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Introducción. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 4.
[33] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Antecedentes. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 5,6.

sectores de la producción y analizando la seguridad, políticas, controles informáticos, arrojan las siguientes conclusiones:

Para trabajar en el área de seguridad de la información, se tiene que tener como experiencia más de dos años, las redes LAN y sus dispositivos conllevan una mayor inversión, los firewall y antivirus son los más buscados para la protección de los equipos de cómputo.

Como dice Pulido[34], la seguridad de la información es la base de toda organización para la realización de todos sus procesos, teniendo como respaldo unos controles y políticas de seguridad bien formuladas, un sistema de gestión de seguridad de la información (SGSI) y objetivos adecuados a lo requerido por la organización. La mayoría de organizaciones que utilizan controles y políticas de seguridad de la información, los han implementado a un alto costo

El sector de transporte de las pequeñas y medianas empresas que tiene redes SOHO en Bogotá, se les hace necesario la implementación de adquirir una salvaguarda para la información, la cual guardan en bases de datos o entregada por medio de la red. Lo anterior soportado por un estudio técnico que instaura

[34] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Justificación. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p.9.

controles y políticas de seguridad de la información. Link: http://bibliotecadigital.usb.edu.co/bitstream/10819/2952/1/Diseno_politicas_controles_pulido_2010.pdf

4.5 MARCO CONTEXTUAL

4.5.1 Nombre de la Empresa.

Hotel y Centro de convenciones Pipatón.

4.5.2 Descripción de la Empresa.

El hotel fue construido en 1940 por el arquitecto español German Tejero de la Torre, con las mismas características de los hoteles El Prado (Barranquilla), El Caribe (Cartagena) y Bucarica (Bucaramanga). Fue inaugurado en el año 1943 constituyéndose en el centro de reuniones de la sociedad Barranqueña y sitio preferido de los viajeros, turistas y personalidades que visitan la región, desde la época de las travesías en los Buques que recorrían el país a través del majestuoso Rio Grande de la Magdalena.

Hoy por hoy el Hotel y Centro de Convenciones Pipatón está catalogado como el mejor de la ciudad. Cuenta con unas instalaciones modernas, 53 habitaciones confortablemente dotadas todas ellas con baño privado, aire acondicionado integral y otros servicios adicionales dentro los cuales se destacan: Televisión, Discado Directo Nacional e Internacional, Mini bar y servicio de Piscina.

El hotel se encuentra localizado en sitio estratégico de la ciudad, el sector del Muelle, cerca de la Avenida del Río y de la Refinería de Ecopetrol. Hemos sido escenario de la mayoría de los eventos a nivel local y nacional, no solamente por poseer un amplio salón para eventos, sino también por el confort de nuestras instalaciones y la calidad en el servicio.

a. Misión Hotel Pipatón.

El Hotel Pipatón presta excelentes servicios hoteleros a todos sus huéspedes y clientes, satisfaciendo sus necesidades y expectativas personales y empresariales; mediante el profesionalismo de su equipo de trabajo, los mejores recursos tecnológicos y de comunicación; generando bienestar a nuestros colaboradores, beneficios a la sociedad y al medio ambiente, y garantizando una efectiva rentabilidad de la operación.

b. Visión Hotel Pipatón.

Para el año 2020 el Hotel Pipatón seguirá siendo el preferido en el Magdalena Medio, reconocido en la industria por los altos estándares de calidad con que prestamos nuestros servicios, evidenciando la eficiencia y la eficacia en todos sus procesos y manteniendo un crecimiento sostenido en armonía con el medio ambiente.

c. Política de calidad:

En el Hotel y Centro de Convenciones Pipatón estamos comprometidos con la formación del personal, mejoramiento de la infraestructura y tecnología, cumplimiento de la normatividad vigente que nos permita, brindar con prontitud y amabilidad a nuestros visitantes; la comodidad, seguridad y satisfacción esperada.

4.5.3 Alcance del sistema de gestión de calidad.

El Sistema de Gestión de Calidad del Hotel y Centro de Convenciones Pipatón tiene como alcance la Prestación de Servicios de Alojamiento y realización de Eventos.

4.5.4 Objetivos de procesos.

a. Dirección

- Planificar, establecer, revisar y mejorar el Sistema de Gestión de Calidad para mantener le eficacia, adecuación y conveniencia del mismo.
- Proveer los recursos necesarios para implementar, mantener y gestionar el sistema de calidad que garantice la satisfacción de las necesidades y expectativas de los clientes del hotel.

b. Mercadeo y Ventas

- Promover los servicios del hotel orientando y asesorando a los clientes de acuerdo con sus necesidades y requerimientos, obteniendo ventas satisfactorias.

c. Recepción

- Facilitar el acceso a los servicios de alojamiento y complementarios que ofrece el hotel dando cumplimiento a los requerimientos del cliente

d. Alojamiento

- Atender las necesidades del hotel en camarería, lavandería y aseo en general haciendo uso apropiado de los recursos y tiempo asignado.

e. Eventos

- Responder al cliente por la realización del evento de acuerdo a los requerimientos pactados.

f. Gestión humana

- Mantener personal competente y comprometido en cada uno de los procesos de la organización.

g. Compras y Almacén

- Garantizar el aprovisionamiento de productos y servicios acorde con las especificaciones requeridas.

h. Mantenimiento e Infraestructura

- Atender las necesidades de mantenimiento preventivo y correctivo de la infraestructura, maquinaria y equipos del hotel haciendo uso adecuado de los recursos, tiempo asignado y garantizando la funcionalidad del servicio prestado.

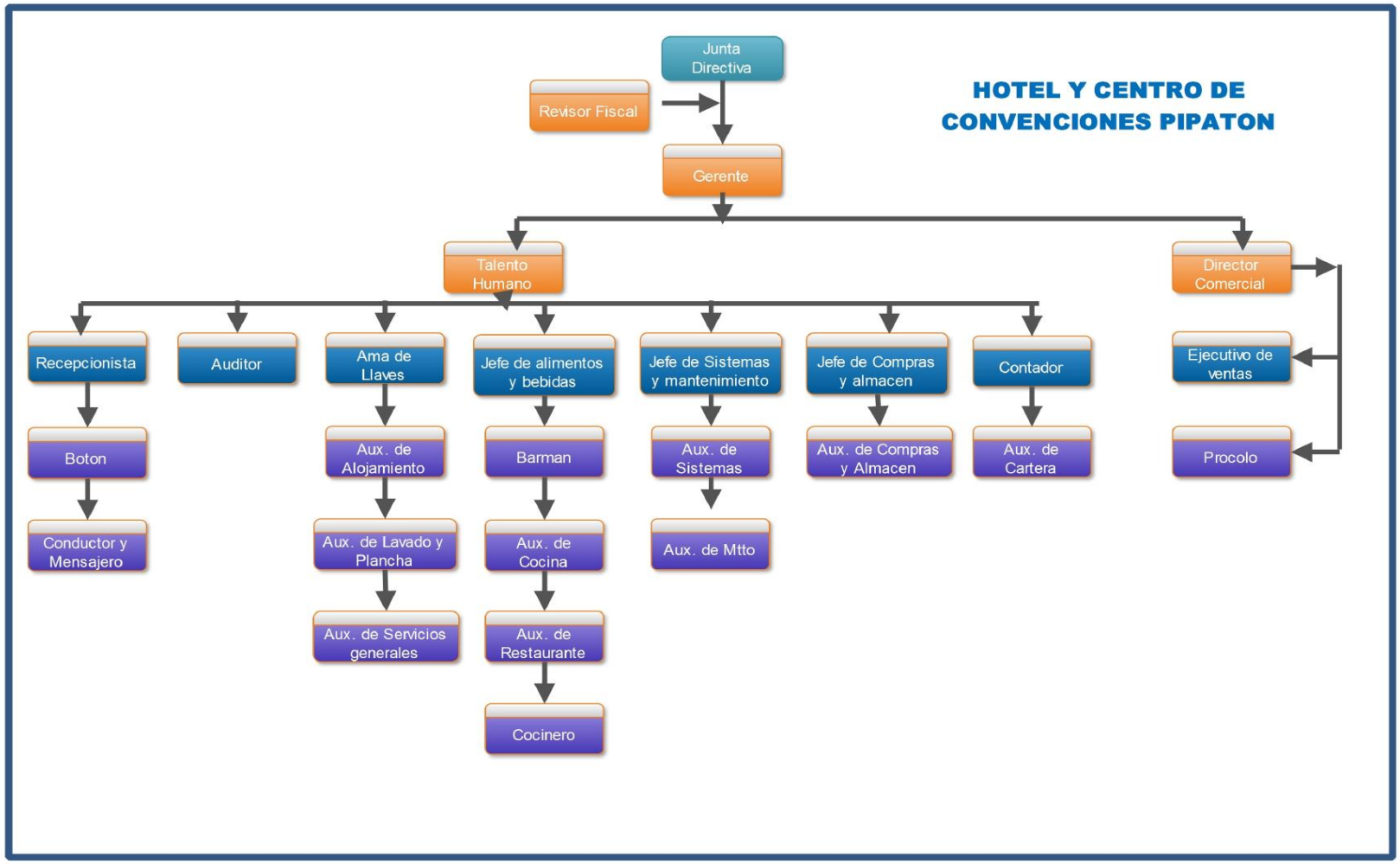
i. Mantenimiento y Mejora del Sistema

- Implementar, mantener y mejorar la eficacia del Sistema de gestión de Calidad para lograr la satisfacción del cliente.

4.5.5 La Organización.

La dirección del hotel Pipatón se compone de varias líneas de administración, en la cuidad de Bogotá, se encuentra la junta directiva y el revisor fiscal, localmente esta la gerencia y de ella dependen las demás ramas de funcionamiento de la organización, como se ilustra en la Figura No. 4, que encontramos a continuación.

Figura 4. Diagrama Organizacional



Fuente: elaboración propia

Funciones en las dependencias:

a. Gerente: El encargado de dirigir, controlar y supervisar las actividades de los funcionarios de las áreas administrativas de la empresa. Orientando la gestión de los funcionarios del área comercial. Administrando y controlando recursos para el manejo y producción de ventas.

b. Oficina Comercial: Está conformada por una funcionaria, encargada de brindar atención y realizar los eventos, ir donde los clientes determinados y posibles, dando a conocer el portafolio de servicios que ofrece el hotel.

c. Oficina Contable: Está conformada por el contador, auxiliar contable y auxiliar de cartera, encargados de realizar las compras del hotel Pipatón. Esta área tiene como función diaria conservar los datos de la contabilidad del Hotel Pipatón.

d. Oficina Talento Humanos: básicamente se constituye por un coordinador.
   - Es la encargada reemplazar a un funcionario vital, en su puesto.
   - Vigilar el buen ambiente de los funcionarios del hotel.
   - Vigilar que se cumpla con el reglamento interno de trabajo en el hotel.[35]

[35] NUÑEZ VERGARA, William y CHACÓN UMAÑA Funciones por dependencia, Edinson. En: diseño del sistema de gestión de seguridad de la información para la empresa serexcel servicios funerarios. 2017. P. 58

5. DISEÑO METODOLÓGICO

5.1 ENFOQUE METODOLÓGICO

La metodología que se va a utilizar para realizar la identificación, clasificación y valoración de los activos de información, logrando determinar las amenazas y vulnerabilidades que lograrían perturbar la seguridad de la información que manipula el Hotel Pipatón, basados en la metodología de análisis y de gestión de riesgos de los sistemas de información MAGERIT, en la que se presenta un estándar detallado en la tabla No. 5.

5.2 TIPO DE INVESTIGACIÓN

La investigación Aplicada[36] cuyo propósito es la de solucionar problemas definitivos optimizando la calidad de los procesos de las empresas, esta investigación va ligada a la investigación pura, el propósito particular de la investigación de riesgos informáticos en el hotel Pipatón, con forma de investigación se buscará la forma de solucionar las dificultades que se conocen o desconocen con respecto a los riesgos informáticos que puedan originar o estén ocurriendo en el hotel Pipatón.

[36] Perafán Ruiz, John y Caicedo Cuchimba, Mildred. Investigación Aplicada. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. 2014. p. 34.

La investigación aplicada se sustenta en datos teóricos y progreso de acciones encaminadas a establecer los potenciales orígenes del problema demostrar los descubrimientos, que con el tiempo y conforme a lo que resulto de la investigación, se planteara un modelo de actividades buscando que las soluciones sean aplicables.

Como pieza del proceso de la investigación aplicada, se proyectan acciones a un nivel general, que dimensionan y abordan la falla relacionada para ofrecer al concluir el proceso, las opciones con que cuenta organización para establecer un procedimiento de mejora, con base en los resultados obtenidos con el análisis de riesgos. A continuación, señalamos varias acciones:

- Definir en el proyecto los objetivos, estableciendo del alcance de acuerdo a la dificultad presentada.
- Analizar los orígenes de la información y la selección de información: se quiere recolectar una gran cantidad de información potencial en comparación con el actual, estudios que posean similitud con el análisis de riesgos y con la seguridad informática en el hotel.
- Concepción de métodos de trabajo y fijación de segmentos de tiempo: se crea un cronograma de actividades que instituya términos de tiempo y asignación de actividades hasta obtener el perfeccionamiento de proyecto.
- Recopilación de archivo de la empresa: es de gran valor conocer el ambiente y argumento que tiene la organización, para realizar el análisis de riesgos, revisando su estructura interna, normas, reglamentos, etc.

- Visualización del ambiente laboral y entorno: se solita elaborar una valoración de activos, infraestructura y visita a las áreas en donde se aplicarán los procesos de análisis de riesgos.
- Progreso del análisis de riesgos: con el plan de trabajo y la evaluación de los activos a valorar, se recopila información que visualice vulneraciones que se puedan presentar a futuro.
- Identificación de vulnerabilidades: se apunta en el progreso de actividades o la aplicación de dispositivos a los sistemas de información, web, redes y activos críticos estableciendo su momento actual desde la perspectiva de la seguridad de la información.
- Análisis de vulnerabilidades: obteniendo las evidencias se efectúa un resumen y la clasificación de la información, con información notable que determine los puntos de las fallas.
- Observación de los datos, descubrimientos de amenazas y generación de recomendaciones: se realiza una matriz con la valoración de los riesgos derivados, propuestas y recomendaciones.
- Exposición del informe decisivo a la administración de la organización: el proyecto se dispone la sustentación y socialización.

5.3 METODOLOGÍA PLANTEADA

La metodología a utilizar para el desarrollo de los objetivos y el alcance planteados en el proyecto y propuesta en la fase de análisis y diseño, en donde se plantea en

cada etapa varias sucesiones de actividades enfocadas a conseguir los resultados del proyecto, las que a continuación se detallan.

5.3.1 Fase 1. Análisis.

Efectuar la recopilación de la información utilizando las técnicas a continuación:

- Diálogos con los diferentes funcionarios de las áreas determinadas del Hotel Pipatón.
- Reconocimiento de la infraestructura existente del Hotel Pipatón.
- Reconocimiento de la infraestructura de redes existente, con la cual se manipula la información.

