UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA DE SISTEMAS Y AFINES
COORDINACIÓN DE INVESTIGACIÓN

EVALUACIÓN MEDIANTE AUDITORÍA DE LA INFRAESTRUCTURA Y SEGURIDAD DE LAS REDES LAN/WAN DE LOS HOTELES LIDOTEL Y TIBISAY, PARA LA MEJORA DE LOS CONTROLES, ESTÁNDARES DE SEGURIDAD DEL DEPARTAMENTO DE SISTEMAS.

Trabajo de Investigación

Autores:
Br. Bauza, Dulce
C.I:27.280.213
Br. Benítez, Oriana
C.I: 27.424.833
Tutora: Esp. Lic. Isis Rueda

El Valle del Espíritu Santo, Marzo de 2020

UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA Y AFINES
COORDINACIÓN DE INVESTIGACIÓN

CARTA DE APROBACIÓN DEL TUTOR

En mi carácter de Tutor del Trabajo de Investigación presentado por las ciudadanas Oriana Paola Benítez López, Dulce Obdalys Bauza López**,** ceduladas con el número: V.-27.424.833, 27.280.213, para optar al Grado de *Ingeniero de Sistemas*, considero que dicho trabajo: EVALUACIÓN MEDIANTE AUDITORÍA DE LA INFRAESTRUCTURA Y SEGURIDAD DE LAS REDES LAN/WAN DE LOS HOTELES
LIDOTEL Y TIBISAY, PARA LA MEJORA DE LOS CONTROLES, ESTÁNDARES DE SEGURIDAD DEL DEPARTAMENTO DE SISTEMAS reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado Examinador que se designe.

Atentamente

Esp. Lic. Isis N. Rueda P.

TUTOR

El Valle del Espíritu Santo, marzo de 2021

DEDICATORIAS

A mi Dios y Salvador Jesucristo, por ser el principal autor de todo lo vivido y lo que me queda por vivir, quien me ha dado de su fortaleza para avanzar en cada circunstancia, vencer los obstáculos y así conquistar las metas propuestas.

A mis padres, hermanos, por velar en todas las necesidades que requería, por ser la fuerza, motor y luz, ser los consejeros primordiales en el desarrollo de mi vida.

A mi abuela, Cruz Elina Rivera porque a pesar de habernos dejado en mi transcurrir universitario, estuvo lo suficiente para darme su apoyo, alegría y sustento.

Al Sr. Juan Farías y Carolina de Farías, por brindarme abrigo, alimento y atención cuando más lo necesité, al igual que sus hijos Catherine, Jhoan y Caleb.

Dulce Bauza

A mis abuelos, a mis padres Auriliz López y Fortunato Benítez, a mis tíos Lisaura López y Anderson Certad que durante mi vida se han encargado de velar por mi educación, como pilares fundamentales que son para mí, les doy las gracias por su apoyo incondicional, consejos, esfuerzo y dedicación para guiarme a cumplir esta meta importante. A mis amigas, compañeros de estudio y profesores, quienes han formado parte del camino de saberes, por su apoyo y motivación que me han otorgado en la carrera. A todos ellos se los agradezco desde el fondo de mi corazón. Para todos ellos hago esta dedicatoria.

Oriana Benítez

AGRADECIMIENTOS

A mis amigas y compañeras de equipo, Oriana Benítez por ser mi compañera de trabajo de grado, por estar atenta a las responsabilidades demandadas, también, a Mariam Rosal por ayudarme y ser apoyo en cada una de las materias cursadas.

A mi tutor académico Isis Rueda, por ayudarme en este trabajo de grado, que, a pesar de los contratiempos, estuvo presente para no rendirme y tirar la toalla, por sus conocimientos impartidos, por su amabilidad, cariño y aprecio.

A la casa de estudio UNIMAR, que me abrió las puertas y garantizó esta culminación en esta trayectoria universitaria con éxitos.

Al Decano Ing. Andrés Pedroza y la Prof. Nelly Cumaraima, por estar prestos y dar soporte en el avance de etapa de mi formación académica.

A Lidotel Hotel Boutique Margarita y Tibisay Hotel Boutique, por permitirme poder realizar la investigación para sustentar dicho trabajo.

Por último, a todas aquellas personas que estuvieron dispuestas a mostrar su favor, cooperación, ayuda y colaboración para que esta meta se haya hecho posible.

Dulce Bauza

A mi Dios Jehová por otorgarme la fortaleza y seguridad para avanzar en mi recorrido académico en momentos difíciles sin desfallecer en el intento y dando la oportunidad a alcanzar y lograr mis metas, entre ellas ser una profesional en esta área.

A mis familiares por con su afecto, apoyo emocional y económico durante mi carrera, sé que a pesar de las circunstancias siempre están y seguirán presentes apoyándome y cuidándome a lo largo de mi vida.

A mis compañeras y amigas, Dulce Bauza y Mariam Rosal, quienes en el camino me brindaron un apoyo y motivación para llevar a cabo mis responsabilidades.

A mi novio por estar presente, apoyarme, enseñarme y ayudarme cuando se me presentaron dificultades en el desarrollo de asignaciones en las materias.

A la casa de estudio UNIMAR, que nos brindó sus espacios y profesionales para llevar a cabo la culminación de la carrera de Ingeniería de Sistemas.

A nuestra tutora Isis Rueda y Decano Andrés Pedroza, que siempre nos guiaron y solventaron bajo cualquier situación que se presentase, por su apoyo, cariño y paciencia que demostraron hacia nosotras en momentos de angustia y preocupaciones.

A la Prof. Nelly Cumaraima y Yemnel Torcat, por su soporte metodológico en el desarrollo de la presente investigación.

A los profesionales que formaron parte de mi instrucción universitaria, quienes no desistieron a enseñarme, aun sin importar las vicisitudes que se han presentado estos 5 años de carrera, motivándonos a superarnos a diario para continuar creciendo en conocimientos.

A todos aquellos quienes nos han guiado a lo largo de la elaboración de este trabajo de investigación, para hoy obtener este valioso trabajo.

A todos ustedes, les agradezco con mucho cariño y reconocimiento del grandísimo apoyo que hemos recibido.

Oriana Benítez

ÍNDICE

LISTA DE TABLAS

LISTA DE GRÁFICOS

UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
COORDINACIÓN DE INVESTIGACIÓN

EVALUACIÓN MEDIANTE AUDITORÍA DE LA INFRAESTRUCTURA Y SEGURIDAD DE LAS REDES LAN/WAN DE LOS HOTELES LIDOTEL Y TIBISAY, PARA LA MEJORA DE LOS CONTROLES, ESTÁNDARES DE SEGURIDAD DEL DEPARTAMENTO DE SISTEMAS.

Autores:
Br. Bauza, Dulce
C.I:27.280.213
Br. Benítez, Oriana
C.I: 27.424.833
Tutor: Esp. Lic. Isis Rueda
Marzo de 2021

RESUMEN

El presente trabajo de investigación tiene por objetivo general evaluar mediante una auditoría la infraestructura y seguridad de las redes LAN/WAN de las sucursales del Estado Nueva Esparta de los hoteles Lidotel y Tibisay para la mejora de los controles, estándares de seguridad del departamento de sistemas. Este estudio se llevó a cabo mediante el modelo cuantitativo, así como también el método evaluativo, el cual proporcionó un análisis de lo investigado. Además, se usó un diseño de investigación de campo y documental para fundamentar lo hallazgos descubiertos. De las técnicas de recolección de datos se utilizaron la encuesta, entrevistas, observación directa y revisión documental, asimismo, se utilizó un análisis deductivo-crítico y bajo el marco de trabajo ITIL se generaron las conclusiones y recomendaciones, por consiguiente, se expresa que es primordial la aplicación y establecimiento de las directrices para el buen desarrollo y funcionamiento de sus operaciones a nivel de redes.
Descriptores: auditoría, TI, infraestructura, redes, estándares de seguridad, ISO 27001, COBIT, ITIL, calidad de servicio, gestión de seguridad, controles de riesgos, políticas de seguridad.

INTRODUCCIÓN

El avance tecnológico ha llegado para facilitar la ejecución de las actividades de la vida diaria, hasta el punto que se han vuelto indispensable para el equilibrio social. Este conjunto de herramientas ha proporcionado numerosos beneficios en diversos ámbitos del desarrollo humano. En el mundo empresarial, se implementan tecnologías en variados procesos que lo ameritan para alcanzar así un alto nivel de competitividad y crecimiento en el mercado. Sin embargo, para el buen desempeño de las operaciones y alcance de objetivos, las organizaciones establecen patrones y directrices como soporte vital para asegurar que los procedimientos, diseños, productos y otras acciones cumplan con requisitos establecidos.

Actualmente, el mundo se ha vuelto muy competitivo en relación a los negocios, es por ello que las organizaciones deben mejorar sus comunicaciones tanto internas como externas, con el fin de mantener un buen desarrollo y crecimiento en el mercado, también, brindar un excelente servicio. En efecto, toda la información de la organización se conduce a través de una red física de cableado que debe ser sólida para brindar soporte a la parte lógica que se encarga de asegurar la integridad, confiablidad y disponibilidad de los datos.

Siendo de evidente la importancia de la seguridad física de las redes, se planteó evaluar el nivel físico de éstas en dos hoteles de cadenas nacionales e internacionales, ubicados en el Estado Nueva Esparta, los cuales fueron Lidotel Hotel Boutique Margarita y Tibisay Hotel Boutique. Por medio de la investigación evaluativa de las infraestructuras de las redes LAN/WAN de población de estudio, junto con las técnicas de recolección, se logró obtener información puntual del área estudiada, que fue analizada y fundamentada en el marco de trabajo de las mejoras prácticas para las tecnologías de información ITIL, el cual provee un conjunto de buenas prácticas para controlar y gestionar los recursos, así como también la seguridad de la información. Basado en ello se formularon recomendaciones pertinentes a cada organización, sin embargo, en algunos casos se interceptan, por lo que se establece que: deben definir un marco de trabajo, seguirlo, estar avalados, mejorar las herramientas encargadas de la seguridad y contar con el personal necesario para mejorar la disponibilidad de servicios.

Para poder lograr dicho objeto, se lleva a cabo el presente trabajo de investigación que se encuentra estructurado de la siguiente manera:

Parte I: Se realiza el planteamiento del problema a través de la descripción y análisis de la situación, seguidamente, se establecen los objetivos tanto general como específicos de la investigación, además, se fija el valor académico.

Parte II: Se muestra el marco teórico referencial, el cual se encuentra integrado por las bases teóricas y bases legales, también, se definen los conceptos básicos utilizados en el presente trabajo.

Parte III: Se presenta el marco metodológico, el cual está compuesto por la naturaleza de la investigación, el tipo y diseño de investigación, asimismo, por la población y muestra, seguidamente, por las técnicas de recolección de datos y técnicas de análisis de datos.

Parte IV: corresponde a la aplicación de Las técnicas e instrumentos de investigación expuesto en el capítulo III.

Y, por último, las conclusiones y recomendaciones.

PARTE I

DESCRIPCIÓN GENERAL

1.1. Formulación del problema

La tecnología comprende la colección de herramientas que hacen más fácil usar, crear, administrar, almacenar e intercambiar información. En sus inicios, los seres humanos hacían uso de ella para el proceso de descubrimiento del mundo y evolución. De igual manera, la utilización de estos elementos tiene como fin la resolución de problemas y hacer más fácil la vida de los seres humanos. Por consiguiente, la tecnología ha aportado grandes beneficios a la sociedad, su papel principal es crear una mejora de implementos adaptados a los usuarios para facilitar, ahorrar esfuerzos, brindar un mejor aprovechamiento y gestión de recursos, sobre todo el tiempo.

De igual manera, los procesos tecnológicos se han ido incorporando dentro de las empresas, los cuales están pasando a ser el eje central sobre el que giran sus actividades, más que una ayuda, una oportunidad de optimizar sus funcionamientos que les proporciona las herramientas necesarias adaptados a las exigencias de los actuales mercados.

Sin embargo, para que estas tecnologías de información (TI) sean óptimas deben cumplir con normas y estándares, y definidos como el proceso de formular y aplicar reglas, en otras palabras, el proceso que apunta a la creación y la aplicación de normas que son utilizadas a nivel general en un determinado ámbito.

De la misma forma, los métodos y estándares de sistemas informáticos o sistemas de información (SI) se han convertido en un elemento de soporte vital de las organizaciones; a medida que se implementan los procesos del negocio, crece la necesidad de aplicarlas para asegurar que los procedimientos, diseños, productos y otras acciones cumplan con requisitos de calidad. No obstante, el equilibrio social está en juego, resulta inaceptable encontrar en la actualidad, empresas con mandos rígidos y ancladas en el pasado, sin la capacidad de adaptarse a los cambios o no enfocarse en sus clientes, por eso es importante, para una firma que desee alcanzar altos niveles de competitividad, el uso y aplicación de estándares de calidad internacionales, que le permitan ampliar sus mercados, mejorar su posicionamiento y crear valor; esto ha conllevado a verse en la

necesidad de recopilar, aplicar y clasificar los distintas metodologías creadas por los diferentes comités de creación en el mundo.

Actualmente, las organizaciones utilizan estas herramientas tecnológicas como un elemento de apoyo para el logro eficaz de los procesos, actividades, servicios y tareas que se llevan a cabo en la misma, donde, el apoyo de estas normas y estándares es muy esencial, contribuye a la mejora de los procesos de negocios, con la finalidad de lograr productos y servicios de calidad que ayuden a la toma de decisiones en las empresas. De igual modo, la calidad incluye todos aquellos aspectos o características de un producto o actividad que son de una importancia sustancial en relación a la satisfacción de los requisitos establecidos.

En la actualidad, las metodologías y estándares de sistemas informáticos, son de gran uso en los diversos campos de la informática porque ayuda a gestionar la utilidad adecuada de la tecnología de información en las organizaciones; para lo cual se han creado desde hace mucho tiempo atrás los estándares y normas que hoy en día rigen en torno a este mundo, para el desarrollo correcto de las actividades cumpliendo con los parámetros establecidos en la que se conseguirá la ansiada calidad.

Uno de los principales comités de creación de los métodos y estándares de sistemas es: Organización Internacional para la Estandarización (ISO), la cual fue creada en 1947 y están representados por organismos nacionales de normalización que trabajan para establecer una forma común en la gestión de sistema de calidad, que permita garantizar la satisfacción de las necesidades y/o expectativas de los consumidores. Además, la Organización Internacional de Normalización actualmente está presente en 193 países y es una organización no gubernamental e independiente; actualmente hay redactadas más de 22.000 normas ISO que abarcan todas las industrias, desde tecnología y seguridad alimentaria, hasta agricultura y salud. De igual forma, se componen de estándares y guías relacionados con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización. Igualmente, dos de las normas más conocidas de esta institución son la ISO 9000, sobre calidad y gestión de calidad proporcionando un aumento en la productividad, reducción de costos innecesarios y garantía la calidad de los procesos y productos. Asimismo, ésta especifica la manera en que una organización opera sus estándares de calidad, tiempo de entrega y niveles de servicio. La otra es la familia ISO 2700, abarca lo que respecta a la seguridad y sistemas de gestión de la seguridad de la información.

No obstante, todos los estándares son referentes, marcos de trabajo, patrones o lineamientos por los que, también, se rigen las auditorías, éstas se centran en ayudar y proveer a las empresas un control que les permita detectar fallos, vulnerabilidades y el estado actual en que ésta se encuentra, mediante una evaluación que genere posibles soluciones o, mejor dicho, que proporcione recomendaciones, por lo que y de acuerdo a su interés de aplicación, existen diversos tipos marcos de trabajo, orientadas a diferentes áreas. Según Arens, A. (2007), auditoría es "la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos, se deben realizar por una persona independiente y competente", (p.4), es decir, que se encargan de recoger, agrupar y evaluar evidencias para determinar si éste protege el activo empresarial.

Los tipos de auditorías son muchos, adecuados a distintas áreas y en todas desempeña un papel importante. Sin embargo, en la seguridad informática, su rol es encargarse de analizar y gestionar la seguridad de los SI, resguardando así los activos empresariales. Por lo contrario, al no ser realizadas traen numerosas consecuencias en las que se encuentran comprometidas gravemente la integridad, calidad, confidencialidad y confiabilidad de sus recursos, así como también generar pérdidas significativas en distintos ámbitos (financieros, tecnológicos, legales, entre otros) exponiendo su imagen y afectando su posición en el mercado. También al verse vulnerables a la pérdida de recursos, fallas en los procesos, equipos, desarrollo de las operaciones, desgastes o deficiencias en diferentes niveles, pierde rentabilidad.

Las organizaciones empresariales deben estar provistas de tecnologías que proporcionen acceso a la información y fácil manipulación, para cumplir con sus actividades utilizan diversos dispositivos que comúnmente están (o deberían estar) interconectados a una red informática. Estos suelen agruparse según su función: gestionar el acceso a la red y las comunicaciones (dispositivos de la red: Hubs, routers, switch, módem, entre otros.) y los que se conectan a ella con el fin de usarla (dispositivos de usuarios finales: tablets, computadoras, impresoras, entre otros).

Los dispositivos suelen tener mucho contacto con la información, lo cual incrementa la importancia de su seguridad, ya que esta siempre debe cumplir con los principios fundamentales de confiabilidad, integridad y confidencialidad, es ahí donde entran en juego las auditorías. El tipo de auditoría dependerá del área y nivel de enfoque, entre los niveles aplicables están físico y lógico. Sin embargo, el fin de ambas es resguardar el activo empresarial.

En la actualidad, existen variedad de maneras y dispositivos con los cuales comunicarse, igualmente protocolos y mecanismos que en ella intervienen, proporcionando una interconexión eficiente. Ahora bien, no hay mucha diferencia en la comunicación que mantienen las organizaciones que, mediante el uso de las redes, realizan la transmisión de información. Sin embargo, son múltiples los elementos involucrados para que las redes cuenten con un nivel de seguridad, desde los dispositivos presentes, los usuarios que tienen acceso, hasta las políticas y procedimientos establecidos por la misma organización. En ellas, los recursos más utilizados para llevar a cabo el proceso de interacción, son las redes de área local (LAN) y redes de área amplia (WAN) por su capacidad de alcance.

Las empresas Lidotel Hotel Boutique Margarita y Tibisay Hotel Boutique, son cadenas hoteleras que cuenta con varias sucursales que brindan servicios a nivel internacional y nacional. Para mantener la comunicación e intercambio de información, entre ellas hacen uso de las tecnologías de información (TI), las cuales les proporcionan la capacidad para gestionar sus operaciones y brindan la continuidad y disponibilidad de los servicios que proveen. No obstante, deben cumplir con una serie de controles que les garanticen una gestión segura de los procesos del negocio, a fin de darle mayor resguardo a la información. Por lo tanto, se plantea evaluar mediante una auditoría, que permita determinar el estado actual en el que se encuentran las infraestructuras de redes, en las sucursales del estado Nueva Esparta, de dichas empresas, a nivel de seguridad informática, asimismo las vulnerabilidades y los riesgos, orientados al cumplimiento de los estándares de seguridad de tecnología de información con el fin de mejorar los controles mediante la aplicación de normas y estándares establecidos por las instituciones, como: ISO 27000-1, COBIT y COSO.