5.3.2 Fase 2. Diseño.

1. Concretar la metodología a efectuar donde se realice el análisis de riesgos de seguridad de la información en el Hotel Pipatón.
   - Clasificar e identificar los activos de información, usando el método de clasificación de los activos de la metodología MAGERIT.
   - Establecer amenazas y vulnerabilidades de los activos de información del Hotel Pipatón.
   - Detallar las debilidades de la seguridad de los datos evidenciados dentro del hotel Pipatón, empleando la metodología MAGERIT para estudio y administración de debilidades para sistemas informáticos.
   - Valorar la posibilidad de que una vulneración descubierta suceda y el impacto en el sistema de información.

- Concretar con la administración el grado de aprobación de las debilidades de seguridad de los datos.

2. Crear los controles para la seguridad del Hotel Pipatón, encargados de proteger la infraestructura tecnológica.
3. Diseñar las políticas de seguridad de la información del Hotel Pipatón.

6. ANÁLISIS DE LA SITUACIÓN ACTUAL

Las acciones programadas para la etapa de estudio se efectuaron identificando los procedimientos que se realizaran la creación de los controles, políticas y el actual momento de la seguridad en la organización, que recopila los datos diarios, su manipulación por medio de la red LAN de la empresa. Para establecer el presente estado con respecto a la seguridad informática en el Hotel Pipatón se utilizaron los métodos siguientes.

- Reconocimiento visual de la infraestructura, áreas administrativas de la empresa, software, hardware y redes utilizadas, empleando una lista de chequeo. Ver anexo C.
- determinar los puntos afectación de la seguridad de los datos, comprobando las vulnerabilidades referidas en la matriz de riesgos.

6.1 FASE 1. ANÁLISIS

6.1.1 Situación actual de la seguridad en el hotel Pipatón.

En la actualidad el hotel y centro de convenciones Pipatón, posee dos estructuras de redes, una red LAN para uso privado u administrativo de la organización y otra red LAN, para uso de los huéspedes del hotel, la cual solo se accede de modo inalámbrico. En la estructura de la red LAN administrativa posee grandes deficiencias de seguridad, tanto en la parte de hardware, software y del personal que tiene a cargo la manipulación de la información captada en el hotel.

En cuanto a los sistemas operativos utilizados en el hotel, encontramos equipos que utilizan todavía sistemas operativos antiguos como el Windows XP, en otros equipos se encuentran versiones como el Windows 7, en diferentes versiones como el Home y Profesional. En algunos portátiles se encuentran que funcionan con sistemas operativos como el Windows 10, sin licencias.

En cuanto al uso de antivirus en los diferentes equipos de mesa, portátiles se encuentran en el inventario del hotel Pipatón, se tiene que solo el 10% de los equipos poseen un antivirus actualizado, pero no activado legalmente, como se hacía en años anteriores, que se compraba el paquete con licencias para varios equipos. El resto de equipos funciona con antivirus desactualizados o de diferentes orígenes.

Las aplicaciones de manejo administrativo del hotel Pipatón, como el Office, se manejan varias versiones desde la versión 2007 hasta la 2013, sin ningún tipo de licenciamiento. Otras herramientas como PDF no se tienen un estándar en la versión utilizada. En cuanto al almacenamiento de la información se cuenta con un servidor HP Proliant, con sistema operativo Windows server 2008 licenciado y manejador de Bases de datos SQL Server 2008 licenciado, con antivirus sin licenciamiento, en igual condiciones que los demás equipos, diferentes aplicaciones y herramientas administrativas sin licenciamiento.

En cuanto a los computadores utilizado por el hotel en su mayoría son equipos de mesa, y con tecnología antigua. La red LAN es una estructura de topología en estrella, con cables de red UTP cat. 5, sin ningún tipo de organización o cableado estructurado. Los puntos de red no son certificados. El medio de conexión utilizado por la red para el acceso a internet, es un Router, el cual administra la red y proporciona el servicio de internet a cada uno de los terminales existentes, por medio de DHCP, en cualquier área de la organización, sin ningún tipo de dispositivos de seguridad, cortafuegos o zonas DMZ.

El personal no tiene un nivel de capacitación en seguridad informática, e instalan aplicaciones descargadas de internet para la realización de algún procedimiento, como la utilización de software para el manejo de PDF, antivirus, programas para el escaneo de documentación del hotel, navegadores, aplicaciones para el uso de redes sociales y software para manipulación de dispositivos móviles. Por otro lado, facilitan los equipos informáticos de uso exclusivo del hotel, a huéspedes, sin tener en cuenta que al manipular información pueden introducir cualquier tipo de infección al terminal usado y desde ahí a los demás equipos, por medio de la red principal.

En la parte de internet se manejan diferentes plataformas para la realización de reservas, pagos y demás acciones correspondientes a hotel, sin ningún tipo de control por parte de la gerencia del hotel. El personal de recepción, tiene el acceso a las aplicaciones y páginas web, teniendo el conocimiento de usuarios y claves de seguridad, que solo deberían ser de dominio de funcionarios de perfil administrativo.

El hotel Pipatón no cuenta con una oficina o un sitio donde esté ubicado el servidor, en la actualidad este equipo reposa en una oficina donde se encuentra el área contable y de cartera, y un escritorio para el área de sistemas, donde se encuentra ubicado el terminal asignado al área y el servidor. Siendo esta oficina de fácil acceso al personal del hotel, donde en cualquier momento pueden causar un daño al servidor, por algún tipo de manipulación de líquidos, o golpes.

En la actualidad, no se cuenta con un tipo de respaldo energía, se trabaja con estabilizadores y UPS deterioradas que no sostienen carga y funcionan como reguladores normales, en alguna ocasión se implementaron unos puntos eléctricos independientes del circuito normal, alimentados por una UPS de gran capacidad, para sostenimiento de la red en más de una hora, pero por motivos de daños y austeridad no se le realizo un mantenimiento correctivo.

En resumen, en el hotel Pipatón, no cuenta con controles y unas políticas claras para la seguridad de la información dentro de la red LAN principal, poniendo en riesgo el activo principal del hotel y quedando potencialmente a meced de ataques que podrían generarle muchos inconvenientes y en el peor de los casos caer en manos de delincuentes informáticos teniendo que pagar un precio muy caro por no tener los mínimos controles de seguridad estándar para la preservación de la información.

6.1.2 Activos.

Un sistema de gestión de seguridad de la información, utiliza los activos de la información como recursos, para el funcionamiento de las organizaciones y conseguir los objetivos propuestos en la dirección. Los activos están agrupados de forma directa o indirectamente, con las demás entidades. Un proyecto tiene como objetivo de seguridad vigilar la seguridad de los activos de información que forman el dominio en el proyecto.

Los pasos iniciales que debe alcanzar la organización para acomodarse a la norma Magerit, es la de realizar un inventario detallado de los activos de la información. Se contemplarán los activos de información que representan valores para la organización quedando incluidos en el alcance del SGSI. Para un funcionario principiante al inicio puede ser aburridor, la cantidad de activos que relacionan. Por esta razón se resuelve empezar a clasificar los activos de alguna manera. Entre las diferentes maneras que tenemos se puede optar por la utilizada por los especialistas, que al parecer es la manera más correcta.[37]

Los recursos de información que son relacionados, son vitales para que la organización se mueva diariamente y de forma correcta alcanzando los objetivos

---

[37] ISOTOOLS EXCELLENCE. SGSI, Blog especializado en Sistemas de Gestión de Seguridad de la Información, 23 febrero, 2017, [En línea]. [Consultado 14 de noviembre, 2018]. Disponible en http://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

planteados por la dirección. Se detallaron los procedimientos elaborados en el hotel Pipatón, en todas las áreas que ayudan a la generación de los servicios prestados. El Hotel Pipatón en la actualidad tiene una serie de procesos, los cuales asumen un compromiso en el proceso de calidad ISO 9001, como se ve a continuación en la Tabla No. 1.

Tabla 1. Identificación de los Procesos

Procesos	Descripción	Frecuencia (Diario/Semanal Mensual)	Responsable
Recepción	Atención de huéspedes y clientes dando atención en la realización de procesos que tienen que ver con los servicios ofrecidos por el Hotel.	diario	Recepcionistas Auditores
Restaurante	Atención de los clientes y huéspedes	diario	Meseros
Comercial	Información sobre el portafolio de servicios	diario	Coordinara comercial
Gestión de Talento Humano	Realización de los documentos legales laborales y derechos, deberes y beneficios del trabajador	diario	Jefa de recurso humano
Área contable	Control de pagos, contabilidad, proveedores, nomina, comparas	diario	Contador Aux contable Aux de cartera
Sistemas	Soporte primario en manejo SW Hotel. Capacitación en las herramientas SW. Optima utilización de los recursos informáticos ofrecidos por el hotel.	diario	Ing. De sistemas

Fuente: elaboración propia

Cada proceso dependiendo su responsabilidad en el hotel maneja una determinada aplicación, generando ingreso de información a nuestros sistemas de información, como se muestra en la Tabla 2.

Tabla 2. Aplicaciones de apoyo en los procesos

Nombre	Concepto	Critico (*)	Equipos de computo	Numero Equipos en las áreas
SQL SERVER	SQL SERVER para el almacenamiento de la información de los Huéspedes y clientes del hotel.	3	SERVIDOR	1
ZEUS TECNOLOGIA FRONT – POS	Aplicación Visual fox y NET encargado de recopilar los datos de los huéspedes y clientes del hotel Pipatón.	3	SERVIDOR	12
ZEUS TECNOLOGIA BACK	Aplicación en red desarrollada en Visual fox y NET en done se puede realizar la manipulación de los datos del hotel Pipatón.	3	SERVIDOR	12

Fuente: elaboración propia

De igual manera el hardware existente en el hotel Pipatón, se tiene debidamente inventariado y registrado en hojas de vida, como se solicita en el sistema de calidad, tal como se evidencia en la Tabla 3.

Tabla 3. Recursos de Hardware Hotel Pipatón

Activos informáticos hotel Pipatón				
Numero	Nombre	Modelo	Cantidad.	Descripción
1	CPU	Desktop	8	
2	CPU Todo en uno	Desktop	2	Sistemas y piscina
3	CPU	Desktop	1	Servidor
4	Monitores	LCD	5	19”
5	Monitores	LCD	3	17”
6	Monitores	LED	1	Servidor
7	Teclados		9	Genius
8	Mouse		10	Genius
9	Teclados		2	HP Y COMPAQ
10	Mouse		1	Geway
11	Impresoras POS	270 agp	2	Samsung
12	Impresora	Laser	1	HP Laserjet
13	Impresora	Laser	1	Multifuncional m1132mpf
14	Impresora	LX300+	1	Matrix de punto
15	Impresora	Laser	1	Fotocopiadora RICOH
16	Video Beam	EPSON	1	
17	Swicht	8 puertos	2	Encore
18	Swicht	16 puertos	2	TP LINK

Fuente: elaboración propia

Tabla 3. (Continuación)

Activos informáticos hotel Pipatón				
Numero	Nombre	Modelo	Cantidad.	Descripción
19	Router Inalámbricos		2	TP LINK / QPCOM
20	Access Point		10	D LINK
21	Disco Duro	Externo	1	500 GB
22	UPS	TITAN	1	6000 WATT / 6 K

Fuente: elaboración propia

Los activos anteriormente inventariados, se tienen clasificados en grupos de activos existentes en la organización, con su tipo de activos correspondiente y descripción del mismo, tal como se observa en la Tabla 4.

Tabla 4. Identificación de activos

Clasificación del Activo	Tipo de Activo	Nombre del Activo	Descripción
Equipamiento auxiliar	[AUX]	[UPS]	1 UPS de 6 k, alimentación eléctrica para el rack de comunicaciones y servidor y terminales hotel
Redes de comunicación	[COM]	[COM_LAN]	1 red LAN ADMINISTRATIVA 1 red LAN WIFI Huéspedes / Clientes
Equipos informáticos	[HW]	[HW_FW]	2 Router
Equipos informáticos	[HW]	[HW_FW]	10 Access Point – Lan WI FI
Equipos informáticos	[HW]	[HW_FW]	4 Swicht
Soportes de información	[MEDIA]	[MEDIA_DISK]	1 discos Duros extraíbles
Equipos informáticos	[HW]	[HW_SERV] [OS_WIN_2008]	1 servidor: contiene las BD SW Hotelero. SQL SERVER 2008
Equipos informáticos	[HW]	[HW_CPU] TODO EN UNO [OS_WIN_7]	2 CPU: contiene las diferentes aplicaciones del software Hotelero.
Equipos informáticos	[HW]	[HW_CPU] DESKTOP [OS_WIN_7]	8 CPU: contiene las diferentes aplicaciones del software Hotelero.

Fuente: elaboración propia

Tabla 4. (Continuación)

Clasificación del Activo	Tipo de Activo	Nombre del Activo	Descripción
Equipos informáticos	[HW]	[HW_MONITOR] LCD	5 LCD 19”:
Equipos informáticos	[HW]	[HW_MONITOR] LCD	3 LCD 17”:
Equipos informáticos	[HW]	[HW_MONITOR] LED	1 LED 20” Equipo Servidor:
Equipos informáticos	[HW]	[HW_IMPRESORAS] POS	2 impresoras: restaurante y piscina Bixolon – Samsung
Equipos informáticos	[HW]	[HW_IMPRESORAS] LASER	3 impresoras: Contabilidad, recepción. HP – RICOH
Equipos informáticos	[HW]	[HW_IMPRESORAS] MATRIZ DE PUNTO	1 impresoras: Contabilidad. EPSON
Equipos informáticos	[HW]	[HW_VIDEO BEAM]	1 video Beam: Salon Real. EPSON
Equipos informáticos	[HW]	[HW_TECLADOS]	11 teclados
Equipos informáticos	[HW]	[HW_MOUSE]	11 Mouse
Datos	[D]	[D_CLIENTES]	Archivos que contienen la información de los clientes
Datos	[D]	[D_USUARIOS]	Datos de ingreso a sistemas informáticos
Aplicaciones Informáticas	[SW]	[OS_WIN_7-PRO]	10 sistema Operativo Windows 7: Terminales del Hotel
Aplicaciones Informáticas	[SW]	[OS_WIN_SERVER 2008 SP 1]	1 servidor del Hotel
Aplicaciones Informáticas	[SW]	[SW HOTELERO]	11 aplicaciones Hoteleras: Terminales del Hotel

Fuente: elaboración propia

Tabla 4. (Continuación)

Clasificación del Activo	Tipo de Activo	Nombre del Activo	Descripción
Aplicaciones Informáticas	[SW]	[SW ANTIVIRUS]	11 terminales del Hotel
Personas	[P]	[ADM]	4 áreas: Gerencia – Área contable – Comercial – Sistemas
Personas	[P]	[OPE]	3 áreas: Recepción, Restaurante, Piscina.
Instalaciones	[L]	[LOCAL]	Infraestructura del hotel

Fuente: elaboración propia

6.2 FASE 2. DISEÑO

En esta fase se concretaron varias actividades planteadas que permitieron la realización del análisis de riesgo de seguridad de la información del Hotel Pipatón, construyendo una propuesta para gestión y la manipulación de los riesgos de seguridad de la información permitiendo su control y mitigación, siendo la organización libre de efectuar su ejecución. Para alcanzar el avance de los objetivos, se tendrán en cuanta las tareas a mencionar:

- Clasificar e identificar los activos de tecnología del hotel Pipatón, usando el método de clasificación definido en la metodología MAGERIT- versión 3.0 Libro II – Catalogo de elementos.

- El hotel Pipatón, para efectuar el pertinente estudio de seguridad de los datos utilizo la “metodología de Análisis y Gestión de Riesgos de los sistemas de información MAGERIT ver. 3.0 definida en el libro I – Método”[38].
- Con la metodología seleccionada se realizó el análisis de riesgos de seguridad de la información.
- Evaluar y valorar las debilidades de la seguridad de los datos palabras de la posibilidad de que un evento ocurra y su impacto.
- Diseñar el plan de tratamiento de riesgos encaminado a proteger la seguridad de la información de los activos del Hotel Pipatón.
- Establecer controles de seguridad de la información para el hotel Pipatón.
- Establecer políticas de seguridad de la información para el hotel Pipatón.

A continuación, se detallan los principales aspectos para establecer para cada una acción determinada en la fase de diseño.

6.2.1 Clasificación e Identificación de los Activos.

La clasificación e identificación de los activos se efectuó en compañía de los funcionarios líderes de cada área del Hotel Pipatón, usando la metodología MAGERIT, que plantea el estándar de categorización descrito a continuación.

[38] MAGERIT. Método de análisis de riesgos. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid, octubre de 2012. p. 22.

Tabla 5. Clasificación de los activos según metodología MAGERIT

Activos		
Numero	Categoría	Descripción
1	Datos e información	Principal activo que facilita a la empresa ofrecer los servicios. La manera de guardar la puede realizar física o digitalizada, como copias de seguridad, etc.
2	Servicios	Se necesitan para poder organizar el sistema, servicios prestados que satisfacen la necesidad de los clientes, correo electrónico, acceso remoto, etc.
3	Aplicaciones Informáticas (SW)	Que admiten manejar los datos, Se identifican porque tramitan, observan y transforman los datos. Tales como, programas de ofimáticas, sistemas operativos, antivirus, etc.
4	Equipamiento Informático	Que permiten hospedar datos, aplicaciones y servicios. Responsables del procesamiento o transmisión de datos. Se clasifican todo lo relacionado con equipos de cómputo, aparatos de la red.
5	Redes de comunicaciones	Que permiten intercambiar datos, Se concentran en los mecanismos de transporte que llevan la información a distintos lugares. Corresponden la red LAN, inalámbricas, Internet, etc.
6	Soportes de información	Que son dispositivos de almacenamiento de datos, dispositivos físicos que admiten almacenar información de manera permanente, como memorias, discos duros y DVD.
7	Equipamiento auxiliar	Complementa el material de sistemas, se utiliza de soporte a los S.I., sin tener un tipo de relación con los datos, como dispositivos de energía, UPS, aire acondicionado, cables, etc.
8	Instalaciones	Que acogen equipos informáticos y de comunicaciones, lugares donde se alojan S.I. y comunicaciones. Ej. Edificios, oficinas.
9	Personal	Que explotan u operan todos los elementos anteriormente citados. Personal relacionado con los S.I., como funcionarios de la empresa y externos, etc.

Fuente: MAGERIT. Método de análisis de riesgos. En: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. España: Min. Hacienda y Administraciones Públicas, 2012. p. 22.

Ahora se clasificarán los activos enumerados en el sistema de información, clasificados e identificados conforme a la metodología definida.

Tabla 6. Inventario de activos

Activo			
Nombre	Descripción	Categoría	Ubicación
Red LAN	Red LAN Hotel Pipatón	Red de comunicación	• Infraestructura de la organización
Red WIFI	Red Wifi utilizada por los clientes para acceder a Internet	Red de comunicación	• Infraestructura de la organización
Sistemas operativos	Software para la manipulación de los diferentes dispositivos	Aplicaciones Informáticas	• Dispositivos de cómputo
Antivirus	SW que salvaguarda el sistema de información del código malicioso (Malware)	Aplicaciones Informáticas	• Equipos de cómputo
Aplicativos – Ejecutable	Ejecutables de Aplicaciones.	Aplicaciones Informáticas	• Equipos de cómputo
Sistemas de gestión de bases de datos	Aplicativo para la manipulación de la base de datos	Aplicaciones Informáticas	• Equipos de cómputo (servidor)
Servidores, computadores, portátiles, Impresoras, fotocopiadoras	Equipos utilizados en los procesos diarios del Hotel Pipatón.	Equipos informáticos	• Infraestructura de la organización
Mecanismos de almacenamiento externos	Dispositivos externos de almacenamiento para datos	Soportes de datos	• oficinas administrativas • Lugar donde este el responsable del activo Ej.: residencia.
Talento Humano Hotel Pipatón.	Personal a cargo de manipulación y equipos de la organización.	Personas	• Infraestructura de la organización

Fuente: elaboración propia

6.2.2 Metodología para el analizar los riesgos.

El objetivo para lograr la estructuración del Hotel Pipatón, se especifica la forma metodológica para implementar siguiendo las pautas efectuando el estudio de los peligros de seguridad de los datos a los que se expone actualmente el sistema de información en la red LAN. Teniendo en cuanta los métodos de MAGERIT con respecto al estudio y administración de las debilidades para los sistemas de información, se establecen algunas acciones a continuación.

La teoría metodológica propone las siguientes acciones:

- Identificación de amenazas y vulnerabilidades en los activos vinculados con los datos, y de igual forma su sensación pertinente.
- establecer las debilidades de la seguridad.
- Determinar la ponderación de la posibilidad del suceso de las debilidades y la sensación generado en el hotel Pipatón, la realización de la debilidad.
- Elaboración de la matriz de debilidades esenciales.
- Elaborar las tácticas de procedimiento y administración de las debilidades de seguridad de los datos.

Ahora se demostrará el progreso de las actividades descritas.

6.2.2.1 Determinar amenazas y vulnerabilidades.

Conforme a los activos elegidos para la realización del estudio de las debilidades especificados como lo muestra la Tabla No.6, efectuando la individualización de amenazas, debilidades y probables resultados por realización con alguna vulneración a una debilidad desde la recopilación de los datos en la etapa de estudio. A continuación, se detallan los activos del hotel Pipatón, analizando las causas como las vulnerabilidades, amenazas y el impacto que tiene sobre la organización, como se detalla en la Tabla No. 7.

Tabla 7. Amenazas y debilidades de los activos objeto del estudio

Activos analizados	Orígenes		Impacto
	Debilidades	Amenazas	
Red LAN y Red WIFI	• En la actualidad no hay una política de seguridad de la información. • Carencia de personal que administre las redes existentes con perspectivas de protección de los datos. • Carencias en las configuraciones de seguridad de la red WIFI. • En la actualidad no se cuenta con listados de funcionarios que pueden ingresar a las aplicaciones y su estado. • Carencia de procedimientos que constituyan los procesos para permitir o no permitir el ingreso o no las cuentas de usuario. • No se tiene un procedimiento determinado para la gestión y administración en el Hotel.	•funcionarios pueden proceder a usar usuarios de ingreso y claves activas de individuos no registrados por el Hotel, robando datos vitales. •Perdida de datos por ingreso de funcionarios sin acreditados a la red del Hotel. •funcionarios realizan procesos de falsificación de identidad para ingresar a las aplicaciones suministradas a través de la red del Hotel.	• Pérdida de prestigio de la imagen del Hotel Pipatón, por información no autorizada por parte del personal. • Colapso de la red ocasionando caídas, retrasos en los servicios ofrecidos por la organización. • Alteración de la integridad, confiabilidad de los datos del hotel Pipatón, formando un impacto negativo en el futuro de la organización. •Divulgación sin autorización de la información del Hotel Pipatón, a la competencia, afectando la economía de la organización.

Fuente: elaboración propia

Tabla 7. (Continuación)

Activos analizados	Orígenes		Impacto
	Debilidades	Amenazas	
Servidores, computadores, portátiles, Impresoras, fotocopiadoras	• Falta en la programación de mantenimiento preventivo en la red LAN y WIFI, para obtener un mejor desempeño de los equipos de cómputo, protegiendo los datos. • El antivirus emplazado en los servidores no se encuentra activo ni actualizado. • Los archivos de copia de seguridad están ubicados en los mismos servidores. • Actualmente no se efectúa un seguimiento de procesos y listados de logs permitiendo descubrir debilidades de seguridad. • No se tienen configuraciones de seguridad en los equipos de cómputo y servidores. • El sistema operativo de los diferentes equipos de cómputo, no se encuentra licenciado ni actualizado.	•Fallas mal intencionadas ocasionadas por funcionarios del hotel Pipatón. • Manejo de los datos y aplicaciones residentes en los equipos de cómputo por funcionarios con perfil administrativo. • Daños en la infraestructura ocasionados por situaciones climatológicas inadecuadas. • Mala manipulación interior o exterior sobre equipos de cómputo teniendo daños temporales o permanentes de los datos.	•Publicidad de información no autorizada por terceros. •Perdida de los datos que puede conllevar a la afectación de la organización. • Manejo de configuración de los procesos de red del Hotel Pipatón sin autorización perjudicando la empresa. • Perdida de información vital para el Hotel Pipatón perturbando desarrollo de los procesos. .

Fuente: elaboración propia

Tabla 7. (Continuación)

Activos analizados	Orígenes		Impacto
	Debilidades	Amenazas	
Antivirus	• En la actualidad no existe antivirus activados y actualizados, con la empresa fabricante del antivirus.	• Retención de información causada por una aplicación ramsomware. • Daños de la información causados por virus informáticos. • Manipulación de información por acceso no autorizado de terceros por uso de malware. • Pérdida de información formada por código malicioso. • Perdida de los equipos de cómputo debido a aplicaciones dañinas.	• Robo de información confidencial del Hotel Pipatón, afectando la continuidad del negocio. • Afectación de la economía del Hotel Pipatón, causados por daños parcial y/o total de la información. • Afectación del hotel Pipatón por retención de la información producido por código malicioso.
Aplicativos - Ejecutable	• Las aplicaciones son débiles en cuanto a las claves originado por: No se restringe el número mínimo de letras para la clave. El registro solo guarda dos claves últimas claves, no pide la mezcla de letras. • El software no tiene un parámetro de seguridad con una periodicidad de renovación y cambio de clave por parte del usuario. • Carencia de configuraciones de seguridad que permita pedir el cambio de la clave de un usuario nuevo.	• Cambio por terceros sin autorización del archivo de configuración, en cliente servidor modificando la aplicación. • Falsificación de identidad, sustracción de datos adjunta en el sistema de información. • Asaltos internos y/o externos capturando usuarios y claves de acceso válidos.	• Perdida en los ingresos económicos por divulgación de las vulnerabilidades de seguridad. • Detrimento de clientes por hurto y divulgación sin autorizada de información clasificada. . • Organización desprestigiada por la explotación de las vulnerabilidades por un tercero.

Fuente: elaboración propia

Tabla 7. (Continuación)

Activos analizados	Orígenes		Impacto
	Debilidades	Amenazas	
Aplicativos - Ejecutable	• Las aplicaciones trabaja con cliente servidor, la instalación crea un registro para configurar y cambiar el proceder de los aplicativos.		
Medios de almacenamiento	• En las unidades de almacenamiento no se pueden efectuar procedimientos de eliminación confiables de datos guardados. • Carencia de estructuras de defensa para mecanismos de almacenamiento exteriores. • No se cuenta con mecanismos de cifrado de datos en estos dispositivos de almacenamiento.	•Pérdida de información confidencial del hotel Pipatón, por robo de discos externos de almacenamiento.	• Perdida de datos privados, causando perjuicios a la empresa. • Circulación por personal externo de los datos del Hotel Pipatón, causando problemas legales y de mala reputación.
Talento Humano Hotel Pipatón.	• falta de directrices claras de seguridad, orientados a funcionarios por carencia de controles y política de seguridad de la información. • Carencia de sensibilización a los funcionarios sobre el valor de su rol en la seguridad de la información. • Inexistencia de capacitación a funcionarios en contenidos relacionados con la manipulación segura del software. • Confianza excesiva de los funcionarios en el entorno de trabajo.	•funcionario insatisfecho del Hotel Pipatón. •Exempleado del hotel Pipatón, con accesos y privilegios habilitados para ingreso a la red física. • Personal mal intencionado, interesados en promover ataques que produzcan indisponibilidad del servicio ofrecido.	• Perdida de datos privados llegando a manos de empresas del mismo sector, para ofrecer excelentes propuestas a clientes del Hotel Pipatón. • Divulgación no autorizada de información personal de clientes, ocasionando problemas legales al hotel Pipatón. • Desprestigio del Hotel Pipatón, a causa de la divulgación de información.

Fuente: elaboración propia

6.2.2.2 Determinar las debilidades de la seguridad.

Conforme con caracterización de amenazas y debilidades de los activos objeto del estudio de riesgo, visualizando las debilidades de seguridad de los activos de información a los que se tienen bajo en el Hotel Pipatón. A continuación, se de tallan los diferentes riesgos de seguridad de cada uno de los activos del Hotel, como se visualiza en la Tabla No. 8.

Tabla 8. Riesgos en la seguridad de los datos.

Activos analizados	Debilidades de seguridad
Red LAN y Red WIFI	**R1** - La carencia de controles y políticas para implementación de claves de ingreso a medios de tecnología del hotel, conllevan a la pérdida de información.
	R2 – Deficiencias de diseño e implementación en la red del Hotel Pipatón, causando que no estén disponibles los servicios y la información.
Servidores, computadores, portátiles, Impresoras, fotocopiadoras	**R3** – Robo de datos del hotel Pipatón, por la carencia de procedimientos que formen directrices y buenos hábitos para seguridad de la información, realizando copias de seguridad.
	R4 - Perdida de la confiabilidad e integridad de la información por causa un mal uso de controles de acceso y gestión de identidades.
	R5 – Software desactualizados en la infraestructura tecnológica produciendo perdida de los datos y afectan el servicio.
	R6 – Demoras para la recuperación de los datos de los equipos de cómputo por el deterioro motivado por fallas en los mantenimientos preventivos.
	R7 – Demoras para la recuperación de los datos en los equipos de cómputo por el deterioro motivado por el abandono de configuraciones de seguridad en los equipos de cómputo.
Antivirus	**R8** – Pérdida de información motivada por la no actualización o falta del antivirus.
	R9 – Hardware dañados inducidos por virus o códigos maliciosos o falta del antivirus.
	R10 – Afectaciones operacionales con la red LAN en hotel Pipatón, por la presencia de malware.