1.2. Interrogantes

Lo expuesto anteriormente conlleva a la siguiente pregunta ¿Cómo una auditoría de la infraestructura y seguridad de las redes LAN/WAN de los hoteles Lidotel Hotel Boutique Margarita Lidotel y Tibisay Hotel Boutique, podrían mejorar los controles, estándares de seguridad del departamento de sistemas?

a. ¿Qué marcos de trabajos utilizan los hoteles para la gestión de la seguridad y gestión de riesgos de las infraestructuras de sus redes LAN/WAN?

b. ¿Cómo es la infraestructura actual, los controles y las gestiones realizadas bajo los estándares internacionales?

c. ¿Cómo son las políticas, de seguridad de TI establecidas para la instalación de redes LAN/WAN de la empresa y su cumplimiento con los estándares?

1.3. Objetivo general

Evaluar mediante una auditoría la infraestructura y seguridad de las redes LAN/WAN de las sucursales del Estado Nueva Esparta de los hoteles Lidotel Hotel Boutique Margarita y Tibisay Hotel Boutique para la mejora de los controles, estándares de seguridad del departamento de sistemas.

1.4. Objetivos específicos

a. Identificar los marcos de trabajo por los cuales se rigen los hoteles Lidotel Hotel Boutique Margarita y Tibisay Hotel Boutique para la gestión de la seguridad y de riesgos de las infraestructuras de redes LAN/WAN.
b. Analizar la infraestructura actual, los controles y gestiones realizadas alineadas a los estándares internacionales.
c. Revisar las políticas de seguridad de TI establecidas para la instalación de redes LAN/WAN de la empresa y su cumplimiento con los estándares.

1.5. Valor Académico de la investigación

Hoy en día, poseer un sistema de información (SI) se ha vuelto indispensable para desenvolverse en esta era tecnológica y de globalización, por lo tanto, es recomendable que todas las organizaciones competitivas implementen un sistema de información que le permita mejorar su productividad, rendimiento y posicionamiento, para ello es importante evaluar las técnicas actuales y la tecnología disponible para desarrollar sistemas que brinden eficiencia y eficacia de la gestión de la información. Ahora bien, estos ameritan un control que permita identificar y obtener información sobre su funcionamiento dentro de la organización, para ello, se recurre a la aplicación de distintos métodos y técnicas que faciliten la recolección de los datos y documentación del proceso, además que sirven como constancia de su ejecución.

Las auditorías de seguridad informática permiten determinar el estado actual en que se encuentra la protección de la información, así como los recursos dentro de las entidades, mediante la aplicación de metodologías o marco de trabajos que proporcionen información, que debe ser expresada éticamente de forma clara e imparcial por el auditor, involucrando la identificación,

análisis y evaluación de las debilidades a nivel de seguridad en base a las medidas aplicadas, además de los componentes tecnológicos que posee la empresa. En el área de redes, está directamente relacionada al método o conjunto de ellos, que ayudan a verificar el cumplimiento de los requisitos de seguridad necesarios para la gestión de los dispositivos interconectados que las conforman. Sin embargo, puede verse orientada a dos niveles: físico y lógico.

Por un lado, la revisión de seguridad lógica consta de la verificación y evaluación las medidas de protección sobre la información y los procesos. Y a nivel físico, se enfoca en conocer y evaluar los mecanismos de protección del hardware y cableado, de manera que se puedan identificar las debilidades en la infraestructura tecnológica. Es así como la valoración física contempla la revisión de las conexiones y apego a las normas de cableado estructurado establecidas por los comités como ISO, las medidas y controles aplicados en los dispositivos y servidores.

Anteriormente, las actividades de las organizaciones carecían de estándares y métodos, y el personal en el ámbito informático realizaba los procesos de acuerdo a sus propios criterios, a su propia manera de ver las cosas, generando de esta manera inconsistencia y oposición a la hora de realizar sus operaciones y lograr así los objetivos planteados.

Por lo tanto, el establecimiento de los estándares y normas de seguridad a nivel físico de las redes, es sumamente importante por los beneficios que la misma otorga a las organizaciones, ya que permiten desarrollar productos y servicios de calidad, el resguardo de uno de los principales activos de la empresa (datos e información), diligenciar el uso adecuado de las tecnologías de información (TI). Además, el establecimiento de los estándares para la gestión de la seguridad de las redes, le proporcionan: el rendimiento de la red de acuerdo a las necesidades y requerimientos de la empresa, el aumento y estabilidad de la confiablidad de la red, reducción de riesgos por implantaciones y actualizaciones en la red y el aumento de la complacencia del cliente tanto internos como externos.

La ejecución de una auditoría de la infraestructura y seguridad de las redes LAN/WAN de los hoteles Lidotel y Tibisay, es sumamente importante para dicha organización, ya que tiene como finalidad mejorar los controles y estándares para el resguardo de sus activos e información. Además, permite detectar las vulnerabilidades existentes, y minimizar los posibles riesgos en la infraestructura, garantizando de esta manera la privacidad de sus datos y la continuidad de los servicios de sus redes, también, la disponibilidad e integridad de los mismos. De igual manera,

contribuirán a la mejora de procesos y madurez de las empresas, debido a que se deben documentar, comunicar, monitorear y medir.

Por lo tanto, al ejecutar estas prácticas se visualizará si es óptima y eficiente la presencia de la auditoría en los hoteles Lidotel y Tibisay ubicados en el estado Nueva Esparta, con el fin de validar la integridad de la información. La relevancia para esta academia también se encuentra en las propuestas dirigidas a corregir los riesgos presentes, con el fin de mejorar la calidad y entrega de los desarrollos y servicios, orientándolos a los estándares y normas internacionales como ISO 27000-1, COBIT y COSO. De igual manera, los integrantes de estos hoteles, así como los clientes, se verán favorecidos y beneficiados porque se determinará las acciones correctivas y preventivas necesarias para mantener a dicha infraestructura confiable y disponible.

PARTE II

DESCRIPCIÓN TEÓRICA

Diversos autores han definido al marco teórico como el conjunto de información que sustenta el trabajo de investigación, recolectando así consideraciones teóricas previas al mismo. Raffino, M. (2020) lo describe como "se trata de un apartado del trabajo de investigación en el cual los autores deberán demostrar en qué autores y libros se basan para elegir el camino investigativo que eligieron". Por otro lado, se dice que es "el soporte teórico, contextual o legal de los conceptos que se utilizaron para el planteamiento del problema en la investigación".

En otras palabras, este marco comprende la recolección documental siendo la base en la que se fundamenta la investigación, análisis, experimento o hipótesis. Asimismo, este se compone de un conjunto de elementos referenciales tales como antecedentes, definiciones teóricas y leyes que regulan el desarrollo de la investigación.

2.1 Antecedentes

González, H (2019) realizó un informe de pasantía titulado: *EVALUACIÓN MEDIANTE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN AMBIENTE WEB Y REDES, CON EL FIN DE DETECTAR RIESGOS Y VULNERABILIDADES DE FORMA QUE SE PUEDAN APLICAR MEDIDAS PREVENTIVAS O CORRECTIVAS OPORTUNAS EN LA EMPRESA SOUTH AMERICAN JETS, CON OFICINAS EN EL CENTRO EMPRESARIAL AB, SECTOR PLAYA EL ÁNGEL, MUNICIPIO MANEIRO, ESTADO NUEVA ESPARTA*. El cual fue realizado con la finalidad de optimizar la calidad de la seguridad de los activos de información que se manejan en la organización, cumpliendo con los estándares de integridad, confiabilidad y disponibilidad de los procesos que se llevan a cabo diariamente dentro de la misma. La auditoría realizada también permite poner en práctica un Sistema de Gestión de la Seguridad de la Información. Este trabajo tuvo como resultado la implementación de un sistema de gestión de seguridad sobre los activos de información manejados y que son responsabilidad de la organización.

Este informe resultó preciso, debido a la disposición de una base robusta para generar una gestión de TI efectiva, asimismo, a las propuestas y recomendaciones que se generaron para minimizar los riesgos y maximizar la seguridad de la información presentes en la empresa. Garantizando de esta manera un sistema seguro y de calidad de los activos de información que se manejan en esta compañía. El mismo, se llevó a feliz término con la implementación de un sistema de gestión. En consecuencia, dicho informe, sirvió de utilidad para esta investigación, ya que proporcionó documentos, referencias y recomendaciones que son de provecho para el óptimo desarrollo del trabajo, además, aportó métodos y técnicas necesarias para detectar peligros y vulnerabilidades en la red, así como, prevenirlas.

Gavino, A (2018) realizó un trabajo de investigación titulado: *AUDITORÍA EN SEGURIDAD INFORMÁTICA Y GESTIÓN DE RIESGO EN EL HOSPITAL REGIONAL DE HUACHO*, el objetivo del trabajo estuvo orientado al análisis en seguridad informática para determinar su relación con la gestión de riesgos en el hospital regional de Huacho; se empleó el método científico en sus niveles de análisis y síntesis y corresponde al diseño no experimental, además es un estudio cuantitativo de investigación. Tuvo como resultado comprobar que la auditoria en seguridad informática tiene una relación directa con la gestión de riesgos.

En el trabajo se presentó, la relación existente entre la auditoría en seguridad informática y la gestión de riesgos en el hospital regional de Huacho, enfocado en el análisis de la seguridad y así como también, la importancia de establecer la gestión de riesgos, en la necesidad que tienen las organizaciones, sean estas grandes o pequeñas, de asegurar y resguardar su información. Es una realidad, que, al aumentar el uso masivo de la tecnología, proporcionalmente aumentan los niveles de vulnerabilidades, amenazas y riesgos de seguridad, por los ataques informáticos en las que se ven expuestos (hacker, troyanos, spyware, entre otros). Motivo por el cual, las organizaciones se ven obligadas a establecer y adoptar procesos de seguridad y una adecuada gestión del riesgo, que les permita identificar administrar, controlar y mitigar los ataques y amenazas existentes, procurando y evitando que sus datos e información sean vulnerados. Esta investigación, aportó, el análisis de la seguridad informática y su relación directa con la gestión de riesgos, entendiendo que ambas se complementan, siendo fundamentales en cada organización, en su enfoque estructurado, brindando una herramienta para el manejo de la incertidumbre, identificación, análisis y evaluación de los diferentes riesgos, utilizando recursos gerenciales, contrarrestando los diferentes ataques,

vulnerabilidades y amenazas, que puedan presentarse en los datos físicos o lógicos, estableciendo las estrategias para su aplicación y poder gestionarlos y controlarlos.

Bermúdez, K y Bailón, E (2015) realizaron un trabajo de investigación titulado: *ANÁLISIS EN SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001- SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DIRIGIDA A UNA EMPRESA DE SERVICIOS FINANCIEROS*, el análisis estuvo dirigido a una empresa financiera, teniendo como objetivo principal el estudio de seguridad en los procesos críticos. A través de reuniones, revisión de documentación, consultas, observación, encuestas y ejecución de entrevistas con directivos que poseen un amplio conocimiento de negocio, se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información. Los resultados obtenidos dan a conocer que, para minimizar los riesgos existentes, es necesario implementar controles de seguridad, lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, la integridad y la disponibilidad de la información.

Este trabajo resultó sumamente importante, debido a su finalidad que era conocer las vulnerabilidades existentes a las que está expuesta la información por la falta de aplicación o utilización de los controles de seguridad, así como, identificar los riesgos presentes en dicha organización. Además, destacaron la importancia que compete establecer o implementar dichos controles de seguridad, con el fin de minimizarlos, fortaleciendo de esta manera la confiabilidad y disponibilidad de la información. El desarrollo de la investigación fue sustentado en la aplicación de la norma Internacional ISO/IEC 27001, que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La contribución de este trabajo resultó oportuno, ya que causa un impacto en la investigación, teniendo como importancia, su aplicación e implementación, así como las técnicas de recolección de datos, como es el caso de cuestionario, encuesta y documentación, utilizados en la recopilar información pertinente, que conlleve al descubrimiento de fallas y riesgos a los que se exponen los datos e información, teniendo de esta manera una base sólida para generar recomendaciones que permitan minimizar dichos riesgos.

Gastón, M (2015) realizó un trabajo de investigación titulado: *AUDITORÍA INFORMÁTICA A LA RED DE DATOS DEL HOSPITAL DE TINGO MARÍA PARA DETERMINAR LA SITUACIÓN ACTUAL EN LA QUE SE ENCUENTRA Y PROPONER MEJORAS QUE GARANTICEN EL*

EFICIENTE FUNCIONAMIENTO DE LA RED CORPORATIVA. El objetivo del trabajo, estuvo orientado a brindar soluciones, planteando métodos y procedimientos de control de los sistemas de información que son válidos para cualquier empresa u organización por pequeña que esta sea. En el mismo, se plantea un estudio exhaustivo de los diversos factores del cableado de red que pueden estar influyendo en la eficiencia de las operaciones de la organización auditada "Hospital de Tingo María", a fin de brindar las recomendaciones pertinentes.

Este trabajo resultó medular, ya que permitió determinar el estado en el que se encontraba el "Hospital de Tingo María", en cuanto a la red de datos, y de esta manera, generar recomendaciones a la alta gerencia, teniendo como premisa principal mejorar y lograr un adecuado control interno en ambiente de tecnología informática con el fin de alcanzar mayor eficiencia operacional y administrativa. Además, incentivando a los directivos a través de propuestas, asegurando la efectividad y un buen funcionamiento de la red. En efecto, este trabajo fue de utilidad para esta investigación, ya que aporta métodos, técnicas e información necesaria para el análisis y estudio exhaustivo de los componentes físicos de la red, que son obtenidos a través del personal que labora en el departamento de sistemas, con el fin de establecer ciertas recomendaciones para el mejoramiento de estos.

2.2 Bases Teóricas

2.2.1 Red informática

La red informática, en términos generales, es definida como un conjunto de equipos o dispositivos interconectados que comparten recursos e intercambian información. En la que interactúan varios roles o elementos de comunicación para que pueda existir el proceso de transmisión y de esta manera fluya la información. "La estructura de las redes informáticas y su modo de funcionamiento se rige a través de los estándares TCP/IP, basados en el modelo OSI" (Alpha Telecom Solutions, 2017).

Por consiguiente, las redes informáticas son aquellas interconexiones que existe entre computadoras por medio de diversos dispositivos alámbricos o inalámbricos que permiten comunicar y/o compartir paquetes de datos o información a través emisión de ondas electromagnéticas u otros medios físicos. Se pueden clasificar según el tamaño o la envergadura de la red, entre las que se pueden mencionar:

- LAN (Local Area Network) o red de área local: es una red cuyo rango de alcance se limita a un área relativamente pequeña, como una habitación, un edificio, un avión, etc. No integra medios de uso público.
- WAN (Wide Area Network) o red de área amplia: se extiende sobre un área geográfica extensa empleando medios de comunicación poco habituales, como satélites, cables interoceánicos, fibra óptica, etc. Utiliza medios públicos.

2.2.2 Infraestructura de redes

Se entiende como infraestructura de red a todos aquellos elementos básicos e imprescindibles para cualquier institución u organización pública o privada (empresa, oficina o industria) que precise todos o algunos de los siguientes servicios de telecomunicaciones: teléfono, fax, ordenador, escáner, impresoras, TPV, cámaras de control y vigilancia, control de accesos, datafonos, climatización, incendio, etcétera. Y los diferentes elementos que conforman la infraestructura de red son:

- Cableado estructurado.
- Alimentación eléctrica equipos de comunicaciones.
- SAI: Sistema de Alimentación Ininterrumpida de equipos de IT.

- Cuarto de comunicaciones.
- Seguridad y control.
- Electrónica de red.

En telecomunicaciones, la infraestructura de redes es aquel conjunto de elementos físicos o servicios tecnológicos que agrupados y organizados proveen conectividad digital, dando soporte a las operaciones de una entidad.

2.2.3 Seguridad informática

Expertos de la Universidad de Valencia, (2018) puntualizan que "el proceso de prevenir y detectar el uso no autorizado de un sistema informático" es la definición precisa de seguridad informática, la cual también "implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente".

La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema, atendiendo a tres clases o divisiones:

- Seguridad de hardware: implica tanto la protección física como el control del tráfico de una red y el escáner constante de un sistema. Algunos ejemplos de seguridad informática de hardware son los cortafuegos de hardware, servidores proxys y claves criptográficas para cifrar, descifrar y autentificar sistemas, copias de seguridad, bancos de baterías para los cortes de electricidad, etc.
- Seguridad de software: dedicada a bloquear e impedir ataques maliciosos de hackers, por ejemplo. La seguridad de software es parte del proceso de la implementación de un programa, trabajo de ingenieros informáticos, para prevenir modificaciones no autorizadas que causen el mal funcionamiento o violación de la propiedad intelectual del programa en sí.
- Seguridad de red: aplicada a través del hardware y el software del sistema. La seguridad en la red protege la facilidad de uso, la fiabilidad, la integridad, y la seguridad de la red y de los datos. Algunos componentes que ayudan en este aspecto son: los antivirus, antispyware,

cortafuegos que cortan el acceso no autorizado, redes privadas virtuales (VPN) y sistema de prevención de intrusos (IPS).

La seguridad informática abarca la prevención y protección, tanto de lo tangible como lo intangible, encargándose de salvaguardar la integridad, fiabilidad y el acceso a los datos o equipos. Por lo que, la seguridad mantiene el hardware y software protegidos mediante el uso de programas de antivirus, firewalls, y otras medidas que restringen o dificultan el acceso a ellos.

2.2.4 Auditoría

Santillana G, Juan R (2000:17) define a la auditoría como:

> Auditoría interna es una función independiente de evaluación establecida dentro de una organización, para examinar y evaluar sus actividades como un servicio a la misma organización. Es un control cuyas funciones consisten en examinar y evaluar la adecuación y eficiencia de otros controles.

Del mismo modo, la actividad de auditar "consiste en realizar un examen de los procesos de la actividad económica de una organización para confirmar si se ajustan a lo fijado por las leyes o los buenos criterios" (Pérez y Gardey, 2012, p.4).

Según Hernández, A (s/f):

> Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Como un concepto general, la auditoría es comprendida como el proceso que permite evidenciar el estado actual en que se encuentran los recursos dentro de una organización, además de identificar los riesgos y los niveles de exposición de la misma. Sin embargo, este proceso va más allá del nivel económico, debido a que, si ocurre alguna irregularidad en otro nivel, igualmente estaría afectándola y generando pérdidas significativas. Partiendo de la evaluación, se determina dónde y cuáles son los problemas, luego se generan recomendaciones que proporcionen una mejora en la realización de sus actividades, conducción de sus operaciones y así dar cumplimiento a los objetivos planteados por la organización, también mediante la implementación de controles se pueden gestionar los riesgos.

2.2.5 Auditoría Informática

Son múltiples las áreas de aplicación de las auditorías. La cantidad de información generada en las organizaciones empresariales es incalculable, junto con las maneras de manejarlas, para que cada departamento pueda funcionar eficientemente debe ser provisto de tecnologías, equipos y software que les permita la mejor manera de manipular la información y que, asimismo sean realizadas sus operaciones y/o actividades. Para que su funcionamiento sea optimo y eficiente, debe cumplir con una serie de criterios, los cuales se verifican mediante la realización de auditorías.