Fuente: elaboración propia

Tabla 8. (Continuación)

Activos analizados	Debilidades de seguridad
Aplicativos – Ejecutable	**R11** – deterioro de los datos sin autorización por personal externo por excesos de autorizaciones en el perfil.
	R12 – Eliminación de datos guardados en las bases de información como consecuencia de la falta de reglas de seguridad para las aplicaciones que especifiquen renovación en las claves por parte de los usuarios.
	R13 – Eliminación de privacidad de los datos por carencia en paradigmas para protección del aplicativo que pidan renovación de claves a funcionarios nuevos.
	R14 – Eliminación de los datos por mala manipulación de protocolos inciertos manejados en la divulgación del sitio web.
Medios de almacenamiento	**R15** – Pérdida de clientes hotel Pipatón, por falta elementos tecnológicos de cifrado de información sobre almacenamiento electrónico.
Talento Humano Hotel Pipatón.	**R16** - Falta de directrices claras de seguridad, orientados a funcionarios por carencia de controles y política de seguridad de la información

Fuente: elaboración propia

6.2.2.3 Valoraciones de probabilidad e impacto en los riesgos.

Con el inicio de las valoraciones de las debilidades es fundamental que se ejecute de forma preliminar el pertinente análisis de los hallazgos descubiertos en cada ambiente descrito que afectaron la seguridad de los datos, posibilitando que suceda la falla y el impacto ocasionado a la empresa cuando se efectué la debilidad. Unidos acordemente con la dirección del hotel Pipatón fueron establecidos los niveles a utilizar para la realización de la valoración de los riesgos detallados en la tabla No. 8.

A continuación de describen la probabilidad, frecuencia y valores de que algo ocurra en un determinado tiempo, como se detalla en la Figura No. 5.

Figura 5. Valoración de la probabilidad de ocurrencia en el tiempo

PROBABILIDAD	FRECUENCIA DE OCURRENCIA	VALOR
Muy Bajo	Por lo menos una vez cada año	1
Bajo	Por lo menos una vez cada semestre	2
Medio	Por lo menos una vez cada trimestre	3
Alto	Por lo menos una vez cada mes	4
Muy Alto	Por lo menos una vez cada quince días	5

Fuente: MAGERIT. Método de análisis de riesgos. En: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. España: Min. Hacienda y Administraciones Públicas, 2012. p. 27.

La siguiente ecuación se deriva de valorar los riesgos en términos de posibilidad e impacto de que el riesgo ocurra.

$$Riesgo\ Inherente = \textbf{Impacto} * \textbf{Probabilidad}$$

En la Figura No. 6 observamos la valoración del riesgo con sus respectivos rangos de calificación.

Figura 6. Ponderación y valoración del riesgo

VALORACIÓN DEL RIESGO	CALIFICACIÓN
Muy bajo	1 – 2
Bajo	3 - 4
Medio	5 - 9
Alto	10 - 15
Critico	16 - 25

Fuente: MAGERIT. Método de análisis de riesgos. En: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. España: Min. Hacienda y Administraciones Públicas, 2012. p. 28.

Con la valoración determinada para las debilidades esenciales en la posibilidad de que algo ocurra y su impacto, logrando los efectos descritos en la tabla No. 9.

Tabla 9. Valoración de las debilidades relacionadas con los activos

Activos analizados	Debilidades de seguridad	Riesgo valorado			
		Probabilidad	Impacto	Valoración	Grado de la debilidad
Red LAN y Red WIFI	**R1** - La carencia de controles y políticas para implementación de claves de ingreso a medios de tecnología del hotel, conllevan a la pérdida de información.	2	5	10	Alto
	R2 – Deficiencias de diseño e implementación en la red del Hotel Pipatón, causando que no estén disponibles los servicios y la información.	2	3	6	Medio
Servidores, computadores, portátiles, Impresoras, fotocopiadoras	**R3** – Robo de datos del hotel Pipatón, por la carencia de procedimientos que formen directrices y buenos hábitos para seguridad de la información, realizando copias de seguridad.	3	4	12	Alto
	R4 - Perdida de la confiabilidad e integridad de la información por causa un mal uso de controles de acceso y gestión de identidades.	3	4	12	Alto
	R5 – Software desactualizados en la infraestructura tecnológica produciendo perdida de los datos y afectan el servicio.	3	4	12	Alto
	R6 – Demoras para la recuperación de los datos de los equipos de cómputo por el deterioro motivado por fallas en los mantenimientos preventivos.	2	4	8	Medio
	R7 – Demoras para la recuperación de los datos en los equipos de cómputo por el deterioro motivado por el abandono de configuraciones de seguridad en los equipos de cómputo.	1	2	2	Muy Bajo
Antivirus	**R8** – Pérdida de información motivada por la no actualización o falta del antivirus.	2	4	8	Medio
	R9 – Hardware dañados inducidos por virus o códigos maliciosos o falta del antivirus.	2	3	6	Medio
	R10 – Afectaciones operacionales con la red LAN en hotel Pipatón, por la presencia de malware.	3	4	12	Alto
Aplicativos - Ejecutable	**R11** – deterioro de los datos sin autorización por personal externo por excesos de autorizaciones en el perfil.	2	4	8	Medio
	R12 – Eliminación de datos guardados en las bases de información como consecuencia de la falta de reglas de seguridad para las aplicaciones que especifiquen renovación en las claves por parte de los usuarios.	2	4	8	Medio

Fuente: elaboración propia

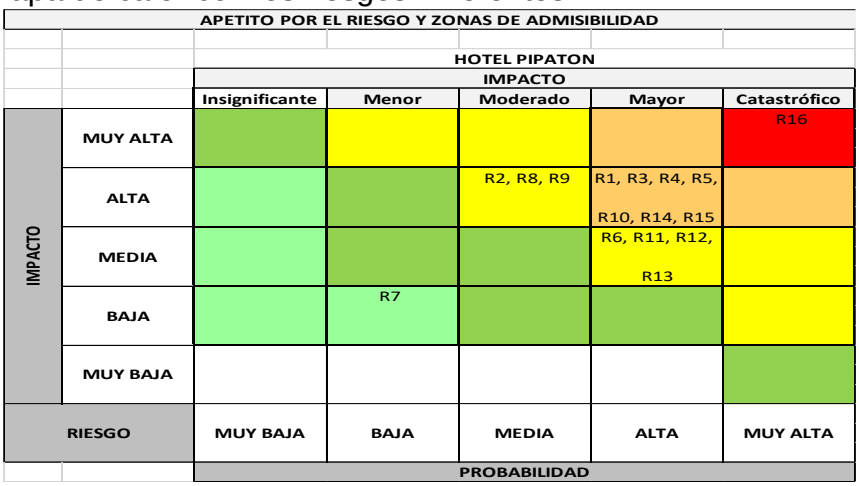
Tabla 9. (Continuación)

Activos analizados	Debilidades de seguridad	Riesgo valorado			
		Probabilidad	Impacto	Valoración	Grado de la debilidad
Aplicativos - Ejecutable	**R13** – Eliminación de privacidad de los datos por carencia en paradigmas para protección del aplicativo que pidan renovación de claves a funcionarios nuevos.	2	4	8	Medio
	R14 – Eliminación de los datos por mala manipulación de protocolos inciertos manejados en la divulgación del sitio web.	4	3	12	Alto
Medios de almacenamiento	**R15** – Pérdida de clientes hotel Pipatón, por falta elementos tecnológicos de cifrado de información sobre almacenamiento electrónico.	3	5	15	Alto
Talento Humano Hotel Pipatón.	**R16** - Falta de directrices claras de seguridad, orientados a funcionarios por carencia de controles y política de seguridad de la información	4	4	16	Critico

Fuente: elaboración propia

Para el hotel Pipatón poder valorar las debilidades en conocimientos de la posibilidad de que algo suceda y el impacto se logró construcción del mapa de calor con las debilidades de la seguridad de los datos encontrados en el actual estudio, logrando el resultado que se muestra en la Figura No. 7.

Figura 7. Mapa de calor con los riesgos inherentes



Fuente: elaboración propia

6.2.3 Método de manejo y administración de riesgos.

Con base en el plan metodológico seleccionado a continuación detallaran el proceso utilizado concretando el método de manejo y administración de vinculados con los activos informáticos, cuyo alcance será el de crear y plasmar las mejoras permitiendo hacer un control para minimizar las vulnerabilidades de la seguridad de los activos informáticos del hotel Pipatón expuestos. Se debe subrayar que actualmente el hotel Pipatón no cuenta con unos controles que minimicen los riesgos de seguridad de la información, como los mencionados anteriormente.

6.2.3.1 Método del manejo del Riesgo.

Después de la evaluación de las debilidades establecidas y definidos por la tabla No. 9, se precisa la planificación del manejo de los riesgos de acuerdo a los paradigmas del Hotel Pipatón y la calidad de la seguridad de la información para la prolongación del negocio, aprobando así que se establezcan acciones para efectuar en cada riesgo reconocido. Seguidamente en la Tabla No. 10, se detallan medidas para aplicar en el método de manejo del riesgo.

Tabla 10. Diseño del método del riesgo

Numero.	Método del manejo del riesgo	Descripción
1	Impedir el riesgo	La probabilidad de que el Riesgo ocurra es alta.
2	Admitir el riesgo	Admitir la debilidad, y no efectuar más controles. Con perspectiva que la posibilidad de ocurrencia sea baja.
3	Transferir el riesgo	Mitigando las consecuencias con los correspondientes seguros. Su probabilidad de ocurrencia es medio.

Fuente: MAGERIT. Método de análisis de riesgos. En: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. España: Min. Hacienda y Administraciones Públicas, 2012. p. 59.

Teniendo en cuenta la planeación del método del manejo del riesgo se analizó para cada el posible impacto que produciría la ejecución para la evolución de la empresa, instaurando el método de manejo en las debilidades con altura baja y medio, Admitiendo el riesgo; los estimados como altos, habrán de ser mitigados por el hotel. Seguidamente en la Tabla No. 11, se puede observar la para cada uno de los riesgos descritos la estrategia de tratamiento seleccionada.

Tabla 11. Estrategia de tratamiento por riesgo identificado

Riesgos de seguridad	Grado De la debilidad	Manejo del riesgo
R1 - La carencia de controles y políticas para implementación de claves de ingreso a medios de tecnología del hotel, conllevan a la pérdida de información.	Alto	Impedir el riesgo
R2 – Deficiencias de diseño e implementación en la red del Hotel Pipatón, causando que no estén disponibles los servicios y la información.	Medio	Impedir el riesgo
R3 – Robo de datos del hotel Pipatón, por la carencia de procedimientos que formen directrices y buenos hábitos para seguridad de la información, realizando copias de seguridad.	Alto	Impedir el riesgo
R4 - Perdida de la confiabilidad e integridad de la información por causa un mal uso de controles de acceso y gestión de identidades.	Alto	Impedir el riesgo
R5 – Software desactualizados en la infraestructura tecnológica produciendo perdida de los datos y afectan el servicio.	Alto	Impedir el riesgo
R6 – Demoras para la recuperación de los datos de los equipos de cómputo por el deterioro motivado por fallas en los mantenimientos preventivos.	Medio	Impedir el riesgo
R7 – Demoras para la recuperación de los datos en los equipos de cómputo por el deterioro motivado por el abandono de configuraciones de seguridad en los equipos de cómputo.	Muy Bajo	Admitir el riesgo
R8 – Pérdida de información motivada por la no actualización o falta del antivirus.	Medio	Impedir el riesgo
R9 – Hardware dañados inducidos por virus o códigos maliciosos o falta del antivirus.	Medio	Impedir el riesgo
R10 – Afectaciones operacionales con la red LAN en hotel Pipatón, por la presencia de malware.	Alto	Impedir el riesgo
R11 – deterioro de los datos sin autorización por personal externo por excesos de autorizaciones en el perfil.	Medio	Impedir el riesgo

Fuente: elaboración propia

Tabla 11. (Continuación)

Riesgos de seguridad	Grado De la debilidad	Manejo del riesgo
R12 – Eliminación de datos guardados en las bases de información como consecuencia de la falta de reglas de seguridad para las aplicaciones que especifiquen renovación en las claves por parte de los usuarios.	Medio	Impedir el riesgo
R13 – Eliminación de privacidad de los datos por carencia en paradigmas para protección del aplicativo que pidan renovación de claves a funcionarios nuevos.	Medio	Impedir el riesgo
R14 – Eliminación de los datos por mala manipulación de protocolos inciertos manejados en la divulgación del sitio web.	Alto	Impedir el riesgo
R15 – Pérdida de clientes hotel Pipatón, por falta elementos tecnológicos de cifrado de información sobre almacenamiento electrónico.	Alto	Impedir el riesgo
R16 - Falta de directrices claras de seguridad, orientadas a funcionarios por carencia de controles y política de seguridad de la información.	Critico	Transferir el riesgo

Fuente: elaboración propia

6.2.3.2 Exposición del plan de trabajo.

Teniendo en cuenta la táctica de manejo escogida en cada uno de las debilidades, se diseñan los controles orientados a controlar, minimizar y mitigar los riesgos inherentes que se hallan actualmente en la infraestructura tecnológica del Hotel Pipatón. En la tabla No. 12, se muestran los riesgos, vulnerabilidades, el tratamiento y los controles a implementar, como también la persona encargada de la realización de control.

Tabla 12. Planeación del manejo para controlar y minimizar los riesgos.

Activo selecciona do para el análisis de las debilidades	Debilidades en la seguridad	Grado de las debilidade s	Que altera			Método de manejo de riesgos referidos			
			Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
Red LAN y Red WIFI	**R1** - La carencia de controles y políticas para implementación de claves de ingreso a medios de tecnología del hotel, conllevan a la pérdida de información.	Alto	C	I		Impedir el riesgo	C1	Diseñar políticas de seguridad de la información en el Hotel	Administrador del sistema de información
							C2	Instalación y configuración de un sistema de seguridad anti robo e incendios.	Administrador del sistema de información
							C3	Realizar una configuración de protección para defender los datos, red LAN y WIFI.	Administrador del sistema de información
	R2 – Deficiencias de diseño e implementación en la red del Hotel Pipatón, causando que no estén disponibles los servicios y la información.	Medio			D	Impedir el riesgo	C4	Actividades de mantenimiento en los sistemas para garantizar su eficacia.	Administrador del sistema de información
							C5	Conocimiento, educación y capacitación en seguridad de la información.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

Activo selecciona do para el análisis de las debilidades	Debilidades en la seguridad	Grado de las debilidade s	Que altera			Método de manejo de riesgos referidos			
			Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
Servidores, computado res, portátiles, Impresoras , fotocopiado ras	**R3** – Robo de datos del hotel Pipatón, por la carencia de procedimientos que formen directrices y buenos hábitos para seguridad de la información, realizando copias de seguridad.	Alto		I	D	Impedir el riesgo	C6	Crear las políticas de seguridad de la información del Hotel.	Administrador del sistemas de información
							C7	Concretar un plan de tratamiento de incidentes de seguridad.	Administrador del sistema de información
							C8	Crear procedimientos para copias de seguridad de la información.	Administrador del sistema de información
	R4 - Perdida de la confiabilidad e integridad de la información por causa un mal uso de controles de acceso y gestión de identidades.	Alto	C	I		Impedir el riesgo	C9	Los equipos se deberían mantener correctamente, deberían proteger contra fallas de energía y otras interrupciones, para asegurar su disponibilidad e integridad continua.	Administrador del sistema de información
							C10	Renovar y limpiar los archivos creados, conociendo las normas de protección.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

			Que altera			Método de manejo de riesgos referidos			
	Debilidades en la seguridad	Grado de las debilidades	Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
Activo seleccionado para el análisis de las debilidades	**R5** – Software desactualizados en la infraestructura tecnológica produciendo perdida de los datos y afectan el servicio.	Alto	C		D	Impedir el riesgo	C11	Utilizar SW (Sistemas Operativos, Antivirus, etc.) licenciados y actualizados en los equipos de cómputo.	Administrador del sistema de información
							C12	Efectuar mantenimientos programados a los equipos de cómputo, para advertir desactualizaciones de SW	Administrador del sistema de información
	R6 – Demoras para la recuperación de los datos de los equipos de cómputo por el deterioro motivado por fallas en los mantenimientos preventivos.	Medio	D			Impedir el riesgo	C13	Crear un plan de mantenimiento preventivo y correctivo de HW y SW, que prolongue el funcionamiento de la red LAN y WIFI, ofreciendo continuidad en los servicios.	Administrador del sistema de información
							C14	Programar y evidenciar los mantenimientos preventivos hechos a los equipos de cómputo.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

Activo selecciona do para el análisis de las debilidades	Debilidades en la seguridad	Grado de las debilidade s	Que altera			Método de manejo de riesgos referidos			
			Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
	R7 – Demoras para la recuperación de los datos en los equipos de cómputo por el deterioro motivado por el abandono de configuraciones de seguridad en los equipos de cómputo.	Muy Bajo			D	Admitir el riesgo	C15	El Hotel Pipatón no escogiera ningún tipo de control porque ha resuelto Admitir el riesgo.	N.A.
Antivirus	**R8** – Pérdida de información motivada por la no actualización o falta del antivirus.	Medio	C		D	Impedir el riesgo	C16	Equipos de cómputo del hotel Pipatón, deben utilizar SW (Sistemas Operativos, Antivirus, etc.) licenciado y con actualizaciones al día	Administrador del sistema de información
							C17	Programar mantenimientos preventivos a la infraestructura informática advirtiendo desactualizados de algún tipo de software.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

			Que altera			Método de manejo de riesgos referidos			
	Debilidades en la seguridad	Grado de las debilidades	Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
Activo selecciona do para el análisis de las debilidades	**R9** – Hardware dañados inducidos por virus o códigos maliciosos o falta del antivirus.	Medio			D	Impedir el riesgo	C18	La infraestructura tecnológica deberá contar con software licenciado y actualizado en los dispositivos del hotel Pipatón.	Administrador del sistema de información
							C19	La infraestructura tecnológica deberá proveer desactualizado realizando mantto preventivos.	Administrador del sistema de información
	R10 – Afectaciones operacionales con la red LAN en hotel Pipatón, por la presencia de malware.	Alto	C		D	Impedir el riesgo	C20	La infraestructura tecnológica deberá contar con software licenciado y actualizado en los dispositivos del hotel Pipatón.	Administrador del sistema de información
							C21	La infraestructura tecnológica deberá proveer desactualizado realizando mantto preventivos.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

Activo selecciona do para el análisis de las debilidades	Debilidades en la seguridad	Grado de las debilidade s	Que altera			Método de manejo de riesgos referidos			
			Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
Aplicativos - Ejecutable	**R11** – deterioro de los datos sin autorización por personal externo por excesos de autorizaciones en el perfil.	Medio	C		D	Impedir el riesgo	C22	Controles seguridad de la información. Políticas de seguridad de la información.	Administrador del sistema de información
							C23	Procedimientos y responsables. Información de los eventos y fallas de la seguridad de la información.	Administrador del sistema de información
	R12 – Eliminación de datos guardados en las bases de información como consecuencia de la falta de reglas de seguridad para las aplicaciones que especifiquen renovación en las claves por parte de los usuarios.	Medio			D	Impedir el riesgo	C24	Software para Salvaguardar de las aplicaciones Informáticas.	Administrador del sistema de información
							C25	Administrador Copias de seguridad (backup). Sistema de Control para emplear perfiles de seguridad	Administrador del sistema de información
							C26	Capacitación al personal del hotel Pipatón en temas de la información.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

			Que altera			Método de manejo de riesgos referidos			
	Debilidades en la seguridad	Grado de las debilidades	Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
Activo seleccionado para el análisis de las debilidades	**R13** – Eliminación de privacidad de los datos por carencia en paradigmas para protección del aplicativo que pidan renovación de claves a funcionarios nuevos.	Medio	C			Impedir el riesgo	C27	Software para Salvaguardar de las aplicaciones Informáticas.	Administrador del sistema de información
							C28	Administrar Copias de seguridad (backup). Sistema de Control para emplear perfiles de seguridad	Administrador del sistema de información
							C29	Capacitación al personal del hotel Pipatón en temas de la información.	Administrador del sistema de información
	R14 – Eliminación de los datos por mala manipulación de protocolos inciertos manejados en la divulgación del sitio web.	Alto	C			Impedir el riesgo	C30	Crear y evidenciar una metodología de software seguro en el hotel Pipatón.	Administrador del sistema de información
							C31	Establecer la metodología de software seguro en el hotel Pipatón.	Administrador del sistema de información
							C32	Obtener un certificado SSL, con una empresa legalmente autorizada.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

Activo selecciona do para el análisis de las debilidades	Debilidades en la seguridad	Grado de las debilidade s	Que altera			Método de manejo de riesgos referidos			
			Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
							C33	Instalar y configurar el certificado SSL, para manejo de información en el sitio WEB	Administrador del sistema de información
Medios de almacenam iento	**R15** – Pérdida de clientes hotel Pipatón, por falta elementos tecnológicos de cifrado de información sobre almacenamiento electrónico.	Alto	C			Impedir el riesgo	C34	Implementar planes de continuidad conteniendo seguridad de la información.	Administrador del sistema de información
							C35	Dar prioridad a información del Hotel Pipatón, definiendo si es confidencial.	Administrador del sistema de información
							C36	Efectuar procesos de cifrado de información equipos de cómputo y de almacenamiento.	Administrador del sistema de información
Talento Humano Hotel Pipatón.	**R16** - Falta de directrices claras de seguridad, orientados a funcionarios por carencia de controles y política de seguridad de la información	Critico	C			Transferir el riesgo	C37	Diseñar la política de seguridad información del Hotel Pipatón.	Administrador del sistema de información
							C38	Implementar planes de continuidad incluido la seguridad información.	Administrador del sistema de información

Fuente: elaboración propia

Tabla 12. (Continuación)

Activo selecciona do para el análisis de las debilidades	Debilidades en la seguridad	Grado de las debilidade s	Que altera			Método de manejo de riesgos referidos			
			Confidencialidad	Integridad	Disponibilidad	Manejo del riesgo	Control	Método de trabajo (control)	Encargado
Talento Humano Hotel Pipatón.	**R16** - Falta de directrices claras de seguridad, orientados a funcionarios por carencia de controles y política de seguridad de la información	Critico	C			Transferir el riesgo	C39	Capacitación en seguridad de la información.	Administrador del sistema de información y Director de Talento Humano.
							C40	Retirar los derechos de ingreso de los funcionarios y usuarios externos al hotel Pipatón, al finalizar su empleo.	Administrador del sistema de información

Fuente: elaboración propia

7. PROPUESTA DE CONTROLES

Para minimizar las debilidades en la seguridad evidenciados en la infraestructura tecnológica del Hotel Pipatón se plantean los controles, son los utilizados por los sistemas de información (SI), clasificándolos en correctivos, preventivos y detectivos. Seguidamente definiremos cada uno de los aspectos relacionados.

7.1 CONTROL PARA LAS INSTALACIONES

Permitirá al hotel y centro de convenciones Pipatón como organización, obtener una apropiada defensa y seguridad del sistema de información, del perímetro de infraestructura, como en la autenticación, control, gestión y administración de la información.

7.1.1 Segmentación.

Utilizando los segmentos se puede impedir el ingreso a la red LAN del hotel Pipatón por parte externa. El fragmento exterior de la LAN solo aprobara el enrutamiento un definido intercambio entre los dispositivos dispuestos (host, swich) de las aplicaciones que suministran los servicios de la empresa. Asegurando de la existencia de los controles a la red LAN que solo admitan el ingreso a los usuarios

autorizados del sistema. Restrinja el ingreso a los servicios prestados de red, así como los ingresos a los diferentes segmentos de la red LAN[39].

7.1.2 Red SOHO.

Se tienen que configurar el ingreso remoto a la interfaz de la red LAN, así como el protocolo TCP/IP. Se debe tener una IP, mascara de subred y dirección de DNS. Los anteriores parámetros son configurados y dados por el distribuidor del servicio de internet. Efectuar una revisión de puertos, identificando cuales puertos están abiertos, observando si está siendo utilizado por una aplicación o servicio. Los puertos no utilizados, se cierran.

7.1.3 Firewall configuración.

Son dispositivos de primera línea de defensa, como los firewalls se tienen que instalar en todos los sitios de borde de la red LAN. La configuración de reglas del firewall debe ser muy condicionales y hacerse servicio a servicio y host a host. Con un dispositivo como el firewall se tiene que dar control de ingreso al nivel de red, es decir, una configuración para dar control de tráfico. Para impedir el ingreso no autorizado a los servicios de red se deberían usar filtros de entrada y de salida. Se

---

[39] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 41.

deberá estudiar las posibles configuraciones del Firewall, para poder realizar los cambios requeridos.

7.1.4 Ingreso remoto.

Para ingreso a usuarios autorizados se limitará conforme a su nivel de permisos, e igualmente el tiempo de duración en la red. Incorpore la forma de conexión sitio a sitio fundamentada en la tecnología IPSEC. Limite el ingreso a los recursos del hotel Pipatón realizando la configuración de las listas de ingreso a la red.

7.1.5 Antivirus.

Como primera medida, utilice las aplicaciones de antivirus en los equipos servidores significativos, seguidamente en los de manejo de correos y base de datos. Pensando también en aplicar el mismo procedimiento con antivirus en los equipos de cómputo restantes.[40]

7.1.6 Seguridad física.

La información tiene que ser la más segura en ser vulnerada externamente, si no hay medidas de control será paupérrima la seguridad, en el momento de afrontar un desastre. Por tal razón se argumenta que la seguridad física consiste en aplicar

---

[40] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 43.

obstáculos físicos y procesos de control, como prevención contra delitos a la información y recursos confidenciales, haciendo referencia a controles y procedimientos que se tienen realizar al interior y cerca de centros de información para protección de los medios para guardar información y el hardware, con esta forma las empresas salvaguardan información fundamental.

a. Catástrofes:

Es dirigida en salvaguardar las falencias derivadas por la naturaleza e individuos mal intencionado, a los dispositivos físicos donde se guarda la información. Las amenazas con más ocurrencia son: incendios, tormentas, inundaciones, desastres naturales, sabotajes internos, disturbios. A continuación, se enumeran los riesgos que pueden generar en los centros informáticos con el fin ofrecer a tiempo pasos para advertir, reducir, rescatar y corregir los diferentes riesgos.[41]

- Incendios:

Los incendios son la principal amenaza contra la información, por lo que puede acabar con un equipo de cómputo en minutos dañando y borrando la totalidad de los archivos de información y aplicaciones. Los sistemas contraincendios logran concebir más daños en los equipos electrónicos que los incendios. Para advertir un incendio se deben contemplar diferentes causas:

[41] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 43.

- La infraestructura que aloja el sistema de información no puede permitir conflagraciones. Tampoco pueden estar ubicados cerca a sitios que acumulen material explosivo e inflamable.
- Las paredes deben ser de material incombustible.
- Construir sobre un piso falso con materiales que resistan el fuego.
- El mobiliario y cesta de basura no debe ser plásticos, preferible metálicos.
- El centro de almacenamiento debe estar impermeabilizado.

➢ Inundaciones:

En su mayoría son las que más perjudican a los centros de cómputo, por los daños en los datos. Para impedir la situación, es viable la implementación de suelos aparentes y a un nivel más arriba del normal. Tener en cuenta la construcción de cubiertas impermeables impidiendo el paso del agua[42].

➢ Instalaciones eléctricas:

Se requieren tener normas de seguridad industrial tratándose de instalaciones eléctricas en la infraestructura informática. También se deberán analizar los riesgos específicos y dar solución acorde a las normas.

---

[42] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 44.

b. Control de Ingreso:

El control de ingreso permite realizar una lista de chequeo de los usuarios quienes han ingresado o salido de la red LAN del hotel Pipatón, con la finalidad de tener una mayor seguridad en la información y disminuir las vulnerabilidades que tenga la red actual.

- Vigilancia privada - acceso de personas

Se recomienda tener un servicio de vigilancia para controlar el ingreso y salida del personal del hotel Pipatón. Este servicio tendría la necesidad de efectuar los listados de las personas a ingresar a la empresa, la persona deberá estar acreditada con carnet con foro y cargo, con la finalidad de realizar el control de acceso y salida del personal.

También se sugiere solicitar un documento donde se pueda realizar la verificación, e identificar para validar nombres, la fotografía y entregar un carnet para visitantes. Cuando el visitante haga la salida del hotel Pipatón, devolverá el carnet entregado y se dará su documento. Con todo este proceso se deberá anunciar para aprobar el ingreso a las instalaciones.

- Acceso de vehículos:

Los vehículos de transporte público se deberán tener en una lista detallada y en una base datos que relacione los datos básicos del vehículo. Se tendrá un registro de las horas de acceso y salida, también deberá efectuar la inspección del vehículo. Los automóviles que no estén inscritos en una empresa deberán llevar un carnet de

autorización para ingresar y deben aparecer en una base de datos con la información del conductor y del automóvil, horas de ingreso y salida del automóvil.

- Sistemas biométricos:

Con esta tecnología podemos identificar con una gran precisión a una persona obteniendo mayor confiabilidad en el momento de validar su identidad. Con esta tecnología eliminamos el uso de carnet en el momento de otorgar el ingreso del funcionario a la empresa. El valor de los mantenimientos de la tecnología biométrica resulta siendo más económica que la de los carnets, porque solo se deberá tener a un funcionario que haga limpieza y este verificando funcionamiento correcto del dispositivo y otra persona será encargada de tener actualizada base datos.

La mejor ventaja con este tipo de tecnología es la característica biométrica de un individuo, no se pueden transferir entre personas. En la actualidad los sistemas que dan economía y sencillos de manipular son los que confirman patrones de huellas dactilares.

- Comprobación por medio huella dactilar:

Este método es fundamentado con la consigna que en el mundo no existirán huellas semejantes, por tener diversos los arcos. Los arcos son revisados para poder conseguir la información del individuo y confrontarla con la información y reconocer absolutamente al individuo. En la actualidad el sistema más utilizado es el reconocimiento por huella dactilar, por lo que es más económico y de fácil compra.

- Circuito cerrado:

Se pueden observar la infraestructura del hotel Pipatón en línea, y al mismo tiempo es vigilada por funcionarios autorizados. Con esta manera se tiene reconocimiento de quien ingresa a las diferentes áreas del hotel Pipatón. Estos dispositivos poseen un sistema de control anti sabotajes de forma que, si falla la energía eléctrica u ocurre una falla, el dispositivo enviara una alerta al centro de cómputo para que se efectúe la tarea correspondiente[43].

- Detectores pasivos sin alimentación:

Algunos sensores están diseñados para detectar incendios, hurtos o ingresos no autorizados. Son comercializados por empresas especializadas en seguridad. En el momento que hay una variación y es descubierta por sensores, es activado el sistema de alarmas emitiendo una señal al centro de cómputo y el dispositivo dependiendo la señal da aviso al organismo correspondiente.