Según Nuño, P (2017, p.3), "la revisión y evaluación de los controles y sistemas de informática, así como su utilización, eficiencia y seguridad en la empresa, la cual procesa la información", su objetivo principal es validar la integridad de la información y datos almacenados, mediante la verificación de controles para así evaluar su efectividad y presentar recomendaciones.

Por medio de este tipo de auditoría, como alternativa de control, seguimiento y revisión, en cuanto a la informatización de procesos y las tecnologías, se evalúa la cantidad de recursos invertidos, la rentabilidad de cada proceso y su eficacia y eficiencia, garantizando una adecuada toma de decisiones.

2.2.6 Auditoría Informática de Comunicaciones y Redes

Lobos, (2005:18) expresa lo siguiente:

> La auditoría de telecomunicaciones es un análisis orientado a proporcionar información y recomendaciones que les permite a las empresas determinar las acciones necesarias para crecer y alcanzar un nivel de rendimiento y disponibilidad de la red, acorde a las necesidades actuales y futuras de su negocio; sin comprometer la seguridad empresarial o institucional.

Las organizaciones hacen uso de los procesos telemáticos, sistemas y redes para llevar a cabo sus fines, también cuando comparten constantemente información entre sus departamentos, sucursales y clientes. Al realizar una auditoría de telecomunicaciones se evalúa el estado de la red, desde la perspectiva de su arquitectura, rendimiento y disponibilidad. Del mismo modo, con ella se busca, como en toda auditoría minimizar los riesgos, pero ésta en las tecnologías de la información.

2.2.7 Auditoria de Seguridad Informática

Es el estudio que comprende el análisis y gestión de los sistemas informáticos de una empresa, llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas

vulnerabilidades que pudieran presentarse en el funcionamiento rutinario de los Servidores, Puestos de Trabajo, Seguridad en el Acceso Remoto y Redes del parque informático de dicha empresa (Grupo Meridian. s/f).

Comprende la evaluación de los sistemas de la organización para analizar las políticas y procedimientos de seguridad definidos por la misma y revisar si son cumplidos, buscando identificar vulnerabilidades, amenazas y riesgos con el fin de minimizarlos o corregirlos.

2.2.8 Metodología

"La metodología es un conjunto de métodos que se siguen en una investigación científica" (Lobos, 2005:67). La metodología se hace necesaria en materias como la informática, ya que sus aspectos son muy complejos y la cual se utiliza en cada doctrina que compone dicha materia, siendo de gran ayuda en la auditoría de los sistemas de información.

2.2.9 Marco de trabajo

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. ISO 27001 puede ser aplicada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.

El punto central de ISO 27001 es resguardar la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los principales problemas que podrían afectar la información (la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (mitigación o tratamiento del riesgo).

Los Objetivos del SGSI son preservar la:

- Confidencialidad.
- Integridad.
- Disponibilidad de la Información.

Además, las cuatro fases que establece la ISO 27001 para constituir un SGSI se basan en el ciclo de mejora continua, llamado ciclo de "Deming".

- Planificación: En esta fase se establecen los objetivos de seguridad de la información que se quieren seguir y realizar un análisis del riesgo a los que se enfrenta la compañía.

- Implementación del Sistema de Gestión de Seguridad de la Información: Implementación de SGSI, se establecen medidas para evitar situaciones perjudiciales como consecuencia de un ciberataque o de un robo de datos.
- Fase de verificación o control: monitorizar el funcionamiento del propio sistema de gestión y controlar que todas las medidas se ponen en marcha correctamente.
- Actuación, mantenimiento y mejora: Esta fase consiste en actuar; quiere decir que la organización tiene que implementar mejoras identificadas en fases anteriores. En el caso de que se hubieran detectado errores que puedan poner en peligro la seguridad de la información, se tendrán que tomar medidas correctoras.

COBIT (Control Objectives for Information and Related Technologies) es un marco de gestión de TI desarrollado por ISACA para ayudar a las empresas a desarrollar, organizar e implementar estrategias en torno a la gestión de la información y la gobernanza. En efecto, su misión es buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores. Los Principios y beneficios de COBIT:

- Cumplir con las necesidades clave de los interesados
- Cubrir la empresa de extremo a extremo.
- Integrar múltiples marcos bajo un paraguas.
- Fomentar un enfoque holístico para los negocios.
- Alejar el gobierno de la administración.

La estructura del modelo COBIT, propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización. ITIL (Information Technology Infrastructure Library), corresponde a una metodología de gestión que propone una serie de prácticas estandarizadas que nos ayudan a mejorar la prestación de un servicio, reorganizando la manera que tiene la empresa de trabajar y en particular, la del departamento de TI.

Además, establece unos estándares que posibilitan el control, la operación y administración de los recursos, además de reestructurar los procesos e identificar las carencias, con el fin de mejorar la eficiencia y conducir a la organización hacia la mejora continua.

El ciclo de vida de ITIL se desglosa en las siguientes fases:

- Estrategia: propone un enfoque de la gestión como una capa estratégica de la compañía, que deja de ser simplemente una burocracia de cumplimentar o acatar.
- Diseño: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
- Transición: se trata del proceso de transición para la implementación de nuevos servicios o de su mejora.
- Operación: cubre las mejores prácticas para la gestión rutinaria.
- Mejora Continua: corresponde a un procedimiento mediante el cual se crea y mantiene del valor ofrecido a los clientes a través de un diseño, transición y operación del servicio optimizado.

2.2.10 Metodología MARGERIT

La metodología MARGERIT es una herramienta de gran ventaja para las empresas, ya que, proporciona un modelo sistemático en el que, mediante el análisis y gestión de riesgos, se obtienen resultados sobre las amenazas y el impacto que pueden acarrear, asimismo, provee medidas de seguridad que ayudan a conocer, minimizar y/o controlarlos.

Esta Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, abreviada como MAGERIT, fue elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información. Ofrece una aplicación para el análisis y gestión de riesgos de un Sistema de la Información.

Se encuentra muy relacionada con la generación en la que se utilizan los medios electrónicos, informáticos y telemáticos, lo que genera grandes beneficios para los empleados y los ciudadanos, aunque también puede dar lugar a diferentes riesgos que se tienen que minimizar con medidas de seguridad que generan confianza. Por lo tanto, se busca facilitar que se pueda llevar a cabo:

El análisis de riesgo en cualquier tipo de Sistema de Seguridad de la Información (SSI), así como todos sus elementos, obteniendo un índice único en el que se realicen las estimaciones de su vulnerabilidad ante todas las posibles amenazas y el impacto que puede generar en la empresa.

La gestión de riesgos, basada en todos los resultados obtenidos durante el análisis realizado, seleccionando medidas de seguridad adecuadas para poder conocer, prevenir, impedir, recudir o controlar todos los riesgos que se identifiquen, pudiendo de este modo reducir al mínimo la potencialidad del riesgo.

Promueve una visión estratégica global de la Seguridad de los Sistemas de Información fundamentada en ISO 27001, comenzando con un modelo de análisis y gestión de riesgos que comprende tres elementos: entidades, eventos y procesos.

Según el Consejo Superior de Administración Electrónica del Gobierno de España (2012), esta metodología persigue los siguientes objetivos:

Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.2.11 Análisis y Controles de riesgo

En la gestión de riesgo se utilizan controles que permitan analizar el funcionamiento, la efectividad y el cumplimiento de las medidas de protección, para determinar y ajustar sus deficiencias. Estos se interrelacionan con las auditorías de sistemas, ya que se utilizan en el proceso de análisis y evaluación, para medir el cumplimiento y la efectividad de las medidas de protección requiere que se levante constantemente registros sobre la ejecución de las actividades, los eventos de ataques y sus respectivos resultados.

El proceso de análisis se cumple su función mediante la aplicación de seis (6) etapas, estas se encargan de registrar una imagen específica de los riesgos a los que se expone una organización. Estas son:

1. Identificación de activos.
2. Evaluación de activos.
3. Identificación de amenazas.
4. Evaluación de amenazas.
5. Identificación de medidas de seguridad existentes.
6. Evaluación de riesgos.

Ahora bien, en cuanto a los controles, Sánchez (2020, pág.) expone la siguiente definición:

> Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Por consiguiente, como proceso sistemático permite determinar por medio de una evaluación la frecuencia con la que pueden llegar a producirse ciertos eventos, es decir se logra saber sus principales vulnerabilidades de sus activos, las amenazas, la posibilidad de ocurrencia y la magnitud de su impacto (las consecuencias). De tal manera se establece el nivel de riesgo de cada evento.

2.3. Bases legales

2.3.1. Constitución de la República Bolivariana de Venezuela. (Publicada en Gaceta Oficial del jueves 30 de diciembre de 1999, Número 36.860)

Art. 156.- Es de la competencia del Poder Público Nacional: (…) 28. El régimen del servicio de correo y de las telecomunicaciones, así como el régimen y la administración del espectro electromagnético (…).

Esta ley abarca las consideraciones a tomar al momento de hacer uso de servicios de telecomunicaciones, así como también se encarga de velar por el cumplimiento de lo adscrito en ella. De tal manera que se brinde protección a todo usuario y operadores que las utilicen. Por consiguiente, al llevar a cabo esta investigación, se comprobó el cumplimiento con los estándares

que de la misma manera tienen por objeto velar por el cumplimiento de los pilares de la seguridad de las tecnologías de la comunicación.

2.3.2. Ley Orgánica de Telecomunicaciones (Publicada en la Gaceta Oficial No. 36.920 de fecha 28 de marzo del año 2000)

Art. 12 - En su condición de usuario de un servicio de telecomunicaciones, toda persona tiene derecho a:

1. Acceder en condiciones de igualdad a todos los servicios de telecomunicaciones y a recibir un servicio eficiente, de calidad e ininterrumpido, salvo las limitaciones derivadas de la capacidad de dichos servicios;

- La privacidad e inviolabilidad de sus telecomunicaciones, salvo en aquellos casos expresamente autorizados por la Constitución o que, por su naturaleza tengan carácter público. (…) 6. Disponer, gratuitamente, de una guía actualizada, electrónica o impresa y unificada para cada ámbito geográfico, relacionada con el servicio independientemente del operador que se trate. Todos los abonados tendrán derecho a figurar en dichas guías y a un servicio de información nacional sobre su contenido, sin perjuicio, en todo caso, del derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías; (…)
- 9. Que en la contratación de servicios de telecomunicaciones se utilicen los modelos de contratos previamente autorizados por la Comisión Nacional de Telecomunicaciones y a obtener copia de los mismos; 10. Que se atiendan a la brevedad y de manera eficaz todas sus solicitudes, quejas o reclamos derivados de la prestación del servicio y, de forma especial, exigir el cumplimiento por parte de los operadores de servicios de telecomunicaciones de parámetros de calidad mínima en la prestación de los servicios que serán establecidos para cada servicio, por la Comisión Nacional de Telecomunicaciones;
- 11. Que se le haga conocer previamente y en forma adecuada la suspensión, restricción o eliminación de los servicios de telecomunicaciones que haya contratado, expresando las causas de tales medidas;

- 12. Que se le haga conocer la existencia de averías en los sistemas de telecomunicaciones que los afecten, el tiempo estimado para su reparación y reclamar por la demora injustificada en la reparación de las averías;
- 13. Acceder a la información en idioma castellano relativo al uso adecuado de los servicios de telecomunicaciones y, al manejo, instalación y mantenimiento de equipos terminales, así como las facilidades adicionales que éstos brinden;
- 14. Que se le proporcione adecuada y oportuna protección contra anomalías o abusos cometidos por los prestadores de servicios de telecomunicaciones o por cualquier otra persona que vulnere los derechos establecidos en esta Ley; (…) 16. Los demás que se deriven de la aplicación de leyes, reglamentos y demás normas aplicables.

Art. 20 - La Comisión Nacional de Telecomunicaciones establecerá, atendiendo a las particularidades del tipo de redes y servicios de que se trate, las Condiciones Generales a las cuales deberán sujetarse los interesados en obtener una habilitación administrativa en materia de telecomunicaciones, de conformidad con las previsiones de esta Ley. En todo caso, de conformidad con los reglamentos respectivos, las Condiciones Generales deberán estar orientadas a garantizar, entre otros aspectos:

1. El cumplimiento por parte de la persona que resulte beneficiaria de la habilitación administrativa de los requisitos esenciales para una adecuada prestación del servicio, el correcto establecimiento o explotación de una red;
2. Mecanismos idóneos para la información y protección de los derechos de los usuarios o contratante de servicios;
3. El adecuado acceso a los servicios por las personas discapacitadas o con necesidades especiales;
4. El comportamiento competitivo de los operadores en los mercados de telecomunicaciones;
5. La utilización efectiva y eficaz de la capacidad numérica;
6. Los derechos y obligaciones en materia de interconexión de redes y la interoperabilidad de los servicios, así como los demás requisitos técnicos y de calidad que se establezcan;
7. La sujeción a las normas ambientales, de ordenación del territorio y urbanismo;

8. El respeto a las normas sobre Servicio Universal, a las medidas adoptadas por razones de interés público y, a la protección de datos de las personas.

A través de este artículo, el Estado venezolano expresa su interés por la prestación de servicios de telecomunicaciones con estándares de calidad. Se plantean garantías basadas en la privacidad de los datos de los usuarios, así como el acceso al servicio y la adecuada documentación para el uso del servicio.

Art. 24 - El Ministerio de Infraestructura, por órgano de la Comisión Nacional de Telecomunicaciones propiciará la convergencia tecnológica y de servicios, siempre que con ello no se desmejore el acceso a los servicios y su calidad.

A través del uso de las tecnologías, se obtienen acceso a servicios de telecomunicaciones que prestan soporte a la ejecución de actividades internas y externas de las instituciones, públicas y privadas, el cual debe ser provisto de manera óptima por el ente de la Comisión Nacional de telecomunicaciones, cumpliendo con lo establecido y enmarcado en la ley. De esta forma, se consta que no fue un impedimento la realización de la auditoría, siempre y cuando no se alteren lo que dictamina la presente ley.

2.3.3. Ley Orgánica de Ciencia, Tecnología e Innovación. (Gaceta Oficial del 3 de agosto de 2005, Nº 38.242)

Art. 9 – Las personas naturales o jurídicas, nacionales o extranjeras, no residentes en el país que deseen realizar investigaciones científicas o tecnológicas en el territorio nacional, deberán realizar un proyecto de investigación enmarcado en los objetivos del Plan Nacional de Desarrollo Económico y Social de la Nación y deberán cumplir con los siguientes requisitos:

1. Estar asociado a una institución oficial nacional.
2. Contar con los permisos correspondientes emitidos por las autoridades nacionales competentes en la materia.
3. Los demás requisitos establecidos en el Reglamento de la presente Ley, sin perjuicio de las obligaciones y sanciones señaladas en el caso de incumplimiento con los extremos de esta Ley y su Reglamento.

Todo aquel individuo no residente que desee llevar a cabo una investigación de carácter científico o tecnológico debe regirse a esta ley, dando cumplimiento a los requisitos adscritos a ella, en caso contrario estará sometido a las sanciones que esta establece. La presente investigación

se ejecutó adscrita a la Universidad de Margarita, como requisito para la obtención del título de la carrera de ingeniería de sistemas.

2.3.4. Ley sobre Protección a la Privacidad de las Comunicaciones. Gaceta Oficial del 6 de diciembre de 1991, Número 34.863)

Art. 1 - La presente Ley tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas.

La Ley sobre Protección a la Privacidad de las Comunicaciones establece, a lo largo de sus artículos, las medidas necesarias para la protección de la privacidad de los usuarios de sistemas de telecomunicaciones en el territorio nacional. Al auditar redes de datos, un punto necesario es la revisión de las acciones en materia de privacidad que afectan a los usuarios de la plataforma.

2.3.5. Ley Especial Contra Los Delitos Informáticos. Gaceta Oficial Nº 37.313, 30 de octubre de 2001)

Art. 21 - Violación de la privacidad de las comunicaciones. Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

En las leyes previamente citadas, por medio de sus artículos que hacen alusión a las telecomunicaciones, se puede constar que no hubo términos legales que imposibilitaron llevar a cabo el desarrollo del análisis y verificación de lo establecido en los estándares de seguridad de la infraestructura de redes LAN/WAN en las empresas.

2.4. Definición de términos

Esta sección, a modo de glosario, busca enriquecer el vocabulario del lector para mejor entendimiento de lo definido en el planteamiento del problema de la investigación en cuestión. De esta manera, se expresan términos con un concepto puntual para ganar mayor claridad del tema tratado.

Activo:

“Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección”. (Magerit, 2012).

Amenaza:

"Acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema" (Tarazona, 2007).

Análisis de Riesgo:

"Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización" (Magerit, 2012).

Auditoría:

"Es un examen y validación del cumplimiento de los controles y procedimientos utilizados para la confidencialidad, integridad y disponibilidad de los sistemas de información" (Auditoria de sistemas, 2001).

Cliente:

"Comprador potencial o real de los productos o servicios" (American Marketing Association, 2009).

COBIT:

"(Control Objetives for Information an Related Technology) Objetivos de control para la información y tecnologías relacionadas" (Wikipedia, 2019).

Confidencialidad:

"Garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información" (Ávila, 2013).

Control:

"Función administrativa por medio de la cual se evalúa el rendimiento" (Robbins, 1996).

COSO:

"(Committee of Sponsoring Organizations), Documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control "(Salvador, 2016).

Datos:

"Representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades" (Wikipedia, 2017).

Disponibilidad:

"Capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información" (Infosegur, 2013).

Dispositivos de comunicación:

"Aquellos que envían y reciben archivos de una computadora a otra" (Criminalística, s/f).

Gestión de Calidad:

"Conjunto de acciones, planificadas y sistemáticas, que son necesarias para proporcionar la confianza adecuada de que un producto o servicio va a satisfacer los requisitos dados sobre la calidad" (ISO 9001:2000).

Gestión de Riesgo:

"Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados" (Magerit, 2012).

Gestión de Tecnología de Información:

"Proceso de supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información dentro de una organización" (Rouse y Lebeaux, 2014).

Eficiencia:

"Relación existente entre los recursos que son empleados para un proyecto y los logros que son obtenidos a través de éste. La eficiencia se consigue en aquellos casos en los que se utiliza un menor número de recursos para poder conseguir un mismo objetivo" (EUDE, 2019).

Estándar:

"Aquello que puede tomarse como referencia, patrón o modelo" (Pérez J, Merino M, 2017).

Impacto:

"Consecuencia que sobre un activo tiene la materialización de una amenaza" (Magerit, 2012).

Incidente de seguridad:

"Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad" (Mintic, s/f)

Información:

"Significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas" (Ley de delitos informáticos, 2001).

Infraestructura:

"Conjunto de servicios, medios técnicos e instalaciones que permiten el desarrollo de una actividad" (Raffinbo, 2020).

Infraestructura de redes:

"Conjunto de recursos de hardware y software necesario para cualquier empresa o industria que utilice servicios de telecomunicaciones e internet" (Raffino, 2020).

Integridad:

"Capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización". (Infosegur, 2013).

ISACA:

"(Systems Audit and Control Association), asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información". (Wikipedia, 2019).