7.1.7 Usuarios administrativos.

Piense en manejar cuentas individuales para los procedimientos administrativos o gestión y este pendiente que los carnets de identificación se cambian con continuamente. Modifique las claves primordiales por claves que contengan

[43] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 46.

caracteres alfanuméricos, que contengan mayúsculas, minúsculas, contengan un carácter especial y un largo de mínimo de 8 caracteres.

7.1.8 Directrices para contraseñas.

Los usuarios de perfil de administración deberán ser más robustos, vigilando todos los ingresos autenticados, erróneos o correctos. Para realizar el almacenaje de los intentos de conexión erróneos por mal acceso de los funcionarios y claves, maneje los logs, permitiendo se realice una alerte a los administradores de los sistemas de los casos presentados.

7.1.9 Cuentas inactivas.

Haga seguidamente auditorías al sistema para verificar la actualización de sus cuentas por parte de los usuarios. Revise con frecuencia las páginas web de los fabricantes o proveedores que proveen aplicaciones de seguridad en busca de información actualizada de delitos y ataque de virus.

7.1.10 Usuarios internos.

Tenga en cuenta tener controles para las claves complicadas en cuanto a la manipulación de los funcionarios, otorgando libertad para el ingreso en su área. Una clave es considerada confusa si maneja los estándares de tener caracteres alfanuméricos, incluyendo caracteres en mayúscula, minúscula, especiales y contar con la longitud mínima de los ocho caracteres.

7.1.11 Ingreso remoto a usuarios.

Disponga en colocar en funcionamiento el control de claves complicadas de acceso y salidas a los funcionarios, sin tener en cuanta, si el ingreso se realiza a través de diferentes tecnologías como VPN o ADSL.

7.2 CONTROLES DE APLICACIONES

Permitirá al hotel Pipatón obtener una apropiada defensa en lo concerniente a las aplicaciones; su uso, ejecución y diseño de ellas y la autenticación necesaria requerida por las organizaciones en todo lo relacionado con la seguridad.

7.2.1 Almacenamiento.

La prohibición mediante el control de ingreso, se pueden efectuar en: aplicaciones específicas, sistemas operacionales, seguridad definida, Bases de datos. Para ejercer control de acceso se tienen diferentes maneras, como: Por medio de sistemas biométricos, así como, el lector de huellas, por medio de contraseñas conocidas solo por el usuario o pin de asignación, por medio de un patrón para escribir, al igual que la firma digital.

Se deberá contar con un proceso de solicitudes de autorización al responsable del informático del hotel Pipatón, será delegado de verificar, eliminar los usuarios inexistentes. El funcionario de perfil superior, deberá ser otorgar autorizaciones y definir a donde puede ingresar.

Se deberá contar con revisiones diarias de las cuentas de los funcionarios y sus privilegios. Organizar auditorias verificando el estado de la seguridad del hotel Pipatón. Se deberá vigilar constantemente para descubrir ingresos no autorizados, de modo que se consiga una confidencialidad de la información que se mueve al interior de la organización[44].

7.2.2 Realizado por un distribuidor independiente de software.

Con respecto a las actualizaciones de aplicaciones, se deberán poner en prueba totalmente, antes de ser utilizadas por los funcionarios. Se deberá tener los manuales de la aplicación para fortalecer su desarrollo. Si la aplicación es configurable, realice una revisión de cada punto.

7.2.3 Directivas de contraseñas.

Se recomienda la utilización de registros para los ingresos fallidos, enviando señales de alerta a los administradores del sistema. En las aplicaciones utilice las contraseñas difíciles. En las aplicaciones más importantes del hotel Pipatón, maneje directivas de bloqueo en las cuentas.

---

[44] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 48.

7.2.4 Autenticación.

Se recomienda la utilización de las claves complejas como puesta en práctica, para la mayoría de las cuentas correspondientes a las aplicaciones principales.

7.2.5 Autorización y control de acceso.

Periódicamente ingrese a páginas web de las aplicaciones y averigüe las actualizaciones que tengan que ver con la seguridad.

7.3 CONTROLES DE PERSONAL.

Es la encargada de crear reglas para que los administradores del hotel Pipatón, obtengan control y manejo de los funcionarios de las diferentes áreas.

7.3.1 Relaciones con terceros.

Los administradores de los sistemas deberán otorgar autorización a terceros conforme a las labores que vayan a realizar en los equipos de cómputo del hotel Pipatón, teniendo en cuenta las prohibiciones de ingreso a información, y día y hora de acceso.

7.3.2 Roles

Para la creación de un rol se deberá tener en cuenta autorizaciones como[45]: La escritura, donde el funcionario solo podrá cambiar los datos. Lectura, solo podrá el

[45] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 49.

funcionario observar los datos, sin autorización para cambiarla. Ejecución, los funcionarios tienen autorización de utilizar o no la aplicación. Borrado, el funcionario posee la autorización de eliminar el archivo, se deberá tener un control de los archivos los cuales se pueden eliminar.

7.3.3 Exigencias en seguridad.

Realizar asignaciones de grados de jerarquía en los elementos de la arquitectura tecnológica admitiendo que gran parte de las inversiones se empleen en dispositivos determinados débiles y equipos vulnerables se les otorguen pocos recursos. Por tal razón, se utiliza con mayor energía los recursos para la seguridad en los equipos de cómputo y sistemas que más lo requieran.

7.3.4 Evaluaciones de seguridad.

Se tendrá que realizar internamente una valoración a la infraestructura, el estado de las aplicaciones y el de la red. Al obtener los resultados del proceso de evaluación se utilizarán para mejorar los procesos internos.

7.3.5 Formación sobre seguridad.

La enseñanza continua y la formación fundamentada en roles son garantía para que todos los funcionarios sean consiente que se espera el hotel Pipatón de ellos y pensar como compensar esas expectativas. Se deberá seguir otorgando capacitaciones a todos los perfiles de la organización y en todos los temas de seguridad de acuerdo a los diferentes cargos.

7.3.6 Comprobaciones del historial personal.

Garantice la comprobación del historial de los funcionarios que contenga una valoración del historial laboral, niveles de estudio y pasado judicial de aspirante al cargo.

7.3.7 Directiva de recursos humanos.

Estudie periódicamente los procedimientos de los funcionarios que se van de la organización de manera desfavorable, dejando un registro anexado en la hoja de vida.[46]

7.4 CONTROLES DE OPERACIONES

Es la encargada de brindar los controles en diferentes áreas administrativas para la continuidad del hotel Pipatón de informar si se presenta disminución de la información importante para la organización.

7.4.1 Copias de seguridad y recuperación.

El administrador del sistema deberá documentarse de la forma como se efectúa los procedimientos de backup y rescate en los procedimientos graves para el normal desarrollo de las organizaciones. Se deberá realizar frecuentemente pruebas a la

[46] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 50.

forma de realizar los backup y rescate para probar que los dispositivos trabajen apropiadamente.

7.4.2 Dispositivos de copia de seguridad.

Para tener en cuenta los medios para realizar backup, pueden ser las copias de respaldo, se establezcan en sitios protegidos, así como mantener en unas instalaciones diferentes o externas al hotel Pipatón.

7.4.3 Eliminación de datos.

En los servidores los procedimientos de borrado de información se deberán realizar mediante autorizaciones especiales y lo podrá efectuar el administrador del sistema, con el previo permiso del Gerente del hotel Pipatón, sin olvidar de diligenciar un registro interno de quien realizo la eliminación de la información.[47]

[47] PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Marco legal o normativo. En: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. 2010. p. 51.

8. POLÍTICAS RECOMENDADAS EN LA ORGANIZACIÓN

Con base en la fase de análisis y diseño y los controles de seguridad establecidos anteriormente se recomienda implementar las siguientes políticas de seguridad de la información al sistema de información y la red LAN del Hotel y centro de convenciones Pipatón.

8.1 ALCANCE

Las políticas y lineamientos son de entera aplicación a la totalidad de procesos y áreas que forman el hotel Pipatón, los recursos, todos los procesos de calidad internos y externos que tienen vínculo con la organización por medio de contratación o alianzas con terceros y a todos los funcionarios del hotel, en cualquier situación contractual, el área en que desempeña sus servicios y el nivel laboral que desarrolle.

8.2 ACUERDOS DE CONFIDENCIALIDAD

En el hotel Pipatón, se deberán obedecer los compromisos de confidencialidad por parte de todos los funcionarios, en donde se realice un compromiso individual con cada funcionario a, en ningún caso usar, popularizar o sacar beneficio de la información confidencial a la que se tenga ingreso, teniendo respeto por los niveles de categorización de la información establecidos, y el desacato en lo estipulado se considerara un “incidente de seguridad”.

8.3 MANEJO ACEPTABLE DE ACTIVOS

El ingreso en la documentación fisca o digital se determinará usando los perfiles del área específica, las autorizaciones y la jerarquía de ingreso al personal, estos estarán fijados por los jefes de cada proceso o área, quien será la encargada de realizar la comunicación al administrador del sistema. Llevar un listado del personal, sus perfiles con el objetivo de bajar o minimizar la manipulación sin autorización de los activos de información existentes en el Hotel Pipatón[48].

8.4 INGRESO A INTERNET

a. Nunca se permite:

- Para ingresar en sitios web que tengan alguna relación con pornografía, alcohol, drogas u otro sitio web que sea contraria a la ética moral, políticas señaladas y leyes actuales.
- El ingreso y utilización de medios interactivos, mensajería, redes sociales, como: Facebook, Skype, MSN Messenger, Twitter, cuyo objetivo sea tener sociedades comercializadoras de datos o con una finalidad distinta a los servicios del Hotel Pipatón.

[48] SUAREZ, Sandra Yomay. Conclusiones. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015.p.102

- No se puede realizar el intercambio de información no autorizada de pertenencia del hotel Pipatón, de sus funcionarios y/o clientes, con personal externo.
- La descarga, instalación, uso de aplicaciones de juegos, música, películas, servicios que violen de una forma la pertenencia intelectual, o el empleo aplicaciones que violen la infraestructura tecnológica, con respecto a la disponibilidad, confidencialidad e integridad.

b. La totalidad de los funcionarios tienen la responsabilidad de otorgar un buen uso a este recurso y no utilizarlo para efectuar prácticas ilegales contra tercero, leyes actuales y reglas de seguridad de la información, etc.
c. La utilización del internet se permitirá cuando se efectúe de forma ética, responsable, razonable, sin abusos y no afectando el desarrollo diario, ni la seguridad de la información de Hotel Pipatón.

8.5 RECURSOS TECNOLÓGICOS

Los recursos de tecnología que posee el hotel Pipatón y que están asignados a los empleados, se reglamentaran a continuación su uso apropiado bajo las siguientes normas.[49]

[49] SUAREZ, Sandra Yomay. Conclusiones. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015.p.103.

a. Instalación de hardware y software, variar la configuración en un equipo de cómputo del hotel Pipatón, el administrador del sistema será la persona responsable de los activos informáticos y por tal motivo es el único con autoridad para efectuar estas actividades.

b. Sincronizar equipos móviles, en los que se pueda intercambiar información con cualquier equipo del hotel Pipatón, tendrá que estar respaldado de manera clara el área pertinente, simultáneamente con el funcionario administrador de los activos informáticos y solo se realizara exclusivamente en equipos suministrados por el hotel Pipatón.

8.6 CAPACITACIÓN Y EDUCACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Los funcionarios nuevos en el instante de ingresar al hotel Pipatón tendrán que tener una capacitación de inducción y seguir habitualmente capacitándose en temas de controles, políticas, procedimientos establecidos en el documento de controles y políticas de seguridad de la información, para tal fin, se debe contar con el apoyo del área de talento humano, dándoles a conocer a los funcionarios sus deberes y sanciones existentes por el desacato a las normas.

8.7 CONTROL DE ACCESO FÍSICO

El hotel Pipatón, deberá controlar y restringir el ingreso a la oficina y/o cuarto de comunicaciones, donde se disponga el servidor y equipos de cómputo. De igual forma deberá crear y conservar los lineamientos, listados y controles de ingreso al área dispuesta.

8.8 SEGURIDAD Y LUGAR DE LOS EQUIPOS

a. Los dispositivos de cómputo, pertenecientes a la red tecnológica de Hotel Pipatón, como terminales de la red, deberán estar situados y resguardados apropiadamente, adaptando los controles requeridos manteniéndoles en ambientes seguros y bien protegidos al menos con: electricidad regulada y protegida por fuentes ininterrumpida (UPS), sistema de incendio y extinción, control de humedad y temperatura, control de ingreso.[50].

b. Para los empleados que utilicen o tengan a cargo los equipos de cómputo de la infraestructura tecnológica de Hotel Pipatón, no deberán ingerir alimentos cerca de los equipos, ni fumar o beber.

---

[50] SUAREZ, Sandra Yomay. Conclusiones. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015.p.104.

8.9 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

a. Los equipos de cómputo pertenecientes a la infraestructura tecnológica del hotel Pipatón, deben estar resguardados con aplicaciones antivirus configurados para actualizaciones automáticas.
b. La comisión de calidad y protección de los datos serán los encargados de realizar y conservar los lineamientos, políticas, procedimientos y guías para garantizar la minimización de las debilidades ligadas a los delitos de software malicioso y métodos hacking.

8.10 COPIAS DE RESPALDO

a. El hotel Pipatón deberá certificar que los datos que tenga algún grado de categorización incluidos en el sitio web de la organización, cuente con la protección diaria por medio de procedimientos apropiados para controlar que certifiquen la seguridad, integridad, disposición e identificación.

b. El hotel Pipatón tendrá que implementar planes para realizar la restauración eficiente de los backup analizados con una frecuencia moderada certificando que se pueden confiar en determinada situación, ya sea una incidencia y resguardadas a lo largo del tiempo.

c. Dispositivos magnéticos encargados de resguardan los datos delicados tendrán que ser guardados externamente del hotel Pipatón, lugar dispuesto para tal fin, se deberá ejercer un control para la seguridad requeridos, cumpliendo con los estándares de precaución para la seguridad.

8.11 CONTROLES PARA INGRESO LÓGICO

a. Todos los funcionarios del hotel Pipatón que tengan a cargo dispositivos informáticos, serán bajo su responsabilidad y confianza del nombre de usuario con su respectiva clave de ingreso.

b. Todos los funcionarios del hotel Pipatón tendrán que realizar autenticación en los dispositivos de control de ingreso lógico antes de acceder a la infraestructura tecnológica de la organización.[51]

c. La identidad del funcionario al momento de acceder a la red será personalizado y único, por lo que el funcionario se hace responsable de las acciones que se realicen con su usuario en el sistema.

---

[51] SUAREZ, Sandra Yomay. Conclusiones. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015.p.105.

8.12 GESTIÓN DE CONTRASEÑAS DE USUARIO

a. El funcionario tiene el deber de realizar el cambio de la contraseña asignada por defecto por el administrador del sistema y recursos tecnológicos.
b. Si el funcionario se le olvido, bloqueo la clave de acceso, tendrá que remitirse o hacer la solicitud al funcionario encargado de administrar el sistema, para que le apruebe el ingreso de una nueva clave de acceso, para que el funcionario realice el cambio respectivo.
c. Se prohíbe tener recordatorios escritos o impresos referentes a las claves de acceso en sitios donde pueda ingresar personal sin autorización.
d. Es responsabilidad de los funcionarios el prestar su clave personal a otras personas para ingresar al sistema y realizar acciones dentro del sistema de información.
e. Los funcionarios deben tener en cuenta los siguientes pasos para la creación de la clave personal.
    - Las claves de ingreso estarán conformadas por combinaciones de caracteres numéricos, alfanuméricos y especiales, de mínimo ocho y máximo doce caracteres.
    - Las claves de ingreso al sistema de información no deben estar relacionadas a nombres, fechas de nacimiento, cargos o sitios de trabajo.
    - El usuario tendrá la responsabilidad de hacer el cambio de la clave de ingreso mínimo una vez al mes, esto sería si el sistema no solicita el cambio automáticamente.

8.13 ESCRITORIO Y PANTALLA LIMPIA

a. Los funcionarios del hotel Pipatón serán responsables de cerrar la sesión de su equipo de cómputo en los instantes que no estén en su puesto laboral y lo abrirán solo con la clave del usuario.[52]
b. Cuando el funcionario de por terminada las labores diarias, se tienen que cerrar las aplicaciones y realizar el apagado de los equipos de cómputo.
c. El hotel Pipatón implementará en sus políticas de seguridad un ítem para el protector de pantalla, que se activará pasados 5 minutos automáticamente después de la inactividad y lo podrá desbloquear solo el usuario.

8.14 INVESTIGACIÓN DE INCIDENTES DE LA SEGURIDAD DE LOS DATOS

Los funcionarios del hotel Pipatón deberán informar con responsabilidad, rapidez y prontitud los supuestos delitos de seguridad a su jefe inmediato y al administrador del sistema y recursos tecnológicos. El hotel Pipatón realizara un procedimiento de comunicación y contestación a eventualidades, mostrando la acción que se realizara al momento de llegar el registro del incidente ocurrido.

---

[52] SUAREZ, Sandra Yomay. Conclusiones. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015.p.106.

En este método se implementará que, en el caso del descubrimiento de una eventualidad o violación de seguridad, se informará al administrador del sistema y recursos tecnológicos, lo más rápido posible, el cual buscará los recursos a utilizar para realizar la investigación y solución de la eventualidad, y verificará su desarrollo. Y así mismo tendrá la obligación de informar de los sucesos ocurridos a la administración.[53]

[53] SUAREZ, Sandra Yomay. Conclusiones. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015 .p.107.

9. CONCLUSIONES

Como dice Perafán[54], con la finalización del proyecto se lograron realizar los objetivos trazados, los controles estipulados permitirán desarrollar una mayor seguridad en la realización de los procesos del hotel Pipatón, llevando a cabo las recomendaciones de seguridad de la información. Con la implementación en la organización de la metodología Magerit para análisis de riesgos, es primordial para certificar la seguridad de los activos de información y el desarrollo interno de la empresa. El desarrollo del análisis de riesgos dio a conocer de forma general las debilidades en seguridad que presenta el hotel Pipatón.

Como dice Suarez[55], como se ha visualizado en la elaboración de este proyecto es inocultable que los “datos e información” ahora son catalogados como el activo de mayor valor para hotel Pipatón, es por esto, e iniciando con esta frase para la empresa, es de suma importancia la elaboración e implementación de controles y políticas de seguridad de la información en la red LAN, con base en los estándares internacionales y corrigiendo las debilidades de la organización.

---

[54] PERAFAN, Jhon Jairo and CAICEDO Cuchimba Mildred. Conclusiones. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. 2014. p.109.

[55] SUAREZ, Sandra Yomay. Conclusiones. En: Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015.p.128

Después de analizar la situación actual del Hotel e Identificar las amenazas y vulnerabilidades se diseñaron controles y políticas de calidad para dar seguridad al sistema de información y a la red LAN, conforme a reconocidos estándares universales, teniendo en cuenta los factores que pudieran afectar la estabilidad de la red LAN. Con la organización de la seguridad, se consigue realizar un análisis técnico adecuado de la organización, obteniendo la identificación al detalle de las vulnerabilidades y los posibles procedimientos para solucionar las amenazas presentadas.

Se organizaron procedimientos de infraestructura tecnológica confiables, robustos y actuales, con tecnología de punta, ofreciendo a la organización confiabilidad en cada uno de las políticas y controles propuestos, brindando la protección requerida por la red LAN del Hotel Pipatón. Con la estructuración de las políticas y controles diseñados para el Hotel, se garantiza la disposición, confiabilidad, e integridad de la información, que es el activo más valioso de las organizaciones en el mundo actual, garantizando la seguridad de la información.

10. RECOMENDACIONES

Se deberá realizar con todos los funcionarios del Hotel Pipatón un ciclo de formación y sensibilización basadas en la protección de los datos minimizando los peligros de un ataque. Teniendo en cuanta que la manipulación de los datos recopilados será de carácter privado, para conocer y adoptar la política de cambio de seguridad informática en pro de las mejores prácticas.

Como dice Perafán[56], el responsable del área de informática, entre sus labores diarias tendrá que realizar auditorías frecuentes sobre los activos de información para estar actualizando controles y de paso apoyar con el proceso de mejorar las prácticas concernientes a la protección de los sistemas. Teniendo en cuenta lo anteriormente mencionado la empresa podrán minimizar los periodos logrando los objetivos estipulados en el proyecto.

Los controles y políticas de seguridad sugeridos se obtuvieron del análisis de riesgos y la empresa debe procurar implementarlos en el menor tiempo posible, garantizando la continuidad y seguridad de la empresa, salvaguardando la información y por ende minimizando los riesgos, vulnerabilidades detectadas.

[56] PERAFAN, Jhon Jairo and CAICEDO Cuchimba Mildred. Conclusiones. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. 2014. p.108.

11. BIBLIOGRAFÍA

ALARCON, Javier Orlando. Diseño e implementación de políticas de seguridad informática, red y virtualización apoyadas con software libre en la compañía tecnología y redes S.A.S [en línea]. Tesis profesional. Fundación universitaria los libertadores, 2016. [Consultado 21 mayo 2020]. Disponible en: https://repository.libertadores.edu.co/bitstream/handle/11371/1332/alarconjavier2016.pdf?sequence=1

ALEGSA. Diccionario de informática y tecnología: definición de encriptación [consultado: 21 mayo 2020]. Disponible en: http://www.alegsa.com.ar/Dic/encriptaci%C3%B3n.php

BLOG Herramientas para la implantación de un SGSI [en línea]. España: Oscar de la Cuesta, 2015 [Fecha de consulta: 21 mayo 2020]. Disponible en: www.palentino.es/blog/herramientas-para-la-implantacion-de-un-sgsi

CÓRDOBA, Nombrado, CORTINA, Óscar Manuel y APONTE, Luis Daniel. Sistema de gestión de seguridad de la información en la fundación medico preventiva IPS [en línea]. Tesis profesional. Universidad popular del cesar, 2019. [Consultado 21 Mayo 2020]. Disponible en: https://www.academia.edu/40885617/TRABAJO_MAGERIT

DOCUMENTACIÓN. Microsoft: Conexión enrutada a Internet [consultado el 21 de mayo de 2020, 10:00]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc736774(v%3dws.10)

DOCUMENTACIÓN. Microsoft: Conexión traducida a internet [consultado el 21 de mayo de 2020, 10:00]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780147(v%3dws.10)

DOCUMENTACIÓN. Microsoft: Red SOHO a Internet [consultado el 21 de mayo de 2020, 10:00]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc783461(v=ws.10)

ESGUERRA, Liz Mayoly y ORTIZ, Geraldine Alejandra. Propuesta de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013 para la empresa LOVATO CITY GAS S.A.S [en línea]. Tesis profesional. Universidad distrital Francisco José de Caldas, 2018. [Consultado 21 mayo 2020]. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/13419/4/Geraldine%20Alejandra%20Ortiz%20C%C3%A1rdenas%202018.pdf

FAJARDO, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano [en línea]. Tesis especialización. Institución universitaria politécnico gran colombiano, 2017.

[Consultado 21 mayo 2020]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%C3%B3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y

GONZÁLEZ, Nury amparo. Diseño del sistema de gestión en seguridad y salud ocupacional, bajo los requisitos de la norma ntc-ohsas 18001 en el proceso de fabricación de cosméticos para la empresa wilcos S.A. [en línea]. Tesis profesional. Pontificia universidad javeriana, 2009. [Consultado 21 mayo 2020]. Disponible en: https://javeriana.edu.co/biblos/tesis/ingenieria/Tesis221.pdf

In SlideShare [en línea]. USA: LinkedIn Corporation, 2020 [Fecha de consulta: 21 mayo 2020]. Disponible en: https://es.slideshare.net/cristiandiazv/redaccin-de-discusin-y-conclusiones

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma técnica colombiana. NTC 1486. Bogotá, D.C: ICONTEC, 2018. 39 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Referencias bibliográficas contenido, forma y estructura. NTC 6166. Bogotá, D.C: ICONTEC, 2016. 52 p.

ISO 27002:2013 Tecnología de la Información – código para la práctica de la gestión de la seguridad de la información. SCS Consulting [consultado: 21 mayo 2020]. Disponible en: https://www.scsconsulting.es/iso-270022013-tecnologia-la-informacion-tecnicas-seguridad-codigo-la-practica-la-gestion-la-seguridad-la-informacion/

ISO/IEC 27001 - Information security management [sitio web]. USA: ISO. [Consulta: 21 mayo 2020]. Disponible en: https://www.iso.org/isoiec-27001-information-security.html

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método [en línea]. Madrid: Ministerio de Hacienda y Administraciones Públicas ,2012 [Consulta: 21 mayo 2020]. Disponible en Internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

NUÑEZ, William Andrés y CHACÓN, Edinson Andrés. Diseño del sistema de gestión de seguridad de la información para la empresa SEREXCEL servicios funerarios [en línea]. Tesis profesional. Universidad distrital Francisco José de Caldas, 2017. [Consultado 21 mayo 2020]. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/8323/1/Edinson%20Andres%20Chacon%20Uma%C3%B1a%20-%20William%20Andres%20Nu%C3%B1ez%20Vergara%202017.pdf

PERAFAN, Jhon Jairo y CAICEDO Cuchimba Mildred. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca [en línea]. Tesis profesional. Universidad Nacional Abierta y a Distancia, 2014. [Consultado 21 mayo 2020]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá [en línea]. Tesis profesional. Universidad de San Buenaventura, 2010. [Consultado 21 mayo 2020]. Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/2952/1/Diseno_politicas_controles_pulido_2010.pdf

ROZO, Jenny Milena y SUAREZ, Omar. Gestión de seguridad de la información en la institución educativa león XIII del municipio de Soacha [en línea]. Tesis profesional. Institución universitaria politécnico gran colombiano, 2016. [Consultado 21 mayo 2020]. Disponible en: http://alejandria.poligran.edu.co/bitstream/handle/10823/659/Rozo%20Suarez%20Proyecto%20trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

SECRETARIA JURÍDICA DISTRITAL [sitio web]. Bogotá: Alcaldía Mayor de Bogotá D.C. [Consulta: 21 mayo 2020]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información [consultado: 21 mayo 2020]. Disponible en: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

SUAREZ, Sandra Yomay. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización [en línea]. Tesis especialización. Universidad Nacional Abierta y a Distancia, 2015. [Consultado 21 mayo 2020]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3777/1/20904541.pdf

TECNOLOGÍA DE LA INFORMACIÓN – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. ESTÁNDAR ISO/IEC INTERNACIONAL 17799 Segunda Edición 2005-06-15 [consultado: 21 mayo 2020]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

ANEXOS

ANEXO A. Carta de permiso acceso a información

IBERTUR S.A.S.
Hotel y Centro de Convenciones PIPATON
Nit 830 081 506-2

SC-CER319424

Barrancabermeja, 10 de Abril de 2018

Señores
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería
La Ciudad.

Estimados Señores:
Yo, **OSCAR CASTILLA ALARCON**, identificado con CC: 19.185.925 de Santa Fe de Bogota, en mi calidad de Gerente Administrativo de la empresa HOTEL Y CENTRO DE CONVENCIONES PIPATON, autorizo a **Wilfrido Alfonso Trujillo Niebles**, identificado con cedula No. 91.444.523, estudiante del programa ESPECIALIZACION EN SEGURIDAD INFORMATICA de la **UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD,** a utilizar información confidencial de la empresa para el proyecto denominado **DISEÑO DE POLÍTICAS Y CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA RED LAN EN EL HOTEL PIPATON.** Como condiciones contractuales, el estudiante se obliga a (1) no divulgar ni usar para fines personales la información (documentos, expedientes, escritos, artículos, contratos, estados de cuenta y demás materiales) que, con objeto de la relación de trabajo, le fue suministrada; (2) no proporcionar a terceras personas, verbalmente o por escrito, directa o indirectamente, información alguna de las actividades y/o procesos de cualquier clase que fuesen observadas en la empresa durante la duración del proyecto y (3) no utilizar completa o parcialmente ninguno de los productos (documentos, metodología, procesos y demás) relacionados con el proyecto. El estudiante asume que toda información y el resultado del proyecto serán de uso exclusivamente académico.
El material suministrado por la empresa será la base para la construcción de un estudio de caso. La información y resultado que se obtenga del mismo podrían llegar a convertirse en una herramienta didáctica que apoye la formación de los estudiantes de la Escuela de Administración.
En caso de que alguna(s) de las condiciones anteriores sea(n) infringida(s), el estudiante queda sujeto a la responsabilidad civil por daños y perjuicios que cause a HOTEL Y CENTRO DE CONVENCIONES PIPATON, así como a las sanciones de carácter penal o legal a que se hiciere acreedor.

Atentamente,
IBERTUR S.A.S.
NIT. 830081506-2

OSCAR CASTILLA ALARCON
CC.: 19.185.925

Avenida del Río No.47-16 PBX (7) 6020250 Fax (7) 602 02 58 Barrancabermeja, Santander / Colombia
Correo eléctronico: reservas@hotelpipaton.com/ comercialhotelpipaton@gmail.com

ANEXO B. Controles ISO 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

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.
- 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.
- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.
- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
- 12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
- 12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
- 12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

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.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 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.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION 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.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

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.
- 18.2.3 Comprobación del cumplimiento.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

ISO27002.es PATROCINADO POR:

Octubre-2013

ANEXO C. Lista de Chequeo Hotel Pipatón

Hotel Pipatón – lista de chequeo				
Tipo	Preguntas	Si	No	Ns/Nr
Auditoria de redes	¿La gerencia de redes tiene una política definida de planeamiento de tecnología de red?			
	¿Esta política es acorde con el plan de calidad de la ¿Organización?			
	¿Existe un inventario de equipos y software asociados a las redes de datos?			
	¿Están establecidos controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados?			
	¿Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red?			
	¿Existen protocolos de comunicaron establecida?			
	¿La transmisión de la información en las redes es segura?			
	¿El acceso a la red tiene password?			
Auditoria de seguridad	¿Existen procedimientos para la realización de las copias de seguridad?			
	¿Existen procedimientos que aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana?			
	¿Existen controles sobre el acceso físico a las copias de seguridad?			
	¿Las copias de seguridad de los ficheros de nivel alto se almacenan en lugar diferente al de los equipos que las procesan?			
	¿Existe un inventario de los soportes existentes?			
	¿Dicho inventario incluye las copias de seguridad?			
	¿Las copias de seguridad, o cualquier otro soporte, se almacenan fuera de la instalación?			
	¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?			
	¿Existen procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual?			
	¿Existen políticas de la instalación en relación con los accesos al sitio donde se guardan las copias de seguridad?			
Auditoria a bases de datos	¿Existe equipos o software de SGBD?			
	¿La organización tiene un sistema de gestión de base de datos (SGBD)?			
	¿Conoce el tipo de Base de Datos existentes en la organización?			
	¿Existe personal restringido que tenga acceso a la BD?			
	¿El SGBD es dependiente de los servicios que ofrece el ¿Sistema Operativo?			
	¿La interfaz que existe entre el SGBD y el SO es el adecuado?			
	¿Existen procedimientos formales para la operación del SGBD?			
	¿Están actualizados los procedimientos de SGBD?			