ISO:

"Organización Internacional para la Estandarización, que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales". (Bembibre, 2009).

ITIL:

"Information Technology Infraestructure Library (ITIL), metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas de Información y Tecnologías de Información". (Donoso, 2006).

Marco de trabajo:

"(Del inglés framework), Conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar" (Wikipedia, 2013).

Matriz de Riesgo:

"Herramienta visual que le permite ver rápidamente qué riesgos deben recibir la mayor atención (Monise, 2019).

Metodología:

"Modelo aplicable que deben necesariamente seguir los métodos de investigación, aun cuando resulten cuestionables" (Raffino, 2020).

Mitigación:

"Limitación de cualquier consecuencia negativa de un suceso particular" (UNE-ISO Guía 73, 2010).

Normalización:

> "Actividad que consiste en establecer, con respecto a problemas reales o potenciales, disposiciones destinadas a usos comunes y repetidos, con el fin de obtener un nivel de ordenamiento optimo en un contexto dado". (Soteldo, 2015).

Políticas:

"Actividad de un grupo acotado que toma las decisiones para concluir con una serie de objetivos" (Raffino M, 2020).

Protocolo:

"Reglamento o una serie de instrucciones que se fijan por tradición o por convenio" (Pérez y Merino, 2013).

Recursos:

"Medios que las organizaciones poseen para realizar sus tareas y lograr sus objetivos: son bienes o servicios utilizados en la ejecución de las tareas de la organización" (Mesa, 2020).

Riesgo:

"Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización". (Magerit, 2012).

Seguridad:

"Mide la ausencia de amenazas a los valores adquiridos; en el sentido subjetivo, la ausencia de miedo a que dichos valores pudieran destruirse. Estar seguro sería, pues, encontrarse libre de miedos y, a la vez, libre de necesidades". (Wolfers, 1962).

Sistema:

"Conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo" (Alegsa 2018).

Sistema de Información:

"Conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones" (Peña, 2006).

Sistema Informáticos:

"Sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático" (Wikipedia, 2010).

Tecnologías de la información:

"Dispositivos, herramientas, equipos y componentes electrónicos, capaces de manipular información que soportan el desarrollo y crecimiento económico de cualquier organización" (Thompson y Strickland, 2004).

Usuario:

"Puede ser tanto una persona como una computadora o una aplicación, ya que el concepto está vinculado al acceso a ciertos recursos o dispositivos" (Pérez y Gardey, 2010).

Verificación:

"Proceso que se realiza para revisar si una determinada cosa está cumpliendo con los requisitos y normas previstos" (Pérez J, Merino M, 2011).

Vulnerabilidad:

"Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza". (Magerit, 2012).

PARTE III

DESCRIPCIÓN METODOLÓGICA

Todo trabajo de investigación debe fundamentarse en un marco metodológico, que se puede describir como los mecanismos utilizados para el análisis de la problemática de investigación, además, es el resultado de la aplicación, sistemática y lógica, de los conceptos y fundamentos expuestos en el marco teórico. Asimismo, se describe el análisis del tema, los métodos, técnicas o procedimientos. Se da una visión clara de lo que se hizo, por qué y cómo. También, se resalta la adecuación de la metodología elegida, así como sus limitaciones. Según Finol y Camacho (2008, p. 60), el marco metodológico está referida al "cómo se realizará la investigación, muestra el tipo y diseño de la investigación, población, muestra, técnicas e instrumentos para la recolección de datos, validez y confiabilidad y las técnicas para el análisis de datos". Esto quiere decir que, se definen los métodos, técnicas e instrumentos a utilizar en el estudio que se desarrolla.

3.1. Naturaleza de la investigación

Hace referencia al enfoque de investigación, la cual se clasifica como cuantitativa, cualitativa o mixta; y abarca el proceso investigativo en todas sus etapas: desde la definición del tema y el planteamiento del problema de investigación, hasta el desarrollo de la perspectiva teórica, la definición de la estrategia metodológica, y la recolección, análisis e interpretación de los datos (Mata, 2019). La investigación cuantitativa, es la investigación empírica sistemática de fenómenos observables a través de técnicas estadísticas, matemáticas o computacionales, esto quiere decir que, consiste en un conjunto estructurado de preguntas que se incluyen la mayoría de los casos en un cuestionario y que van dirigidas a un grupo de la población, o a una muestra representativa de la misma, para conocer su opinión y sus actitudes sobre un tema, hecho o fenómeno determinado. Este tipo de investigación es cuantitativa ya que, su propósito estuvo direccionado hacia hallar leyes generales que expliquen la naturaleza de su objeto de estudio a partir de la observación, la comprobación y la experiencia.

3.2. Tipo de investigación

La presente investigación realizada se fundamentó en una investigación evaluativa, según menciona Haro, J (s/f), tiene como objetivo evaluar los resultados de uno o más programas que

hayan sido o estén aplicados dentro de un contexto determinado. La intención fue medir los efectos de un programa por comparación con las metas propuestas, a fin de tomar decisiones para mejorar la ejecución futura.

Por lo antes expuesto, se define que el presente caso es de tipo evaluativo, en donde se obtuvo información útil y descriptiva con la cual se fundamentaron las recomendaciones que brindaron la mejora de controles de seguridad de la infraestructura de redes LAN/WAN de los hoteles.

3.3. Diseño de la investigación

Según Arias (2004), la investigación de campo "consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variables algunas" (p. 94).

Del mismo modo, el autor Arias, F (2012) define la investigación documental como:

> Un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos (pág. 27).

Para esta investigación se utilizó el diseño de investigación de campo y documental, debido a que los hechos son estudiados tal como ocurren en la realidad apoyados en fuentes secundarias, es decir, documentales, además de fuentes primarias, obtenidas a través de observación y revisión de documentos.

3.4. Población y muestra

Se habla de población como el número de habitantes que integran un estado, ya sea el mundo en su totalidad, o cada uno de los continentes, países, provincias o municipios que lo conforman; y pueden referirse también a aquel acto poblacional que significa dotar de personas a un lugar. Según Tamayo y Tamayo, (1997), "la población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación" (pag.114).

Debe señalarse que, del universo de los hoteles distribuidos en el Estado Nueva Esparta, el cual corresponde a cuarenta y cuatro (44) hoteles aproximadamente, la población seleccionada fueron los departamentos de sistemas de los hoteles Lidotel y Tibisay, los cuales están estructurados o

conformados por 2 empleados en la sede de Lidotel Hotel Boutique Margarita en el Centro Comercial Sambil Margarita y por parte del hotel Tibisay. Hotel Boutique un solo empleado.

Ahora bien, muestra es la que puede determinar la problemática, ya que le es capaz de generar los datos con los cuales se identifican las fallas del proceso. Tamayo y Tamayo (1997), afirma que, "la muestra es el grupo de individuos que se toma de la población para estudiar un fenómeno estadístico" (pág. 38).

Para efecto de esta investigación, la muestra estuvo representada por la totalidad de la población para que esta fuese representativa. Por lo que estando el departamento de sistemas de ambos hoteles comprendidos por 2 empleados (jefe de sistemas y coordinador de sistemas en el caso de Lidotel), y un jefe de sistemas en el Tibisay, la muestra 3 empleados en su totalidad.

3.5 Técnicas de recolección de datos

Méndez (1999, p.143) define a las fuentes y técnicas para recolección de la información como "los hechos o documentos a los que acude el investigador y que le permiten tener información". También señala que las técnicas son los medios empleados para recolectar información, además manifiesta que existen: fuentes primarias y fuentes secundarias. Esto quiere decir que, son técnicas que le permitirán al investigador obtener información necesaria para dar cumplimiento a sus objetivos de investigación.

Por consiguiente, para esta investigación las técnicas de recolección de datos que se utilizaron fueron, la revisión documental, observación directa y entrevistas. Por lo cual, cada una de estas técnicas se llevaron a cabo para obtener información oportuna, relevante y pertinente y así dar respuesta a los objetivos planteados. En efecto, la revisión documental se describe como la acción de revisar la información de manera objetiva y sistemática seleccionando los contenidos relevantes, según sea la variable a estudiar. Se empleó para recopilar la información necesaria para el desarrollo de este trabajo, la consulta de libros, tesis de grados, manuales, normas, páginas de internet, entre otros. Esta técnica, se utilizó con el fin de obtener información documental referente a los estándares y metodologías internacionales, lo que permitió efectuar el análisis de la infraestructura actual de los hoteles, así como, conocer las políticas de seguridad establecidas para la instalación de redes LAN/WAN de la empresa y su cumplimiento con los estándares.

Por otro lado, la observación es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis. La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Mediante ello, se pudo obtener una información más veraz de la infraestructura de datos y la seguridad física del lugar, además, el contacto directo con el personal proporcionó mejores resultados a la recolección de los datos.

Asimismo, se hizo uso de la entrevista, la cual es un intercambio de ideas u opiniones mediante una conversación que se da entre una, dos o más personas donde un entrevistador es el designado para preguntar. El objetivo de las entrevistas es obtener determinada información, ya sea de tipo personal o no. La entrevista estructurada se centra en la precisión de las diferentes respuestas, gracias a las cuales se pueden recopilar datos extremadamente organizados; cada encuestado tiene diferentes respuestas a la misma estructura de preguntas. Por medio de esta técnica, se consiguió datos referentes al estado actual de la infraestructura de las redes LAN/WAN de la muestra seleccionada. Esto se hizo utilizando como instrumento el cuestionario, que según Fidias Arias (2004) señala que, "el cuestionario es una modalidad de encuesta. Se realiza de forma escrita con serie de preguntas". (p.72). Por lo tanto, las preguntas realizadas al personal del departamento de sistema, constaron aproximadamente de cincuenta y cinco (55) interrogantes.

3.6 Técnicas de análisis de datos

Las técnicas de análisis de datos son herramientas útiles para organizar, describir y analizar los datos recogidos con los instrumentos y técnicas de investigación, esto consiste en la realización de las operaciones a la que el investigador someterá los datos con la finalidad de alcanzar los objetivos de estudio, que según Arias (2004), "en este punto se describen las distintas operaciones a las que será sometidos los datos que se obtengan" (p.99).

Por ende, la presente investigación se basó en una de las técnicas de análisis de datos, la cual consistió en la validación de contenido y criterio, que permitió comprobar la calidad de un instrumento o técnica de recolección de datos a emplear, a fin de conocer el punto de vista o el criterio que tengan las personas, con la finalidad de generar conclusiones y recomendaciones. A esto también se le puede conocer como un análisis deductivo-crítico, obteniendo juicios a partir de hechos y generando criterios para el mejoramiento de funcionamientos de sus procesos.

Por consiguiente, al llevar a cabo la evaluación mediante auditoría se hizo uso del marco de trabajo ITIL, este recoge un conjunto de buenas prácticas para la gestión de servicios TI, comprendiendo desde los procesos, requerimientos técnicos y operacionales, gestión estratégica, de operaciones y finanzas. Sin embargo, esta aplicación fue a nivel de infraestructura, servicios de TI, control y gestión de seguridad. ITIL también es definido como un estándar que unifica fundamentos del ISO/IEC 20000 y COBIT para obtener un fluido y eficiente soporte de las necesidades de las organizaciones.

A través de la recolección de datos se pasó a registrar las incidencias encontradas, ineficiencias y malas implementaciones de las prácticas de TI que perjudican el trato a la tecnología de la organización, con las que se establecieron recomendaciones orientadas a la corrección de errores y lograr el cumplimiento de los objetivos propuestos por la institución. De tal modo que mediante ITIL, se verificó la calidad de los servicios de TI en los hoteles.

PARTE IV

ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Identificación de los marcos de trabajo por los cuales se rigen los hoteles Lidotel Hotel Boutique Margarita y Tibisay Hotel Boutique para la gestión de la seguridad y de riesgos de las infraestructuras de redes LAN/WAN.

El marco de trabajo es el patrón o prácticas que siguen las empresas para llevar a cabo sus operaciones, gestionar y controlar los procesos, de manera estandarizada, en este caso se buscó conocer los marcos de trabajos por los que se rigen los hoteles Lidotel y Tibisay para la gestión de la seguridad y riesgos en sus infraestructuras de redes actualmente. Para ello, se realizó una encuesta, con preguntas abiertas y cerradas, al jefe del departamento de sistemas de cada hotel, con el fin de obtener información acerca del marco implementado y su cumplimiento dentro de la organización.

Por otro lado, se procede a comparar los marcos de trabajo con el fin de dar a conocer las variaciones del campo de aplicación de cada uno de estos estándares.

Tabla 1. Cuadro comparativo de los marcos de trabajos.

Marcos de trabajo / Criterios	ISO	COBIT	ITIL
Infraestructura de red	ISO 27001 se basa en el ciclo PHVA: 1. Planificar 2. Hacer 3. Verificar 4. Actuar Todo se integra de forma perfecta con el enfoque de gestión de seguridad de la red.	Se basa en la: 1. Planificación y organización 2. Adquirir e implementar 3. Entregar y dar soporte 4. Monitorear y evaluar	La Infraestructura de TI es definido en ITIL V3: 1. Desarrolla 2. Prueba 3. Entrega 4. Monitorea 5. Controla 6. Da soporte
Niveles de Seguridad	1. El sentido común. 2. El cumplimiento de la legislación obligatoria. 3. Evaluación del proceso de Gestión de Seguridad. 4. Analizar el riesgo y la gestión de su resolución. 5. Adquisición de productos para integrarlos en los Sistemas de Gestión.	COBIT, tiene una guía básica para definir, operar y monitorear un sistema de gestión de seguridad: 1. APO13: Gestión de la seguridad. 2. DSS04: Gestión de la continuidad. 3. DSS05: Gestión de servicios de seguridad.	1. Diseño de controles de seguridad. 2. Pruebas de seguridad. 3. Gestión de incidentes de seguridad. 4. Revisión de seguridad.

Marcos de trabajo Criterios	ISO	COBIT	ITIL
	6. Integración de los componentes certificados en sistemas compuestos y su certificación.		
Disponibilidad de Servicios en Redes	Para la calidad y disponibilidad se especifica los derechos de acceso a cada red, los medios autorizados para dicho acceso, define los procedimientos adecuados para obtener la autorización de derechos de acceso y los controles implantados para protegerse sobre el acceso no autorizado.	Uno de los procesos de soporte que permiten la ejecución eficaz y eficiente de estos sistemas de TI, son: • DSS02 Gestionar las Peticiones y los Incidentes del Servicio. Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. • DSS05 Gestionar los Servicios de Seguridad. Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad.	ITIL Cuenta con una guía de procesos, esta guía alberga: • Gestión en nivel de servicios: trata de mantener un nivel óptimo de servicio al cliente y que el mismo disponga de un buen servicio en todo momento. • Gestión de seguridad: Asegurar la confidencialidad, la integridad y la disponibilidad de las informaciones, datos y servicios de TI de una organización.

Fuente: Elaboración Propia. 2021.

De acuerdo a lo anterior se presenta la escala de valores que pondera los resultados adquiridos en la evaluación de auditoría representada por:

Tabla 2. Ponderación del marco de trabajo e infraestructura.

INFRAESTRUCTURA		
Ponderación		**Descripción**
No cumple	0	No cumplen con los estándares internacionales de infraestructura de redes.
Deficiente	1	Conocen los estándares, pero no lo aplican en todos los procesos.
Suficiente	2	Cumplen con las políticas y controles de seguridad para la protección de sus redes, pero existen detalles que deben mejorar.
Excelente	3	Utilizan marcos de trabajos y tienen estandarizados sus procesos.

Fuente: Elaboración Propia. 2021.

Tabla 3. Nivel de aplicación de marco de trabajo en LIDOTEL.

Segmento/Rubros0	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Marco de trabajo	**OBJETIVO Nº1** Comprobar el nivel de aplicación del marco de trabajo dentro del hotel	1. ¿Tienen conocimiento de algún estándar internacional?			2		**7**	**15**	**47%**
		2. ¿Se rigen por algún estándar internacional, para la gestión de redes? ¿Cuál es el marco de trabajo por los que se rigen actualmente?				3			
		3. ¿Tienen políticas y controles definidos para la gestión y control de la seguridad en sus redes?			2				
		4. ¿Qué certificados avalan el seguimiento del marco de trabajo?	0						
		5. ¿Cuál es la última actualización de la normativa por la cual se rigen?	0						
		TOTAL	**0**	**0**	**4**	**3**			

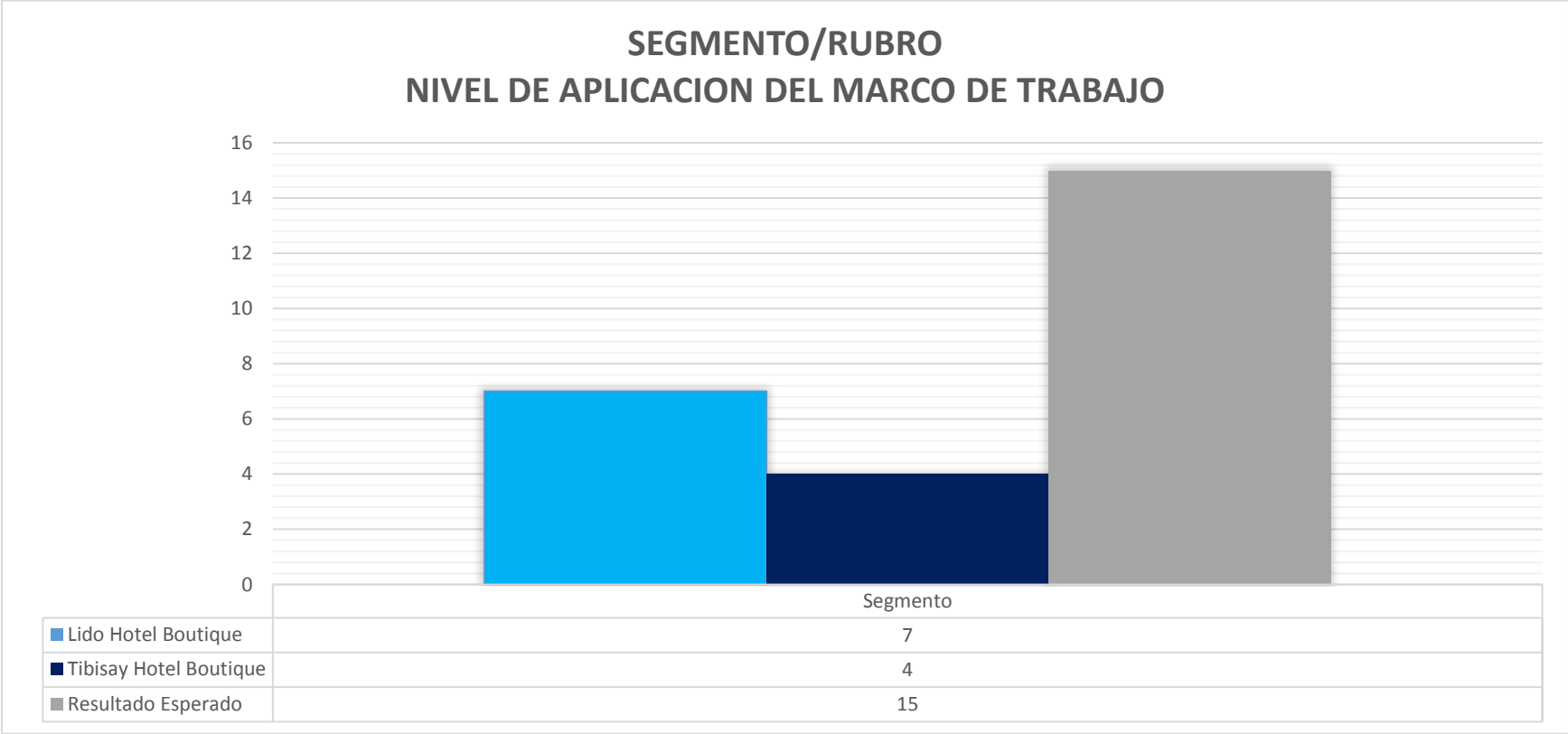
Fuente: Cuestionario realizado al departamento del hotel LIDOTEL. Elaboración Propia. 2021.

Tabla 4. Nivel de aplicación del marco de trabajo en TIBISAY.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Marco de trabajo	**OBJETIVO Nº1** Comprobar el nivel de aplicación del marco de trabajo dentro del hotel	1. ¿Tienen conocimiento de algún estándar internacional?			2		**6**	**15**	**27%**
		2. ¿Se rigen por algún estándar internacional, para la gestión de redes? ¿Cuál es el marco de trabajo por los que se rigen actualmente?		1					
		4. ¿Tienen políticas y controles definidos para la gestión y control de la seguridad en sus redes?		1					
		5. ¿Qué certificados avalan el seguimiento del marco de trabajo?	0						
		6. ¿Cuál es la última actualización de la normativa por la cual se rigen?	0						
		TOTAL	**0**	**2**	**4**	**0**			

Fuente: Cuestionario realizado al departamento del hotel TIBISAY. Elaboración Propia. 2021.

Gráfico 1. Nivel de aplicación del marco de trabajo en los hoteles LIDOTEL y TIBISAY.



Fuente: Elaboración propia. 2021.

Análisis e interpretación.

De los datos ilustrados en el gráfico anterior, se pudo apreciar que, en ambos hoteles, sus empleados del departamento de sistemas, tienen conocimientos sobre los Marcos de trabajo y se rigen por un estándar internacional para la gestión de servicios de TI y otro para la seguridad de los datos. Por lo que los resultados obtenidos mediante la ponderación fueron un siete (7) equivalente a un 54% por parte de Lidotel, lo cual dejó en evidencia que conocen y siguen un estándar para la gestión de los servicios de TI (ITIL), pero no lo aplican en todos sus procesos, debido a que en las respuestas dadas fueron contradictorias al momento de definir el estándar. No obstante, en cuanto a las certificaciones y actualizaciones respecta, no tienen aval que justifique su aplicación.

En cambio, el hotel Tibisay cuenta con un (4) que corresponde a un 46% respectivamente al conocimiento y la aplicación del marco de trabajo, para la seguridad de la información dado que se rigen actualmente por ISO 27000-1. Sin embargo, tampoco cuentan con una certificación.

Dando a demostrar que el resultado que se obtuvo en ambos hoteles está por debajo de lo deseado (15), debido a que, para obtener un buen rendimiento en los procesos empresariales y desarrollo de sus actividades, deben estandarizar todas sus operaciones.

4.2 Análisis de la infraestructura actual, los controles y gestiones realizadas alineadas a los estándares internacionales.

La infraestructura es la unión de elementos básicos e imprescindibles para cualquier institución u organización pública o privada (empresa, oficina o industria) que precise todos o algunos de los siguientes servicios de telecomunicaciones: teléfono, fax, ordenador, escáner, impresoras, TPV, cámaras de control y vigilancia, control de accesos, datafonos, climatización, incendio, entre otros. La manera en la que se gestionan las tecnologías de la información comprende un conjunto de lineamientos establecidos por organizaciones de estandarización (ISO, ANSI, IEEE, entre otros), siendo los puntos de partida de todo protocolo de actuación para el control y gestión de los recursos empresariales.

Tabla 5. Descripción de la infraestructura, controles y gestiones alineados a los estándares LIDOTEL.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Infraestructura, controles y gestiones	**OBJETIVO Nº2** Describir la infraestructura de red actual y examinar la implementación de estándares, para los controles y gestiones	7. ¿Cuál es el tipo de red que utilizan actualmente?				3	**18**	**24**	**75%**
		8. ¿Cuáles son los tipos de redes inalámbricas que usan?			2				
		9. ¿Qué topología de red usan?			2				
		10. ¿Qué tipo de cables usan en estos momentos?				3			
		11. ¿Qué tipo de marco de trabajo utilizan para un sistema de cableado?			2				
		12. ¿Están los cables de los ordenadores recogidos?				3			
		13. ¿Están identificados los conectores de corrientes de los equipos?				3			
		14. ¿Cumplen con los estándares internacionales actualmente?	0						
		TOTAL	**0**	**0**	**6**	**12**			

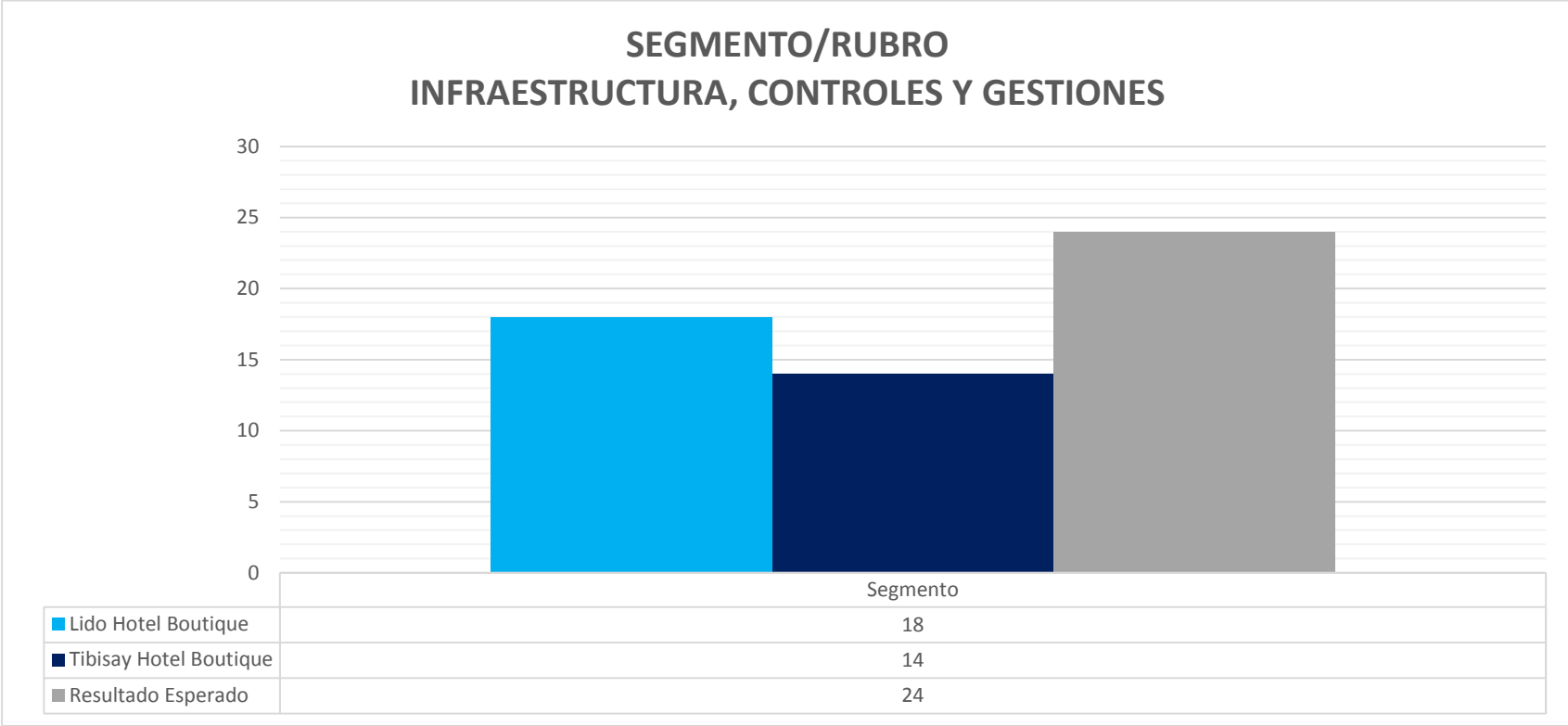
Fuente: Cuestionario realizado a los empleados del departamento del hotel LIDOTEL. Elaboración Propia. 2021.

Tabla 6. Descripción de la infraestructura, controles y gestiones alineados a los estándares TIBISAY.

Segmento /Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Infraestructura, controles y gestiones	**OBJETIVO Nº2** Describir la infraestructura de red actual y examinar la implementación de estándares, para los controles y gestiones	7. ¿Cuál es el tipo de red que utilizan actualmente?		1			**14**	**24**	**58%**
		8. ¿Cuáles son los tipos de redes inalámbricas que usan?		1					
		9. ¿Qué topología de red usan?		1					
		10. ¿Qué tipo de cables usan en estos momentos?			2				
		11. ¿Qué tipo de marco de trabajo utilizan para un sistema de cableado?			2				
		12. ¿Están los cables de los ordenadores recogidos?				3			
		13. ¿Están identificados los conectores de corrientes de los equipos?				3			
		14. ¿Cumplen con los estándares internacionales actualmente?		1					
		TOTAL	**0**	**4**	**4**	**6**			

Fuente: Cuestionario realizado a los empleados del departamento del hotel TIBISAY. Elaboración Propia. 2021.

Gráfico 2: Descripción de la infraestructura, controles y gestiones alineados a los estándares en los hoteles LIDOTEL y TIBISAY.



Fuente: Elaboración Propia. 2021.

Análisis e interpretación.

De los datos recolectados se obtuvieron los resultados mostrados anteriormente, donde se determinó la topología, la extensión de su infraestructura física, entiéndase todos los componentes que conforman la red (cableado, dispositivos, entre otros) y los estándares que siguen en la instalación de su infraestructura. Dando como resultado un dieciocho (18) cuyo equivalente en porcentaje es 75% por parte del hotel Lidotel, este cuenta con una red LAN que se encarga de suministrar servicios en la sede del Sambil Margarita, igualmente para abarcar sus otras sucursales hacen uso de servicios de redes WAN. Cabe destacar, que dicho hotel no cuenta con personal en el área, lo cual al momento de realizar las actividades referentes a las operaciones de seguridad y la atención de estos de los requerimientos se realizan con demora.

Además, especificaron que los usuarios que tienen acceso a las redes inalámbricas son numerosos, entendiéndose como empleados y huéspedes, por lo que se demuestra que los controles de acceso son deficientes, proporcionando un posible vector de ataque y aumentar el nivel de riesgos. Por otro lado, el hotel Tibisay arrojó como resultado de aplicación catorce (14), lo que sería en porcentaje un 58% a lo que refiere a infraestructura de redes, en donde se expuso que su alcance en redes es WAN, aun cuando aclaró que no brinda servicios a otras localidades, también relató que sólo dos (2) empleados tienen acceso a ella, constando que llevan un control, pero no son suficientes para atender a tiempo los requerimientos exigidos.

De los lineamientos establecidos por los estándares internacionales para un sistema de cableado, Lidotel señaló que se rigen por la norma TIA/EIA-568-B, la cual se ocupa de definir los tipos de cables, distancias, conectores, arquitecturas de sistemas de cableado, estándares para los terminales y características de prestación, requerimientos de instalación del cableado, y métodos de comprobación de los cables instalados. Mientras que Tibisay se maneja por la norma EIA/TIA-568-A referida a las topologías, la distancia máxima de los cables, el rendimiento de los componentes, las tomas y los conectores de telecomunicaciones. Ahora bien, ambos hoteles reflejaron que no cumplen con él hoy en día, esto podría generar un impacto en los costes, por muy mínimo que sean, y en el rendimiento de la red, debido a que este sistema es la base principal para la entrega exitosa de aplicaciones dentro del Data Center.

En toda empresa debe existir un medio de comunicación que permita la interacción entre los diversos departamentos, localidades u otras sucursales. Por ello en el cuestionario se tomaron en

cuenta dichas variables, a manera de dejar constancia cuales son los estándares a emplear en gestiones de sus redes. Además, cabe resaltar que la topología que usan ambos hoteles se denomina Árbol, la misma puede acarrear inconvenientes que afecten a su disponibilidad de servicios dado que si se cae el segmento principal (el tronco) todo el segmento también cae. Por lo contrario, puede ser muy útil para poder llevar a cabo una expansión de la red y en la resolución de problemas es más rápido que otras.

4.3 Revisar las políticas de seguridad de TI establecidas para la instalación de redes LAN/WAN de la empresa y su cumplimiento con los estándares.

La forma en la que se manejan, protegen, resguardan y administran la información es a través de protocolos de seguridad. En las redes, los protocolos de seguridad son un tipo de estandar que afianzan la seguridad y la integridad de los datos en circulación a través de una conexión de red como Internet. Estos son esenciales para prevenir o evitar que agentes externos aceden a los datos de la red. Se puede decir que éstas son subjetivas, cada organización es la que establece las políticas, debido a los objetivos, metas y/o expectativas de negocio. En este sentido, se buscó verificar el cumplimiento de las políticas y normas de seguridad de TI por las que actualmente se dirigen los hoteles Lidotel y Tibisay para la instalación de redes LAN/WAN.

A continuación, se presenta la escala de valores que pondera los resultados adquiridos en la evaluación de auditoría representada por:

Tabla 7. Ponderación de la seguridad y controles de riesgos.

SEGURIDAD Y CONTROLES DE RIESGOS		
Ponderación		**Descripción**
No cumple	0	El hotel no cuenta con ningún tipo de seguridad en los medios de telecomunicaciones.
Deficiente	1	Cuenta con ciertos niveles de seguridad, pero no completo dentro de la infraestructura.
Suficiente	2	Posee normalizaciones de seguridad establecidas, que le permiten desempeñar sus funciones, sin embargo, pueden mejorarse.
Excelente	3	Cumple con todos los lineamientos y estándares de seguridad.

Fuente: Elaboración Propia. 2021.

Tabla 8. Clasificación de las incidencias y las formas de gestionarlas en LIDOTEL**.**

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Control y gestión	**OBJETIVO Nº2** Clasificar las incidencias y formas en que se gestionan	15. ¿Existen fallas en las redes?			2		**7**	**15**	**47%**
		16. ¿Cuáles? ¿De qué tipo?			2				
		17. ¿Sobre quién recaen las decisiones del departamento de sistemas?		1					
		18. ¿Cumple otras funciones además de encargarse del departamento de sistemas? ¿Cuáles?		1					
		19. ¿Cuánto tarda en atender un requerimiento?		1					
		TOTAL	**0**	**3**	**4**	**0**			

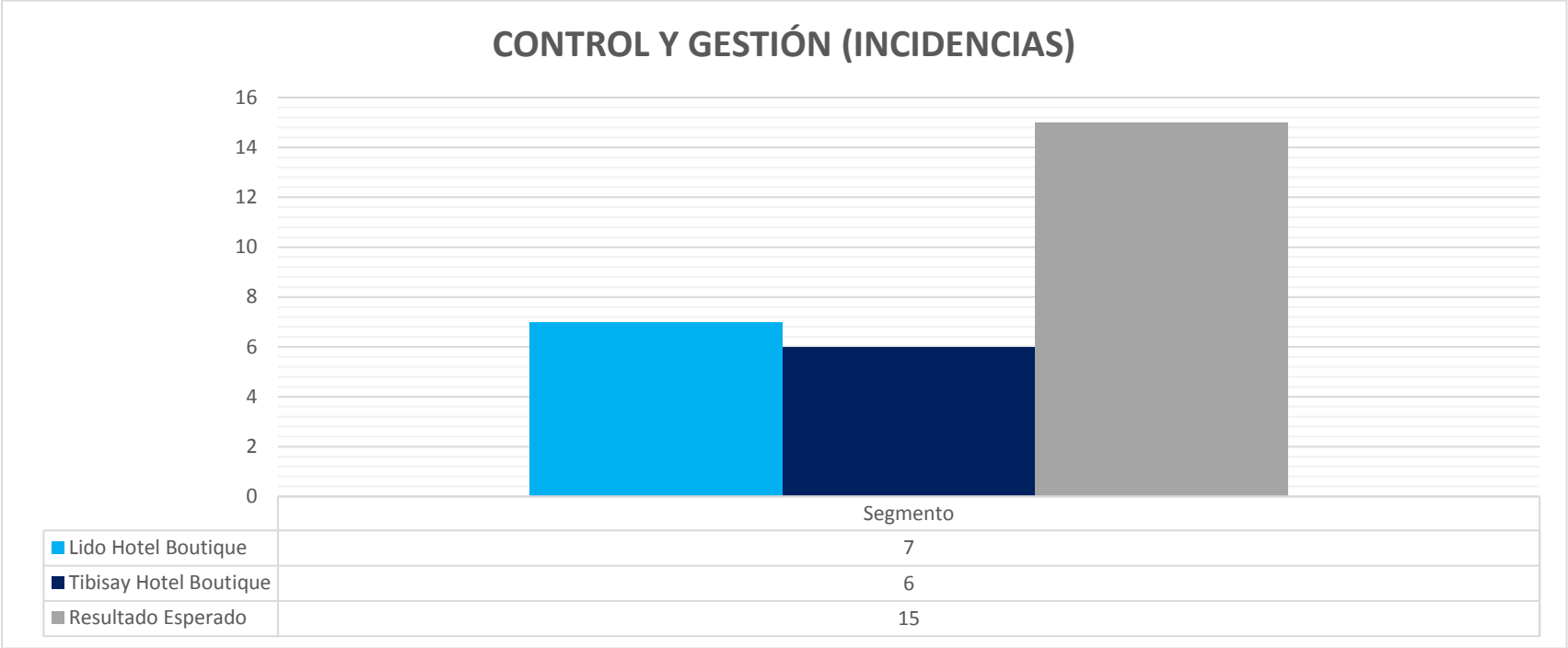
Fuente: Cuestionario realizado al departamento de sistemas de LIDOTEL. Elaboración Propia. 2021.

Tabla 9. Clasificación de las incidencias y las formas de gestionarlas en el hotel TIBISAY**.**

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Control y gestión	**OBJETIVO Nº2** Clasificar las incidencias y formas en que se gestionan	15. ¿Existen fallas en las redes?					**6**	**15**	**40%**
		16. ¿Cuáles? ¿De qué tipo?							
		17. ¿Sobre quién recaen las decisiones del departamento de sistemas?			2				
		18. ¿Cumple otras funciones además de encargarse del departamento de sistemas? ¿Cuáles?				3			
		19. ¿Cuánto tarda en atender un requerimiento?		1					
		TOTAL	**0**	**1**	**2**	**3**			

Fuente: Cuestionario realizado al departamento de sistemas del hotel TIBISAY. Elaboración Propia. 2021.

Gráfico 3: Clasificación de las incidencias y las formas de gestionarlas en los hoteles LIDOTEL y TIBISAY.



Fuente: Elaboración propia. 2021.