	¿Son suficientemente claras las operaciones que realiza la BD?			
	¿Existe un control estricto de las copias de estos archivos?			
	¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?			
	¿Se tiene un responsable del SGBD?			
	¿Se realizan auditorias periódicas a los medios de almacenamiento?			
	¿Se tiene relación del personal autorizado para manipular la BD?			
	¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD?			
	¿Existen integridad de los componentes y de seguridad de datos?			
	¿De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipos capaces que soportar el trabajo?			
	¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?			
	¿La capacidad de almacenamiento máximo de la BD es suficiente para atender el proceso por lotes y el proceso remoto?			
	¿El personal responsable del manejo, manipulación de los sistemas de información es el adecuado?			

ANEXO D. Formato RAE

1. Información General	
Tema	Seguridad de la Información
Titulo	Diseño de controles y políticas para la seguridad de la información en la red LAN en el hotel Pipatón
Tipo de proyecto	Monografía
Autor (es)	Wilfrido Alfonso Trujillo Niebles
Director	Ing. Hernando José Peña Hidalgo
Fuente bibliográfica	ALARCON, Javier Orlando. Diseño e implementación de políticas de seguridad informática, red y virtualización apoyadas con software libre en la compañía tecnología y redes S.A.S [en línea]. Tesis profesional. Fundación universitaria los libertadores, 2016. [Consultado 21 mayo 2020]. Disponible en: https://repository.libertadores.edu.co/bitstream/handle/11371/1332/alarconjavier2016.pdf?sequence=1 CÓRDOBA, Nombrado, CORTINA, Óscar Manuel y APONTE, Luis Daniel. Sistema de gestión de seguridad de la información en la fundación medico preventiva IPS [en línea]. Tesis profesional. Universidad popular del cesar, 2019. [Consultado 21 Mayo 2020]. Disponible en: https://www.academia.edu/40885617/TRABAJO_MAGERIT ESGUERRA, Liz Mayoly y ORTIZ, Geraldine Alejandra. Propuesta de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013 para la empresa LOVATO CITY GAS S.A.S [en línea]. Tesis profesional. Universidad distrital Francisco José de Caldas, 2018. [Consultado 21 Mayo 2020]. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/13419/4/Geraldine%20Alejandra%20Ortiz%20C%C3%A1rdenas%202018.pdf FAJARDO, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano [en línea]. Tesis especialización. Institución universitaria politécnico gran colombiano, 2017. [Consultado 21 mayo 2020]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/995/3.%20Documento%20Final%20Opci%C3%B3n%20de%20grado%20II.pdf?sequence=1&isAllowed=y GONZÁLEZ, Nury amparo. Diseño del sistema de gestión en seguridad y salud ocupacional, bajo los requisitos de la norma ntc-ohsas 18001 en el proceso de fabricación de cosméticos para la empresa wilcos S.A. [en línea]. Tesis profesional. Pontificia universidad javeriana, 2009. [Consultado 21 mayo 2020]. Disponible en: https://javeriana.edu.co/biblos/tesis/ingenieria/Tesis221.pdf NUÑEZ, William Andrés y CHACÓN, Edinson Andrés. Diseño del sistema de gestión de seguridad de la información para la empresa SEREXCEL servicios funerarios [en línea]. Tesis profesional. Universidad distrital Francisco José de Caldas, 2017. [Consultado 21 mayo 2020]. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/8323/1/Edinson%20Andres%20Chacon%20Uma%C3%B1a%20-%20William%20Andres%20Nu%C3%B1ez%20Vergara%202017.pdf

	PERAFAN, Jhon Jairo y CAICEDO Cuchimba Mildred. En: Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca [en línea]. Tesis profesional. Universidad Nacional Abierta y a Distancia, 2014. [Consultado 21 mayo 2020]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf PULIDO, Andrea Marcela, RINCÓN, Paulo César y VELÁSQUEZ, Óscar Mauricio. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá [en línea]. Tesis profesional. Universidad de San Buenaventura, 2010. [Consultado 21 mayo 2020]. Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/2952/1/Diseno_politicas_controles_pulido_2010.pdf ROZO, Jenny Milena y SUAREZ, Omar. Gestión de seguridad de la información en la institución educativa león XIII del municipio de Soacha [en línea]. Tesis profesional. Institución universitaria politécnico gran colombiano, 2016. [Consultado 21 mayo 2020]. Disponible en: http://alejandria.poligran.edu.co/bitstream/handle/10823/659/Rozo%20Suarez%20Proyecto%20trabajo%20de%20grado.pdf?sequence=1&isAllowed=y SUAREZ, Sandra Yomay. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización [en línea]. Tesis especialización. Universidad Nacional Abierta y a Distancia, 2015. [Consultado 21 mayo 2020]. Disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3777/1/20904541.pdf
Año	2020
Resumen	El hotel Pipatón, para la protección de la información que recopila de sus clientes, huéspedes o proveedores que manipula en las diferentes áreas con que cuenta la organización para poder prestar y ofrecer sus servicios. Describiremos los diferentes pasos que se tomaron para la realización del diseño de los controles y políticas de calidad que servirán para minimizar las diferentes vulneraciones existentes en el hotel Pipatón con ayuda de la metodología Magerit. Se identificaron las diferentes fallas de seguridad de la información en las diferentes áreas con el apoyo de los funcionarios involucrados en el manejo de los sistemas de cómputo. Después e lograron identificar los activos de información y se realizó el respectivo análisis para determinar el grado de vulnerabilidad existente y plasmarlo en el mapa de calor diseñado para este fin. Después de haber identificado los activos informáticos y su respectiva valoración, pasamos a plantear controles para poder minimizar las falencias o debilidades presentadas y por último se presentan unas políticas a tomar para que la empresa implemente con todos sus funcionarios. Los Controles y políticas de seguridad, tendrán éxito si concientizamos a los usuarios que ellos son los encargados de salvaguardar los datos en el hotel Pipatón.
Palabras claves	Seguridad informática, seguridad de la información, seguridad en red LAN, Vulnerabilidades, controles y políticas de calidad.
Contenidos	Actualmente los sistemas de información y las empresas, afrontan, un incremento de inseguridades y riesgos informáticos, derivados de una amplia diversidad de fuentes, en los que se tienen los delitos relacionados a la informática, sabotajes, espionajes,

	perjuicios que ocasionan los virus informáticos y agresiones de intrusión o de servicios de navegación, que se han vuelto cada día más comunes de las empresas. El Hotel y centro de convenciones Pipatón, recibe información de sus proveedores y clientes por multiplex medios y canales (personal, redes de datos, sistemas en línea, telefónico, empresas de mensajería, electrónicos, entre otros); información financiera y personal. Esta gran cantidad de información y datos forman la principal materia prima para los procesos del hotel, convirtiéndolo en el activo más importante que se debe proteger desde el ingreso hasta su disposición final. "Los datos son para las organizaciones lo que significa el corazón para el cuerpo humano", en este pasaje se puede afirmar a los datos pasan a ser el activo con un alto valorado que conserva una empresa, debido a que estos datos se ya que se proporcionan a los demás procesos de servicios que ofrece el hotel, la información se vuelve el todo, de tal forma, resguardarla de personas extrañas, conservarla segura y es de importante en el entorno laboral.

2. Descripción del Problema de Investigación

¿Qué puede hacer el Hotel Pipatón en la red LAN, para minimizar los factores de vulneración y riesgo a los que exponen día a día, la información de la organización, y así poder contribuir con el mejoramiento de la seguridad?

3. Objetivos

OBJETIVO GENERAL

- Realizar el análisis de la situación actual del Hotel Pipatón, diseñar controles y políticas de seguridad de la información en el sistema de información, red LAN, ofreciendo a la infraestructura tecnológica una apropiada protección en seguridad informática a la organización.

OBJETIVOS ESPECÍFICOS

- Realizar el diagnóstico actual de la situación de la seguridad de la información del Hotel Pipatón.
- Identificar por medio del análisis de riesgo los activos de información, las amenazas y vulnerabilidades a las que está expuesto el sistema de información, a través de cuestionarios, entrevistas a los funcionarios, responsables.
- Elegir los controles más importantes de la seguridad de la información, que garanticen la integridad, disponibilidad y confidencialidad de la información.
- Establecer unas políticas de seguridad conforme a los patrones universales, buscando establecer una manipulación aceptable para los activos de información.

4. Metodología

La metodología que se va a utilizar para realizar la identificación, clasificación y valoración de los activos de información, logrando determinar las amenazas y vulnerabilidades que lograrían perturbar la seguridad de la información que manipula el Hotel Pipatón, basados en la metodología de análisis y de gestión de riesgos de los sistemas de información MAGERIT.

La metodología a utilizar para el desarrollo de los objetivos y el alcance planteados en el proyecto y propuesta en la fase de análisis y diseño, en donde se plantea en cada etapa varias sucesiones de actividades enfocadas a conseguir los resultados del proyecto, las que a continuación se detallan.

Fase 1. Análisis.
Efectuar la recopilación de la información utilizando las técnicas a continuación:

- Diálogos con los diferentes funcionarios de las áreas determinadas del Hotel Pipatón.
- Reconocimiento de la infraestructura existente del Hotel Pipatón.

- Reconocimiento de la infraestructura de redes existente, con la cual se manipula la información.

Fase 2. Diseño.

1. Concretar la metodología a efectuar donde se realice el análisis de riesgos de seguridad de la información en el Hotel Pipatón.
   - Clasificar e identificar los activos de información, usando el método de clasificación de los activos de la metodología MAGERIT.
   - Establecer amenazas y vulnerabilidades de los activos de información del Hotel Pipatón.
   - Detallar las debilidades de la seguridad de los datos evidenciados dentro del hotel Pipatón, empleando la metodología MAGERIT para estudio y administración de debilidades para sistemas informáticos.
   - Valorar la posibilidad de que una vulneración descubierta suceda y el impacto en el sistema de información.
   - Concretar con la administración el grado de aprobación de las debilidades de seguridad de los datos.
2. Crear los controles para la seguridad del Hotel Pipatón, encargados de proteger la infraestructura tecnológica.
3. Diseñar las políticas de seguridad de la información del Hotel Pipatón.

4. Referentes Teóricos

ALEGSA. Diccionario de informática y tecnología: definición de encriptación [consultado: 21 mayo 2020]. Disponible en: http://www.alegsa.com.ar/Dic/encriptaci%C3%B3n.php

IN SLIDESHARE [en línea]. USA: LinkedIn Corporation, 2020 [Fecha de consulta: 21 mayo 2020]. Disponible en: https://es.slideshare.net/cristiandiazv/redaccin-de-discusin-y-conclusiones

ISO 27002:2013 Tecnología de la Información – código para la práctica de la gestión de la seguridad de la información. SCS Consulting [consultado: 21 mayo 2020]. Disponible en: https://www.scsconsulting.es/iso-270022013-tecnologia-la-informacion-tecnicas-seguridad-codigo-la-practica-la-gestion-la-seguridad-la-informacion/

SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información [consultado: 21 mayo 2020]. Disponible en: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

TECNOLOGÍA DE LA INFORMACIÓN – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. ESTÁNDAR ISO/IEC INTERNACIONAL 17799 Segunda Edición 2005-06-15 [consultado: 21 mayo 2020]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

5. Referentes Teóricos y Conceptuales

BLOG Herramientas para la implantación de un SGSI [en línea]. España: Oscar de la Cuesta, 2015 [Fecha de consulta: 21 mayo 2020]. Disponible en: www.palentino.es/blog/herramientas-para-la-implantacion-de-un-sgsi

DOCUMENTACIÓN. Microsoft: Conexión enrutada a Internet [consultado el 21 de mayo de 2020, 10:00]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc736774(v%3dws.10)

DOCUMENTACIÓN. Microsoft: Conexión traducida a internet [consultado el 21 de mayo de 2020, 10:00]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780147(v%3dws.10)

DOCUMENTACIÓN. Microsoft: Red SOHO a Internet [consultado el 21 de mayo de 2020, 10:00]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc783461(v=ws.10)

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma técnica colombiana. NTC 1486. Bogotá, D.C: ICONTEC, 2018. 39 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Referencias bibliográficas contenido, forma y estructura. NTC 6166. Bogotá, D.C: ICONTEC, 2016. 52 p.

ISO/IEC 27001 - Information security management [sitio web]. USA: ISO. [Consulta: 21 mayo 2020]. Disponible en: https://www.iso.org/isoiec-27001-information-security.html

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método [en línea]. Madrid: Ministerio de Hacienda y Administraciones Públicas ,2012 [Consulta: 21 mayo 2020]. Disponible en Internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

SECRETARIA JURÍDICA DISTRITAL [sitio web]. Bogotá: Alcaldía Mayor de Bogotá D.C. [Consulta: 21 mayo 2020]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

6. Resultados y Conclusiones

Después de analizar la situación actual del Hotel e Identificar las amenazas y vulnerabilidades se diseñaron controles y políticas de calidad para dar seguridad al sistema de información y a la red LAN, conforme a reconocidos estándares universales, teniendo en cuenta los factores que pudieran afectar la estabilidad de la red LAN. Con la organización de la seguridad, se consigue realizar un análisis técnico adecuado de la organización, obteniendo la identificación al detalle de las vulnerabilidades y los posibles procedimientos para solucionar las amenazas presentadas.

Se organizaron procedimientos de infraestructura tecnológica confiables, robustos y actuales, con tecnología de punta, ofreciendo a la organización confiabilidad en cada uno de las políticas y controles propuestos, brindando la protección requerida por la red LAN del Hotel Pipatón.

Con la estructuración de las políticas y controles diseñados para el Hotel, se garantiza la disposición, confiabilidad, e integridad de la información, que es el activo más valioso de las organizaciones en el mundo actual, garantizando la seguridad de la información.

Con la estructuración tecnológica realizada, se garantiza en la organización la continuidad, cumplimiento y altos estándares de trabajo y manipulación de la información con normas internacionales vigentes, enfocadas para minimizar los tipos de vulnerabilidades existentes. Contribuyendo a el correcto funcionamiento de la operación diaria de la organización, sin producir afectación en los procesos.