Análisis e Interpretación.

En cuanto a la gestión y control de las incidencias y formas, a nivel de redes, entradas y salida de documentos fuente, es atendida, revisada y controlada únicamente por el jefe de sistemas en ambos hoteles, así como también esta persona comprende otros roles en el área, en las que desempeña las funciones de apoyo operativo al departamento de seguridad, CCTV (cámaras) y su mantenimiento, a causa de ello se pudo ver un bajo rendimiento en sus operaciones. Es decir, solventa los problemas, pero no cumplen con el personal necesario para dividirse las actividades y llevar un desarrollo eficiente. Los resultados obtenidos se encuentran entre un seis y siete (6 – 7) correspondientes a un 47% Lidotel y Tibisay 40% siendo esperado un quince (15).

Por otra parte, en relación a roles y funciones de los empleados, se determinó un bajo rendimiento en sus operaciones ya que existe pocos empleados para atender tareas en el departamento de sistemas. Es decir, solventa los problemas, pero no cumplen con el personal necesario para dividirse las actividades y llevar un desarrollo eficiente. En efecto, las operaciones requeridas por el departamento de sistemas de Lidotel se realizan de manera remota. Esto conlleva a que los resultados obtenidos sean nueve (9) Lidotel y Tibisay catorce (14) y su valor esperado quince (15).

Tabla 10. Identificación de los roles y funciones de los empleados del departamento de sistemas de LIDOTEL.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Control y gestión	**OBJETIVO Nº3** Determinar los roles y funciones de los empleados	20. ¿Cuántas personas le reportan, de qué departamento son y cuál es el rol que desempeña cada uno?			2		**9**	**15**	**60%**
		21. ¿Quién controla las entradas de documentos fuente?		1					
		22. ¿En qué forma las controla?			2				
		23. ¿Existe un registro del control?			2				
		24. ¿Quién lo revisa?			2				
		TOTAL	**0**	**1**	**8**	**0**			

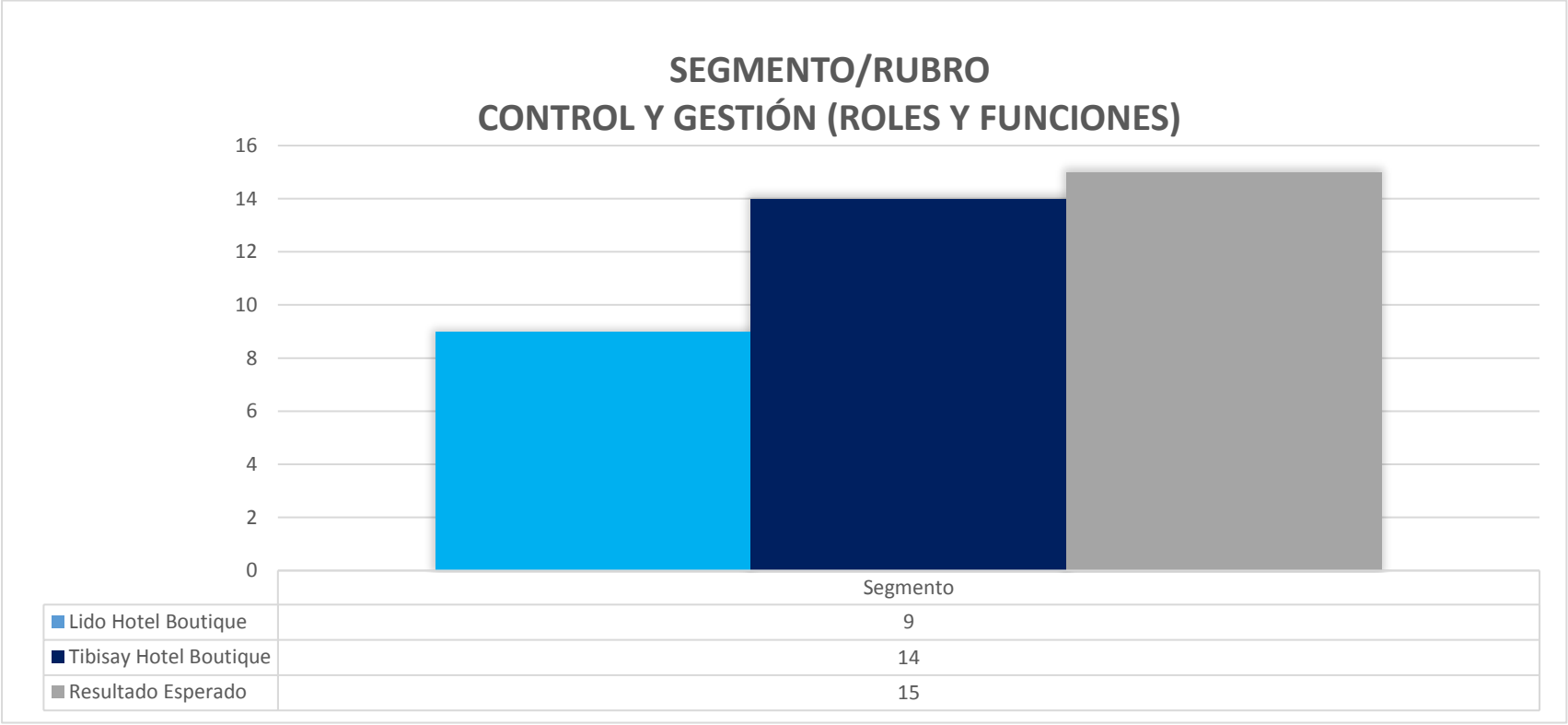
Fuente: Cuestionario realizado al departamento de sistemas del hotel LIDOTEL. Elaboración Propia. 2021.

Tabla 11. Identificación de los roles y funciones de los empleados del departamento de sistemas de TIBISAY.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				TIBISAY HOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Control y gestión	**OBJETIVO Nº3** Determinar los roles y funciones de los empleados	20. ¿Cuántas personas le reportan, de qué departamento son y cuál es el rol que desempeña cada uno?			2		**14**	**15**	**93%**
		21. ¿Quién controla las entradas de documentos fuente?				3			
		22. ¿En qué forma las controla?				3			
		23. ¿Existe un registro del control?				3			
		24. ¿Quién lo revisa?				3			
		TOTAL	**0**	**0**	**2**	**12**			

Fuente: Cuestionario realizado al departamento de sistemas del hotel TIBISAY. Elaboración Propia. 2021.

Gráfico 4. Identificación de los roles y funciones de los empleados del departamento de sistemas de los hoteles LIDOTEL y TIBISAY.



Fuente: Elaboración Propia. 2021.

Tabla 12. Verificación del cumplimiento de las políticas de TI establecidas para la instalación de redes en LIDOTEL.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Seguridad de la red e infraestructura	**OBJETIVO Nº3** Verificar el cumplimiento de las políticas de seguridad de TI establecidas para la instalación de redes por el hotel	25. ¿Qué políticas y/o protocolos de actuación utilizan ante cualquier amenaza?			2		**85**	**108**	**79%**
		26. ¿El centro de cómputo da hacia el exterior?			2				
		27. ¿El lugar donde se ubica el centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos actualmente?		1					
		28. Donde se ubican las redes, ¿Existen materiales que puedan ser inflamables o causar algún daño a los equipos?				3			
		29. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información? ¿Cuáles?				3			
		30. ¿Existen personas responsables de la seguridad en el				3			

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		departamento de sistemas?							
		31. ¿Existe personal de vigilancia en la institución?				3			
		32. ¿Se investiga a los vigilantes cuando son contratados directamente?				3			
		33. ¿La institución posee cámaras de circuitos cerrados?				3			
		34. El edificio donde se encuentra la infraestructura de red está a salvo de: Inundación - Terremoto - Fuego - Sabotaje – Nada		1					
		35. ¿Qué tipo de extintores de fuego existen en la institución?				3			
		36. ¿Se ha adiestrado el personal en el manejo de los extintores?				3			
		37. ¿Se han tomado medidas para minimizar la posibilidad de fuego?				3			

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		38. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños a los equipos?				3			
		39. ¿Existe personal capacitado para el mantenimiento de las redes?			2				
		40. ¿Cada cuánto se hace mantenimiento preventivo a la red?				3			
		41. ¿Cada cuánto se hace mantenimiento correctivo a la red?				3			
		42. ¿Existe alarma para detectar condiciones anormales del ambiente?	0						
		43. Esta alarma está conectada: Al puesto de guardias - A la estación de bomberos - A ningún lado	0						
		44. ¿Existe detector de calor, de humo y de agua?			2				
		45. ¿Existe salida de emergencia?				3			

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		46. Esta puerta solo es posible abrirla: Desde el interior - Desde el exterior – Ambos				3			
		47. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas?				3			
		48. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?				3			
		49. ¿Existe seguridad de acceso físico? ¿De qué tipo?				3			
		50. ¿Los equipos informáticos se encuentran ubicados a una distancia no menor a 30 cm del piso?				3			
		51. ¿En el lugar donde se encuentran los ordenadores existe la presencia de aire acondicionado?				3			
		52. ¿Está en la ubicación correcta?				3			
		53. ¿Tiene alguna falla?				3			

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		54. ¿El cableado se encuentra correctamente instalado?				3			
		55. ¿Los cables están dentro de paneles y canales eléctricos?				3			
		56. ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige?		1					
		57. ¿Cuántos usuarios tienen acceso a las redes?		1					
		58. ¿Cómo calificarías lo controles de riesgos?			2				
		59. Las políticas de seguridad son: Satisfactorias - Aceptables – Deficientes			2				
		60. ¿Se han realizado auditorías de seguridad física anteriormente?	0						
		TOTAL	**0**	**4**	**12**	**69**			

Fuente: Cuestionario realizado al departamento de sistemas de LIDOTEL. Elaboración Propia. 2021.

Tabla 13. Verificación del cumplimiento de las políticas de TI establecidas para la instalación de redes en TIBISAY.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Seguridad de la red e infraestructura	**OBJETIVO Nº3** Verificar el cumplimiento de las políticas de seguridad de TI establecidas para la instalación de redes por el hotel	25. ¿Qué políticas y/o protocolos de actuación utilizan ante cualquier amenaza?			2		**90**	**108**	**86%**
		26. ¿El centro de cómputo da hacia el exterior?			2				
		27. ¿El lugar donde se ubica el centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos actualmente?				3			
		28. Donde se ubican las redes, ¿Existen materiales que puedan ser inflamables o causar algún daño a los equipos?				3			
		29. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información? ¿Cuáles?				3			
		30. ¿Existen personas responsables de la seguridad en el departamento de sistemas?				3			

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		31. ¿Existe personal de vigilancia en la institución?				3			
		32. ¿Se investiga a los vigilantes cuando son contratados directamente?				3			
		33. ¿La institución posee cámaras de circuitos cerrados?				3			
		34. El edificio donde se encuentra la infraestructura de red está a salvo de: Inundación - Terremoto - Fuego - Sabotaje – Nada				3			
		35. ¿Qué tipo de extintores de fuego existen en la institución?		1					
		36. ¿Se ha adiestrado el personal en el manejo de los extintores?			2				
		37. ¿Se han tomado medidas para minimizar la posibilidad de riesgo?				3			
		38. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños a los equipos?							

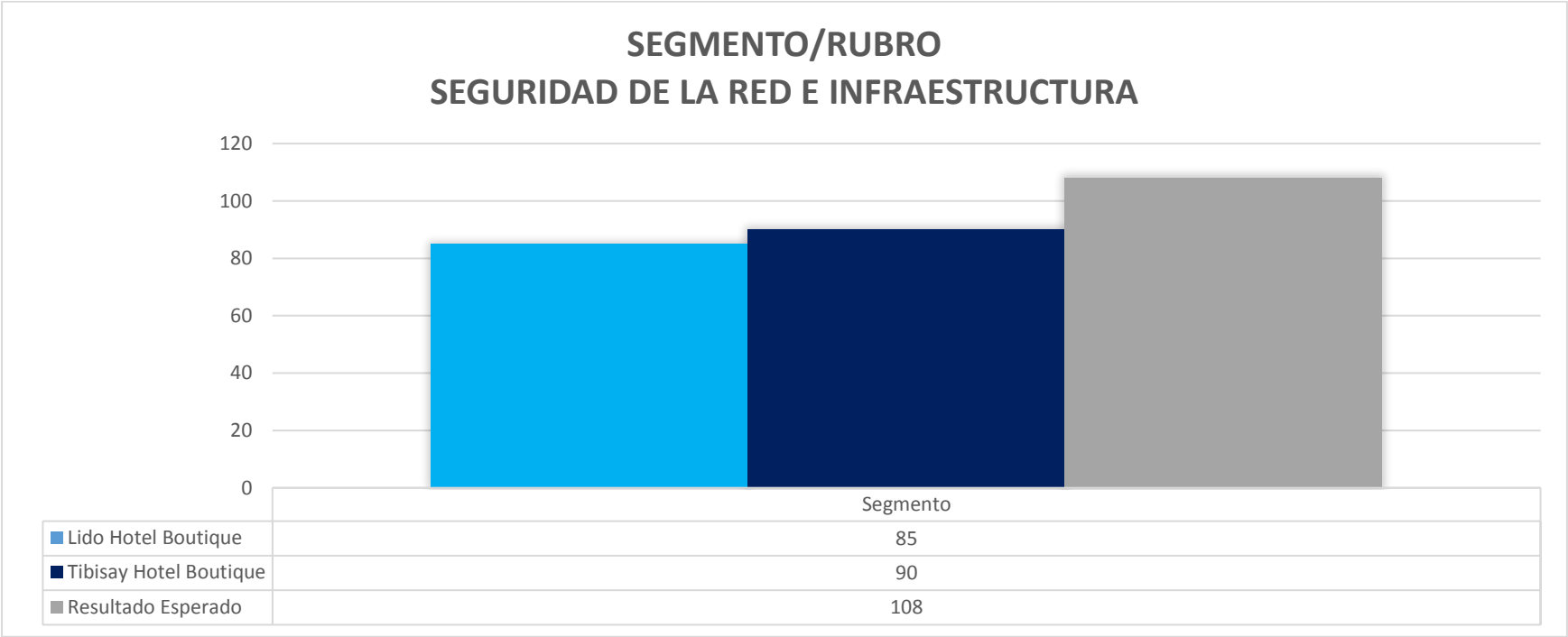
Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		39. ¿Existe personal capacitado para el mantenimiento de las redes?				3			
		40. ¿Cada cuánto se hace mantenimiento preventivo a la red?				3			
		41. ¿Cada cuánto se hace mantenimiento correctivo a la red?				3			
		42. ¿Existe alarma para detectar condiciones anormales del ambiente?				3			
		43. Esta alarma está conectada: Al puesto de guardias - A la estación de bomberos - A ningún lado				3			
		44. ¿Existe detector de calor, de humo y de agua?				3			
		45. ¿Existe salida de emergencia?				3			
		46. Esta puerta solo es posible abrirla: Desde el interior - Desde el exterior - Ambos			2				
		47. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas?				3			

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		48. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?				3			
		49. ¿Existe seguridad de acceso físico? ¿De qué tipo?		1					
		50. ¿Los equipos informáticos se encuentran ubicados a una distancia no menor a 30 cm del piso?				3			
		51. ¿En el lugar donde se encuentran los ordenadores existe la presencia de aire acondicionado?			2				
		52. ¿Está en la ubicación correcta?				3			
		53. ¿Tiene alguna falla?			2				
		54. ¿El cableado se encuentra correctamente instalado?				3			
		55. ¿Los cables están dentro de paneles y canales eléctricos?				3			
		56. ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige?		1					

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				HOTEL TIBISAY		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
		57. ¿Cuántos usuarios tienen acceso a las redes?				3			
		58. ¿Cómo calificarías lo controles de riesgos?			2				
		59. Las políticas de seguridad son: Satisfactorias - Aceptables – Deficientes			2				
		60. ¿Se han realizado auditorías de seguridad física anteriormente?			2				
		TOTAL	**0**	**3**	**18**	**69**			

Fuente: Cuestionario realizado al departamento de sistemas del hotel TIBISAY. Elaboración Propia. 2021.

Gráfico 5: Verificación del cumplimiento de las políticas de TI establecidas para la instalación de redes en los hoteles LIDOTEL y TIBISAY.



Fuente: Elaboración Propia. 2021.

Análisis e interpretación.

Los resultados dieron a conocer que los hoteles establecieron políticas de seguridad de TI para la protección de sus infraestructuras. La aplicabilidad de las políticas dependerá del objetivo que previamente hayan definido, las estrategias desarrolladas e implementadas tienen por labor ayudar a la organización a darle valor a la información y reforzar el resguardo, igualmente contribuyen a la efectividad de entrega de servicios y enseñan a los usuarios para el uso correcto de los servicios de red al interior de la empresa. En Lidotel se afirmó el uso de antivirus y firewall para la prevención y protección de las redes LAN/WAN de ataques e infiltraciones, por medio del bloqueo de acceso. Del mismo modo, el acceso físico está comprendido por diversos mecanismos de seguridad, tales como puertas con combinación, con tarjetas y seguros en puertas y ventanas, el jefe de sistemas expresó que "estadísticamente nunca ha habido infiltraciones, contamos con protocolos que han funcionado, hasta el punto de sufrir rara vez fallas, además se hacen respaldos constantemente en dos sedes". Sin embargo, el porcentaje que se obtuvo fue de ochenta y cinvo (85) correspondiente a un 86%, diferencia de lo esperado (108) puesto que cuentan con ciertos niveles de seguridad, pero no completamente en cuanto a la infraestructura, por más que nunca han realizado auditorías de seguridad física.

Las políticas que estableció el hotel Tibisay se basan en Windows Server, directivas de grupo y firewall, para la gestión y configuración de su red de área amplia, aunque para la seguridad de acceso físico no tienen determinados más que puertas con tarjetas, siendo una vulnerabilidad para posibles infiltraciones y para la seguridad del área poseen un aire que mantiene a los equipos en óptimas condiciones. Es de vital importancia que entre las políticas y normas se establezcan mantenimientos hacia la seguridad física, de los cuales este hotel ya ha realizado previamente. El resultado obtenido fue de noventa (90), por muy poco debajo de los deseado (108), lo que expresó que es suficiente para desempeñar sus funciones.

A continuación, se presenta la escala de valores que pondera los resultados adquiridos en la evaluación de auditoría representada por:

Tabla 14. Ponderación de la calidad de servicios.

CALIDAD DE SERVICIOS		
Ponderación		**Descripción**
No cumple	0	Solventan los problemas, pero no poseen el personal necesario para dividirse las actividades
Deficiente	1	Cuentan con los recursos necesarios, sin embargo, hay poco personal para la entrega y disponibilidad de servicios
Suficiente	2	En cuanto a la disposición de recursos necesarios, llevan a cabo asesoramientos a la gerencia, para un mejor funcionamiento de la empresa
Excelente	3	Dispone de buena seguridad, ya que los protocolos se han llevado satisfactoriamente. Además, cuenta con respaldos

Fuente: Elaboración Propia. 2021.

Tabla 15. Estimación del servicio brindado por el departamento de sistemas mediante lo especificado en los estándares en LIDOTEL.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				LIDOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Calidad y entrega de Servicios al Cliente	**OBJETIVO Nº3** Valorar el servicio brindado por el departamento de sistemas mediante lo especificado en los estándares.	53. ¿Considera que el departamento de sistemas cuenta con los recursos necesarios? ¿Por qué?			2		**6**	**9**	**67%3**
		54. ¿Cómo considera usted el servicio proporcionado por el departamento de sistemas? ¿Por qué?		1					
		55. ¿Qué piensa de la seguridad de la infraestructura de redes en la institución?				3			
		TOTAL	**0**	**1**	**2**	**3**			

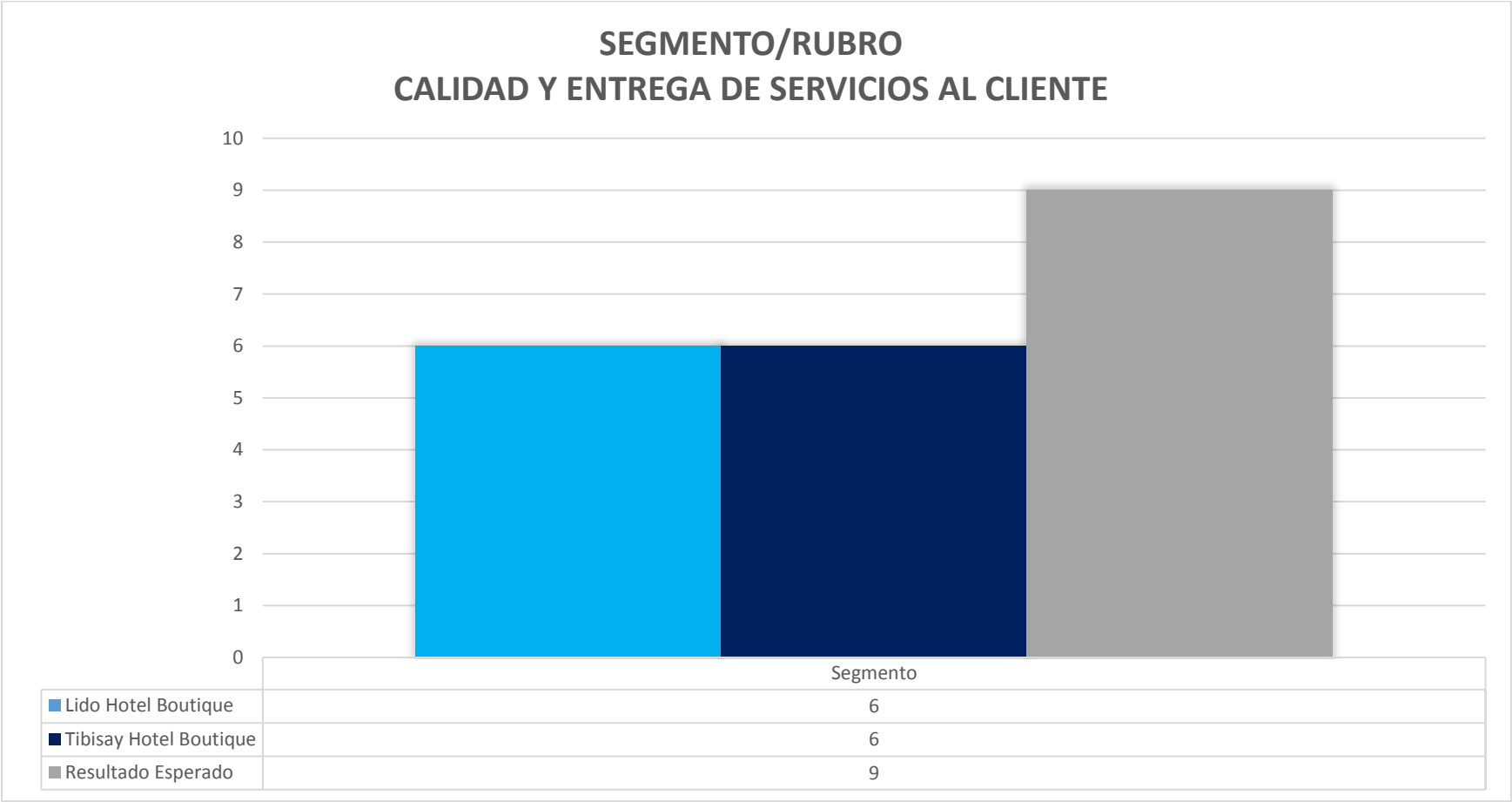
Fuente: Cuestionario realizado al departamento de sistemas del hotel LIDOTEL. Elaboración Propia. 2021.

Tabla 16. Estimación del servicio brindado por el departamento de sistemas mediante lo especificado en los estándares en TIBISAY.

Segmento/ Rubros	Objetivo de Control	PREGUNTAS	Tabulación de los datos				TIBISAY HOTEL		
			0 No cumple	1 Deficiente	2 Suficiente	3 Excelente	Resultado Obtenido	Resultado Esperado	%
Calidad y entrega de servicios al cliente	**OBJETIVO Nº3** Valorar el servicio brindado por el departamento de sistemas mediante lo especificado en los estándares.	53. ¿Considera que el departamento de sistemas cuenta con los recursos necesarios? ¿Por qué?			2		**6**	**9**	**67%**
		54. ¿Cómo considera usted el servicio proporcionado por el departamento de ¿Por qué?			2				
		55. ¿Qué piensa de la seguridad de la infraestructura de redes en la institución? ¿Por qué?			2				
		TOTAL	**0**	**0**	**6**	**0**			

Fuente: Cuestionario realizado al departamento de sistemas del hotel TIBISAY. Elaboración Propia. 2021.

Gráfico 6: Estimación del servicio brindado por el departamento de sistemas mediante lo especificado en los hoteles LIDOTEL y TIBISAY.



Fuente: Elaboración Propia. 2021.

Análisis e interpretación.

Respecto a la calidad y entrega de servicios al cliente, se obtuvo por respuesta que es satisfactorio el servicio que estos proporcionan, el cual dio como resultado un 6 / 6, razón de haber encontrado deficiencias en estos, descritas a continuación.

En Lidotel cuentan con los recursos necesarios para solventar los problemas que se presenten. Sin embargo, cabe acotar que los puestos se encuentran vacantes, por lo que no se tiene total disposición de una persona encargada del departamento, eso conlleva a que la calidad del servicio prestado sea poco eficiente y la atención de un requerimiento se retrase.

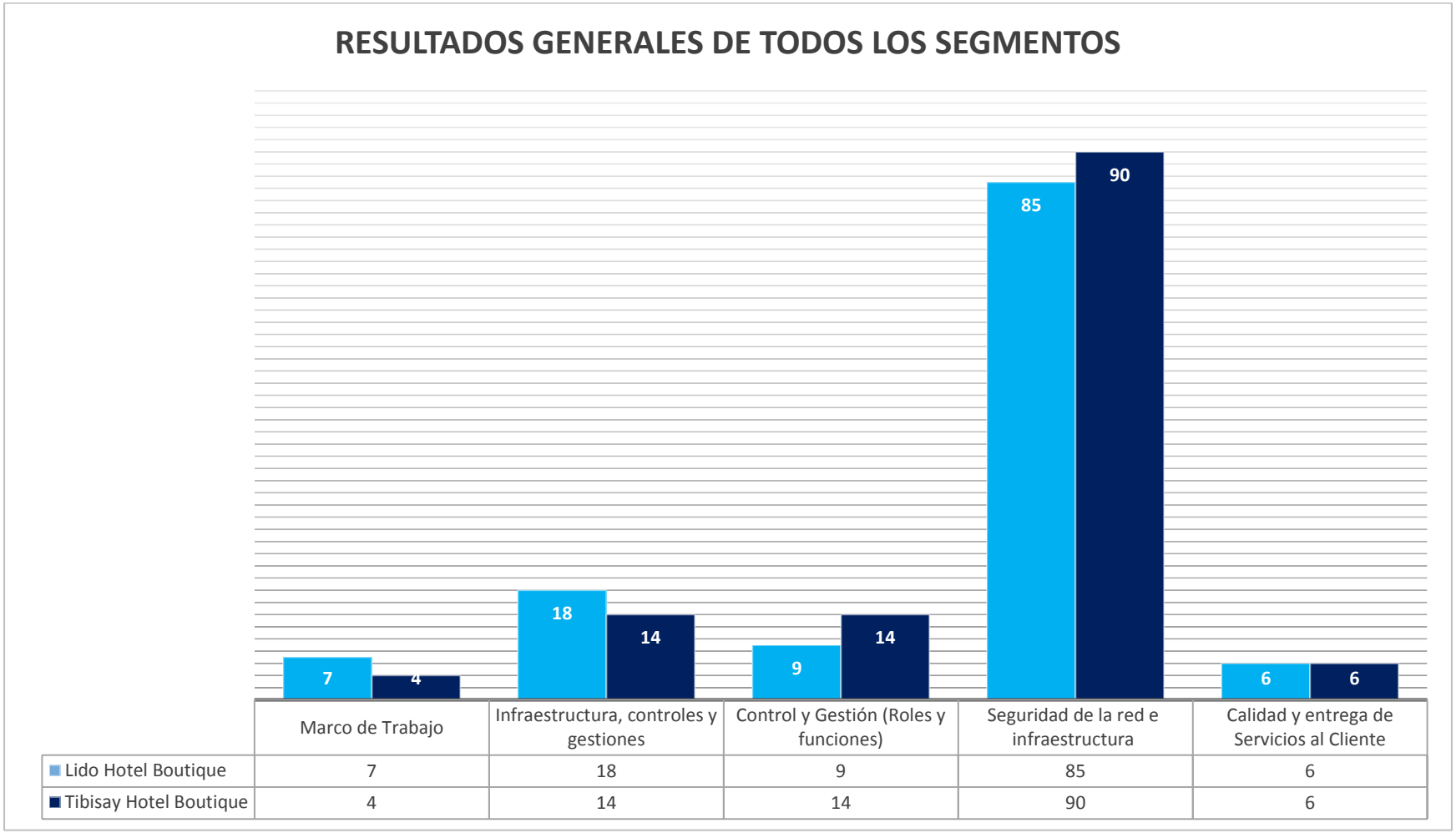
Por su parte, Tibisay también cuenta con recursos necesarios para implementar un plan de trabajo trimestral de inventarios exigidos por la empresa, para así ejecutar sus operaciones. No obstante, cuenta con pocos empleados requeridos para llevar a cabo las funciones específicas del departamento de sistemas, generando a su vez tardanza en la resolución de los problemas.

Tabla 17. Presentación de los resultados de todos los segmentos.

	Resultado Obtenido		
Segmento	**Lido Hotel Boutique**	**Tibisay Hotel Boutique**	**Resultado Esperado**
Marco de Trabajo	7	4	15
Infraestructura, controles y gestiones	18	14	24
Control y Gestión (Incidencias)	7	6	15
Control y Gestión (Roles y funciones)	9	14	15
Seguridad de la red e infraestructura	85	90	108
Calidad y entrega de Servicios al Cliente	6	6	9
Resultado por Hotel	**132**	**134**	**186**

Fuente: Cuestionario realizado al departamento de sistemas de los hoteles LIDOTEL y TIBISAY. Elaboración Propia. 2021.

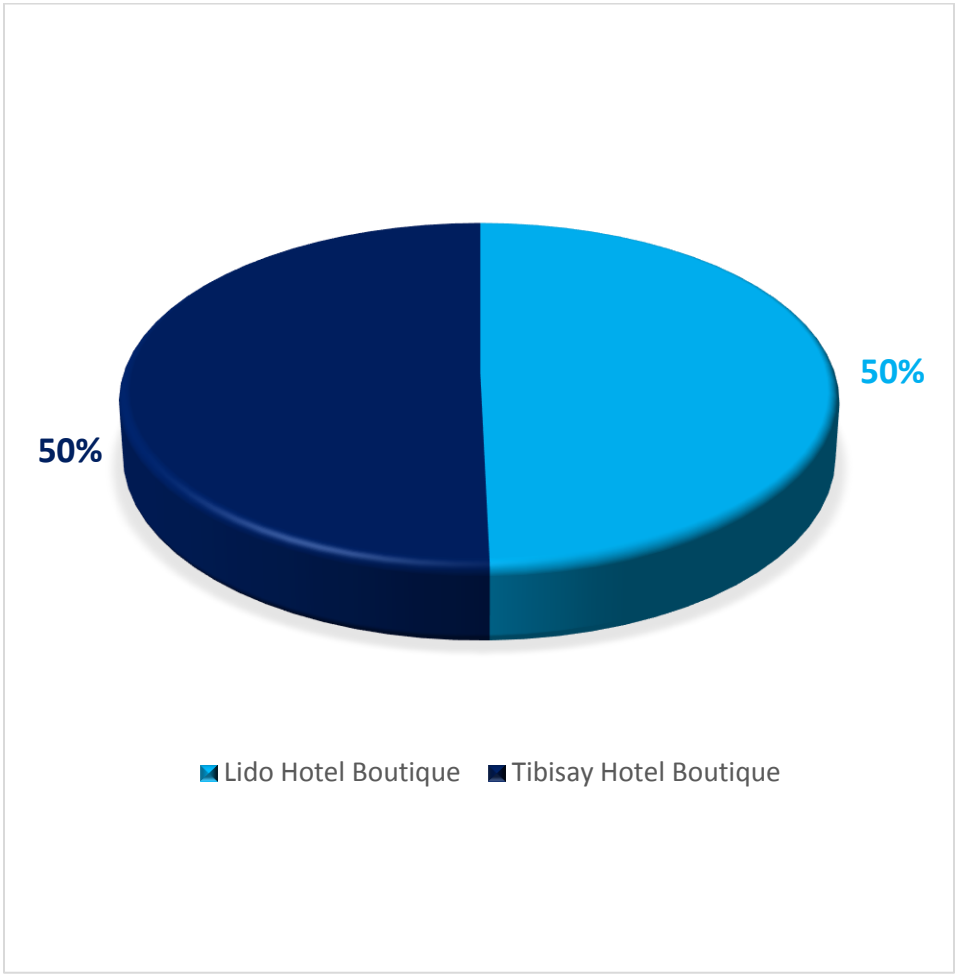
Gráfico 7: Presentación de los resultados en todos los segmentos/rubros.



	Marco de Trabajo	Infraestructura, controles y gestiones	Control y Gestión (Roles y funciones)	Seguridad de la red e infraestructura	Calidad y entrega de Servicios al Cliente
Lido Hotel Boutique	7	18	9	85	6
Tibisay Hotel Boutique	4	14	14	90	6

Fuente: Elaboración Propia. 2021.

Gráfico 8: Resultados generales de todos los segmentos/rubros.



Fuente: Elaboración Propia. 2021.

Análisis e interpretación.

De acuerdo a lo anterior, se pudo determinar que los hoteles actualmente disponen de políticas, estándares y normas para el resguardo de sus recursos, pero existe deficiencia en cuanto a su cumplimiento, ya que no se rigen por los estándares internacionales, permitiendo de esta manera que sus datos e información se vean amenazas por agentes externos.

En efecto, el no trabajar bajo una serie de prácticas estandarizadas impiden la prestación de servicios, existe un desorden en la manera que tiene que trabajar la empresa, y en particular, la del departamento de TI. Por lo contrario, la aplicación de la misma asegura el tiempo de vida de un proyecto, brinda la interoperabilidad nacional e internacional de los datos y la tecnología (alcance), y los procesos de telecomunicaciones, que hoy por hoy crece a diario. Además, ofrece guías para toda empresa grande o pequeña con el fin de asegurar el tipo de interconexión esencial en los mercados presente y en las comunicaciones a nivel mundial.

Actualmente, existe un marco de trabajo de mejores prácticas que posibilitan el control, la operación y administración de recursos, asimismo, reestructuran los procesos e identifican las carencias, teniendo como finalidad la efectividad en todos sus aspectos y conducen a la organización a la mejora continua. Este marco de trabajo se conoce como ITIL, el cual se hace mención porque engloba muchas áreas, como son las actividades de administración de la seguridad que están inmersas en casi todos sus procesos, también, en la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma; ITIL da descripciones de cómo deberían realizarse una serie de procedimientos detallados para ayudar a las empresas u organizaciones a llevar de manera eficiencia y de calidad sus operaciones. Por consiguiente, este marco de trabajo es de vital importancia debido a que identifica los riesgos asociados al proceso para definir líneas de acción, con la finalidad de mitigarlos. De la misma manera, esta biblioteca contiene 10 elementos para la administración de la seguridad de la información: Políticas de seguridad, organización de la seguridad, clasificación y control de los activos, seguridad del personal, seguridad física y ambiental, administración de comunicaciones y operaciones, control de acceso, desarrollo y mantenimiento de los sistemas, administración de la continuidad del negocio y conformidad.

CONCLUSIONES Y RECOMENDACIONES

La ejecución de la evaluación mediante auditoría a la infraestructura y seguridad de las redes LAN/WAN de los hoteles Lidotel Hotel Boutique Margarita y Tibisay Hotel Boutique, tuvo por objeto mejorar los controles y estándares de seguridad para el resguardo de sus activos empresariales, a través de sugerencias y recomendaciones. En efecto, se realizó mediante la identificación del marco de trabajo que utilizan para el desarrollo de sus actividades, la verificación del cumplimiento de los estándares de seguridad y controles de gestión implementadas en las cadenas hoteleras para detectar las posibles vulnerabilidades y reducir los posibles riesgos en la infraestructura.

Con la finalidad de generar recomendaciones a las debilidades encontradas en forma puntual, se plantearon el objetivo general y los objetivos específicos, los cuales se considera que se ejecutaron de manera completa.

Para ello, se tomó como base fundamental el marco de trabajo ITIL, lo cual permitió el diseño de cuestionario, entrevista y cuadro comparativo, permitiendo de este modo identificar los riesgos y peligros, a los que están expuestos los hoteles en cuanto a la seguridad de su información, también, fue de utilidad para detectar el cumplimiento de los estándares internacionales en los mismos.

Una vez cumplidos todos los objetivos propuestos para el desarrollo del presente trabajo de investigación, se llegó a la conclusión que, mediante la auditoría se evaluó el nivel en el que se encuentran actualmente la infraestructura de red en cuanto a su seguridad, y la deficiencia que existe en el cumplimiento de los estándares, esto se realizó comparándolo con el marco de trabajo ITIL.

Entre las primordiales recomendaciones emanadas de las investigaciones y actividades realizadas, cabe resaltar las siguientes, las cuales están dispuestas por importancia según porcentaje general:

- Los hoteles deben establecer un estándar con el cual garanticen el desarrollo y la mejora continua de sus operaciones. Es indispensable que hoy en día las empresas establezcan estándares, con el fin de resguardar sus activos (la información), con la finalidad no solo de aplicar, sino de controlar y monitorear todos sus procesos.

- En el área de tecnología se recomienda acoplar varios estándares para el resguardo de los activos empresariales, ya sea a nivel físico o lógico, ITIL interacciona de buena manera con otros marcos.
- Deben estar avalados por una certificación del marco de trabajo para así delimitar sus propios procesos de gestión de riesgos. Es importante que cada empresa cuente con certificados que avalen el seguimiento del marco de trabajo, ya que esto demuestra la calidad de la seguridad en cuanto a la infraestructura de sus redes para llevar de esta manera un mejor control y gestión de sus operaciones, asimismo, determina que los servicios informáticos que se ofrecen sean de la máxima confianza y han sido regulados.
- En la seguridad deben mejorar las herramientas implementadas, tomando en cuenta, que lo medular en una empresa es la información, por lo tanto, el establecimiento de las normas y políticas reducen el número de fallos y les permite estar preparados para posibles alteraciones en su red. De hecho, uno de los procesos de la guía ITIL es sobre la "Gestión de seguridad", esta mantener la información a salvo de intrusos, ayuda a mantener una fiabilidad en la empresa y segura la confidencialidad, la integridad y la disponibilidad de los datos y servicios de TI de una organización.
- Limitar el acceso a las redes.
- La calidad de servicios puede hacer la diferencia en cualquier empresa, importante hacer hincapié en este punto, ya que es la atención que una empresa o negocio ofrece a sus clientes. Para ello, es recomendable establecer normas basadas en ITIL que brindan una serie de procesos de una forma estructurada que permiten tener un programa de mejora continua y una mejor calidad de los servicios que se presta a los clientes.

REFERENCIAS

Alegsa, L. (2018). *Definición de sistema.* [Artículo en Línea]. Recuperado el 19 de noviembre de 2020 de https://www.alegsa.com.ar/Dic/sistema.php

Alpha Telecom Solutions. (2019) ¿*Qué es una red informática? Tipos de redes y características.* [Artículo en línea]. Recuperado el 20 de noviembre de 2020 de https://alphaenginyeria.com/red-informatica/

American Marketing Association. (s.f*). Definición de cliente*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://www.promonegocios.net/clientes/cliente-definicion.html#:~:text=Seg%C3%BAn%20la%20American%20Marketing%20Association,final)%22%20%5B3%5D

Arens, A. (2007). *Auditoría de Sistemas de Información.* [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://www.gestiopolis.com/auditoria-de-sistemas-informacion/

Arias, F. (2012) *Tipos y diseño de la investigación: Diseño de campo y documental.* [Artículo en Línea]. Recuperado el 24 de noviembre de 2020 de http://planificaciondeproyectosemirarismendi.blogspot.com/2013/04/tipos-y-diseno-de-la-investigacion_21.html?m=1

Bermúdez, K y Bailón, E. (2015). *Trabajo de investigación: Análisis en seguridad informática y seguridad de la información.* [Artículo en línea]. Recuperado el 16 de noviembre de 2020 de https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Bembibre, V. (2009). *Definición de ISO*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://www.definicionabc.com/economia/iso.php

CEUPE. ¿Qué es COBIT? [Blog en Línea]. Recuperado el 23 de Febrero de 2021 de https://www.ceupe.com/blog/que-es-cobit.html

Emagister (2019). ¿Qué es ITIL? [Blog en Línea]. Recuperado el 23 de Febrero de 2021 de https://www.emagister.com/blog/que-es-itil/CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. Gaceta Oficial extraordinaria Número 36.860 de fecha 30 de Diciembre de 1999. [Documento en línea]. Recuperado el 18 de febrero de 2021 de https://www.oas.org/juridico/spanish/cyb_ven_ley_telecomunicaciones.pdf

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica del Gobierno de España (2012). *MAGERIT – versión 3.0.*

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método [Documento en Línea]. Disponible el 11 de noviembre de 2020 de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xcr8pyjB_Dc

Donoso, J. (2006). *Metodología ITIL*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de http://repositorio.uchile.cl/handle/2250/108405

EUDE. (2019). *Eficiencia y Eficacia: Principales diferencias*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://www.eude.es/blog/eficiencia-eficacia-diferencias/

Finol y Camacho (2008). Marco metodológico. [Artículo en Línea]. Recuperado el 23 de Febrero de 2021 de http://virtual.urbe.edu/tesispub/0094671/cap03.pdf

Gastón, M. (2015). *Trabajo de investigación: Auditoría informática a la red de datos.* [Artículo en línea]. Recuperado el 16 de noviembre de 2020 de http://repositorio.unas.edu.pe/handle/UNAS/1033

Gavino, A (2018). *Trabajo de investigación: Auditoría en seguridad informática y gestión de riesgos.* [Artículo en línea]. Recuperado el 17 de noviembre de 2020 de http://repositorio.unjfsc.edu.pe/bitstream/handle/UNJFSC/2924/raul-gavino.pdf?sequence=1&isAllowed=y

García, Cisneros y Díaz. (2011). Técnicas Cuantitativas: análisis de los datos cuantitativos. [Artículo en línea] Recuperado el 24 de noviembre de 2020 de http://entornovirtualparaeldesarrollode.weebly.com/41tecnicas-cuantitativas.html

González, H (2019). Informe de pasantía: *Evaluación mediante auditoría de la seguridad de los sistemas de información en ambiente web y redes.* Informe final de pasantías. Noviembre de 2019. Universidad de Margarita. Venezuela.

INFOSEGUR. (2013). *Conceptos básicos de la seguridad informática, 1.2- objetivos de la seguridad informática.* [Artículo en línea]. Recuperado el 20 de noviembre de 2020 de https://infosegur.wordpress.com/tag/disponibilidad/

ISO9001-2000. (s.f) *¿Qué es la gestión de calidad?* [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://iso9001calidad.com/que-es-la-gestion-de-la-calidad-23.html

ISOTools.org, (s.f).*Software ISO Riesgos y Seguridad.* [Página web]. Recuperado el 18 de febrero de 2021 de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

IsoTools-Excellence. (2019). *Sistemas de Gestión de Riesgo y Calidad.* [Artículo en Línea]. Recuperado el 23 de Febrero de 2021 de https://www.facebook.com/275770419170516/posts/c%C3%B3mo-funciona-la-iso-27001el-eje-central-de-iso-27001-es-proteger-la-confidencia/2524229690991233/

Ley Especial Contra Delitos Informáticos. Recuperado el 18 de febrero de 2021 de https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Ley de Reforma de la Ley Orgánica de Ciencia, Tecnología e Innovación. Recuperado el 18 de febrero de 2021 de http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Org%C3%A1nica-de-Ciencia-Tecnolog%C3%ADa-e-Innovacion.pdf

Ley sobre Protección a la Privacidad de las Comunicaciones. Recuperado el 18 de febrero de 2021 de http://www.conatel.gob.ve/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones-2/

Lobos, E. (2005). *Auditoría de empresas en el área de telecomunicaciones.* [Documento en línea]. Recuperado el 18 de febrero de 2021 de http://biblioteca.usac.edu.gt/tesis/08/08_0249_CS.pdf

Mata, L. (2019). *El enfoque de investigación: la naturaleza del estudio.* [Artículo en línea]. Recuperado el 25 de noviembre de 2020 de https://investigaliacr.com/investigacion/el-enfoque-de-investigacion-la-naturaleza-del-estudio/#:~:text=Cuando%20hablamos%20de%20enfoque%20de,el%20desarrollo%20de%20la%20perspectiva

Méndez (1999). *Técnicas de recolección de datos.* [Artículo en línea]. Recuperado el 24 de noviembre de 2020 de https://www.eumed.net/tesis-doctorales/2012/eal/tecnicas_recoleccion_datos.html

Mesa J. (2020). *¿Qué son los recursos?* [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://blog.grupo-pya.com/recursos-definicion-tipologia-la-empresa/

Nuño, P. (2017). *¿Qué es la auditoría de sistemas?* [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://www.emprendepyme.net/auditoria-de-sistemas.html

Peña. (2006). *Sistema de información*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de http://virtual.urbe.edu/tesispub/0095501/cap02.pdf

Pérez, J y Gardey, A. (2010). *Definición de usuario*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://definicion.de/usuario/

Pérez, J y Merino, M. (2017). *Definición de estándar*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://definicion.de/estandar/

Pérez, J y Merino, M. (2013). *Definición de protocolo de investigación*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://definicion.de/protocolo-de-investigacion/

Pérez J, Merino M, (2011). *Definición de verificación*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://definicion.de/verificacion/

Raffino, M. (2020). *Concepto de infraestructura*. [Artículo en Línea]. Recuperado el 19 de noviembre de 2020 de https://concepto.de/infraestructura/

Raffino, M. (2020). *Marco teórico.* [Página web]. Recuperado el 18 de febrero de 2021 de https://concepto.de/marco-teorico/

RedUSERS. (2013) *¿Qué es una red informática?* [Artículo en línea]. Recuperado el 20 de noviembre de 2020 de http://www.redusers.com/noticias/que-es-una-red-informatica/

Robbins. (1996). *El control como fase del proceso administrativo.* [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de https://www.gestiopolis.com/el-control-como-fase-del-proceso-administrativo/

Rouse, M. y Lebeaux, R. (2014). *Definición de gestión de TI*. [Artículo en línea]. Recuperado el 19 de noviembre de 2020 de: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-TI

Salvador. (2016). *COSO: Gestión de Riesgo*. [Artículo en Línea]. Recuperado el 19 de noviembre de 2020 de https://fraudeinterno.wordpress.com/2016/02/19/coso-gestion-de-riesgos/

Sanchez, K. (2020). *Vulnerabilidades, Riegos y Control Informático.* [Página en línea]. Recuperado el 19 de noviembre de 2020 de https://www.mindmeister.com/es/1464701610/vulnerabilidades-riegos-y-control-inform-tico

Santillana, J (2011). *Auditoría.* [Blog en Línea]. Recuperado el 19 de noviembre de 2020 http://auditoria.over-blog.com/article-auditoria-68941282.html

Tamayo, M. (2012). *La población y la muestra de un proyecto de investigación.* [Documento en línea] Recuperado el 19 de noviembre de 2020 de http://virtual.urbe.edu/tesispub/0094051/cap03.pdf

Tarazona, C. (2007). *Amenazas Informáticas y Seguridad de la Información* [Documento en Línea]. Recuperado el 19 de noviembre de 2020 de https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/

Thompson y Strickland. (2004). *Tecnología de información y comunicación.* [Documento en Línea]. Recuperado el 19 de noviembre de 2020 de https://dialnet.unirioja.es/descarga/articulo/3217615.pdf

UNE-ISO Guía 73. (2010). *Gestión de riesgos. [*Documento en Línea]. Recuperado el 19 de noviembre de 2020 de https://iso.cat/wp-content/uploads/2019/09/Cap-1-8-2-a-6-Guia_ISO-IEC-73.pdf

UPEL. (1998). *Proyecto factible: una modalidad de investigación.* [Documento en línea]. Recuperado el 23 de noviembre de 2020 de https://www.redalyc.org/pdf/410/41030203.pdf

Universidad Internacional de Valencia. (2018) *¿Qué es la seguridad informática y cómo puede ayudarme?* [Artículo en línea]. Recuperado el 20 de noviembre de 2020 de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Wikipedia, La Enciclopedia libre (2013). *Framework.* [Artículo en Línea]. Recuperado el 19 de noviembre de 2020 de https://es.wikipedia.org/wiki/Framework

Wikipedia, La Enciclopedia libre (2017). *Dato*. [Artículo en Línea]. Recuperado el 19 de noviembre de 2020 de https://es.wikipedia.org/wiki/Dato

Wolfers. (1962). *Seguridad*. [Artículo en Línea]. Recuperado el 19 de noviembre de 2020 de https://es.wikip de diciembre de edia.org/wiki/Seguridad

Znet it Solutions. *Qué es la infraestructura de redes y el cableado estructurado.* [Bblog en línea]. Recuperado el 28 de diciembre de 2020 de https://www.z-net.com.ar/blog-post/que-es-la-infraestructura-de-redes-y-el-cableado-estructurado/#:~:text=Se%20entiende%20como%20infraestructura%20de,esc%C3%A1ner%2C%20impresoras%2C%20TPV%2C%20c%C3%A1maras

ANEXOS

Cuestionario

Del marco de trabajo que se rigen:

1. ¿Tienen conocimiento de algún estándar internacional?
   - □ Sí
   - □ No
2. ¿Se rigen por algún estándar internacional, para la gestión de redes?
   - □ Sí
   - □ No

   De ser afirmativa:
3. ¿Cuál es el marco de trabajo por los que se rigen actualmente?
   - □ COBIT
   - □ COSO
   - □ ISO 27000-1
   - □ ITIL
   - □ Otros: _____
4. ¿Tienen políticas y controles definidos para la gestión y control de la seguridad en sus redes?
   - □ Sí
   - □ No
5. ¿Qué certificados avalan el seguimiento del marco de trabajo?

_____

6. ¿Cuál es la última actualización de la normativa por la cual se rigen?

De la infraestructura, controles y gestiones realizada bajo los estándares internacionales:

7. ¿Cuál es el tipo de red que utilizan actualmente?
   - □ LAN
   - □ WAN
   - □ MAN

8. ¿Cuáles son los tipos de redes inalámbricas que usan?
    - Wifi
    - Infrarrojo
    - Microondas
    - Laser
    - Bluetooth
    - Otra: _____
9. ¿Qué topología de red usan?
    - Anillo
    - Árbol
    - Bus
    - Estrella
    - Malla
    - Híbrida
10. ¿Qué tipo de cables usan en estos momentos?
    - Coaxial
    - Trenzado
    - Fibra óptica
    - Otro: _____
11. ¿Qué tipo de marco de trabajo utilizan para un sistema de cableado?

    _____
12. ¿Están los cables de los ordenadores recogidos?
    - Sí
    - No
13. ¿Están identificados los conectores de corrientes de los equipos?
    - Sí
    - No
14. ¿Cumplen con los estándares internacionales actualmente?
    - Sí
    - No

De las políticas de seguridad TI establecidas para la instalación de redes LAN/WAN:

15. ¿Qué políticas y/o protocolos de actuación utilizan ante cualquier amenaza?

    _____

    _____

    _____

16. ¿El centro de cómputo da hacia el exterior?

    - Sí
    - No

17. ¿El lugar donde se ubica el centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?

    - Sí
    - No

18. Donde se encuentran las redes, ¿Existen materiales que puedan ser inflamables o causar algún daño a los equipos?

    - Sí
    - No

19. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?

    - Sí
    - No

De ser afirmativa:

20. ¿Cuáles son?

    _____

    _____

    _____

21. ¿Existen personas responsables de la seguridad en el departamento de sistemas?

    - Sí
    - No

22. ¿Existe personal de vigilancia en la institución?

    - Sí
    - No

23. ¿Se investiga a los vigilantes cuando son contratados directamente?

- Sí
- No

24. ¿La institución posee cámaras de circuitos cerrados?

- Sí
- No

25. El edificio donde se encuentra la infraestructura de red está a salvo de:

- Inundación
- Terremoto
- Fuego
- Sabotaje
- Nada

26. ¿Qué tipo de extintores de fuego existen en la institución?

- Manuales
- Automáticos
- Ninguno

27. ¿Se ha adiestrado el personal en el manejo de los extintores?

- Sí
- No

28. ¿Se han tomado medidas para minimizar la posibilidad de fuego?

- Sí
- No

29. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?

- Sí
- No

30. ¿Existe personal capacitado para el mantenimiento de las redes?

- Sí
- No

31. ¿Cada cuánto se hace mantenimiento preventivo a la red?

- Nunca
- Frecuentemente
- Siempre

32. ¿Cada cuánto se hace mantenimiento correctivo a la red?
    - Nunca
    - Frecuentemente
    - Siempre
33. ¿Existe alarma para detectar condiciones anormales del ambiente?
    - Sí
    - No

De ser afirmativa:

34. Esta alarma está conectada:
    - Al puesto de guardias
    - A la estación de bomberos
    - A ningún lado
35. ¿Existe detector de calor, de humo y de agua?
    - Sí
    - No
36. ¿Existe salida de emergencia?
    - Sí
    - No

De ser afirmativa:

37. Esta puerta solo es posible abrirla:
    - Desde el interior
    - Desde el exterior
    - Ambos
38. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas?
    - Sí
    - No

39. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
    - Sí
    - No
40. ¿Existe seguridad de acceso físico?
    - Sí
    - No

De ser afirmativa:

41. ¿De qué tipo?
    - Seguros en puertas y ventanas
    - Puertas con combinación
    - Puertas con tarjetas
    - Puerta con digitalización de código y alarma
    - Puertas basadas en la retina y en voz
    - Puertas basadas en huellas dactilares
42. ¿Los equipos informáticos se encuentran ubicados a una distancia no menor a 30 cm del piso?
    - Sí
    - No
43. ¿En el lugar donde se encuentran los ordenadores existe la presencia de aire acondicionado?
    - Sí
    - No

De ser afirmativa:

44. ¿Está en la ubicación correcta?
    - Sí
    - No
45. ¿Tiene alguna falla?
    - Sí
    - No
46. ¿El cableado se encuentra correctamente instalado?

- Sí
- No

47. ¿Los cables están dentro de paneles y canales eléctricos?
    - Sí
    - No
48. ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige?
    - Sí
    - No
49. ¿Cuántos usuarios tienen acceso a las redes?

_____

50. ¿Cómo calificarías lo controles de riesgos?
    - Satisfactorio
    - Aceptable
    - Deficiente
51. Las políticas de seguridad son:
    - Satisfactorias
    - Aceptables
    - Deficientes
52. ¿Se han realizado auditorias de seguridad física anteriormente?
    - Sí
    - No

Entrevista

1. ¿La empresa cuenta con otras localidades, a nivel regional, nacional o internacional?
    - Sí
    - No

De ser afirmativa:

2. ¿Prestan algún servicio de tecnología en varias localidades?
    - Sí
    - No
3. ¿Qué servicios de redes prestan y administran LAN/WAN?
    - Protocolo simple de administración de red
    - Correo electrónico
    - Protocolo de transferencia de archivos (FTP)
    - Domain Name System (DNS)
    - Otro:
4. ¿Existe interconexión entre las localidades?
    - Sí
    - No
5. ¿Considera que el departamento de sistemas cuenta con los recursos necesarios?
    - Si
    - No

    ¿Por qué?
6. ¿Cómo considera usted el servicio proporcionado por el departamento de sistemas?
    - Deficiente
    - Aceptable
    - Satisfactorio
    - Excelente

    ¿Por qué?
7. ¿Qué piensa de la seguridad de la infraestructura de redes en la institución?
    - Nula
    - Riesgosa

- Satisfactoria
- Lo desconoce

¿Por qué?

8. ¿Existen fallas en las redes?
   - Sí
   - No

   ¿Cuáles? ¿De qué tipo?

   -La desconoce-

9. ¿Sobre quién recaen las decisiones del departamento de sistemas?

_____

10. ¿Cumple otras funciones además de encargarse del departamento de sistemas?
    - SÍ
    - No

De ser afirmativo:

11. ¿Cuáles?

_____

12. ¿Cuánto tarda en atender un requerimiento? (continuidad y disponibilidad de servicio).

_____

13. ¿Cuántas personas le reportan, de qué departamento son y cuál es el rol que desempeña cada uno?

_____

14. Trabajan de manera:

    Presencial

    Remota

    Ambas

De ser remota:

15. ¿Actualmente en qué localidad se ubican?

_____

16. ¿Quién controla las entradas de documentos fuente?
17. ¿En qué forma las controla?

_____

18. ¿Existe un registro del control?

- Sí
- No

19. ¿Quién lo revisa?