UNIVERSIDAD DE MARGARITA

SUBSISTEMA DE DOCENCIA

DECANATO DE INGENIERIA Y AFINES

COORDINACIÓN DE INVESTIGACIÓN Y PASANTÍA

AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MUNDO SHOP C.A. UBICADA EN LA CALLE IGUALDAD, PORLAMAR, ESTADO NUEVA ESPARTA

Elaborado por: Angel E. Gómez F.

Tutor Prof. Ing.: Valentina Martínez

El Valle del Espíritu Santo, julio 2022

UNIMAR
Universidad de Margarita

APROBACIÓN DEL JURADO

En el día de hoy 14 de Julio de 2022, constituidos como Jurados en la Universidad de Margarita: Profesora ***Isis Rueda****, Profesora* ***Ana Blanco*** *y la Profesora* ***Valentina Martínez como*** *Tutora, a los fines de la Evaluación del Trabajo de Investigación titulado:* ***AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA MUNDO SHOP, C. A. UBICADA EN LA CALLE IGUALDAD, PORLAMAR, ESTADO NUEVA ESPARTA****, que como requisito parcial de grado para optar al título de* ***INGENIERO DE SISTEMAS*** *presenta el Bachiller:* ***ANGEL ENRIQUE GOMEZ FERRER,*** *titular de la cédula de identidad* ***N.° 27.935.796****.*

Luego de revisado, presentado y cumpliendo con lo establecido en el artículo 21 del Capítulo VII de la Normativa de Trabajo de Investigación para Pregrado de la Universidad de Margarita, el Jurado emitió el Veredicto de ***APROBADO****. Se deja constancia que, de conformidad con lo establecido en el artículo 23 literal de la normativa antes mencionada, por decisión unánime del jurado se otorga la* ***MENCIÓN HONORÍFICA APROBADO SOBRESALIENTE****, ante lo cual los abajo firmantes dan fe de lo expuesto.*

Msc. Ana Blanco
C.I. V- 10.298.994.
Jurado

Esp. Isis Rueda
C.I. V-6.511.850.
Jurado

Ing. Valentina Martínez
C.I. V- 24.765.943.
Tutor

UNIVERSIDAD DE MARGARITA
UNIMAR
DECANATO DE INGENIERÍA
MARINES

Refrendado: Decano de Ingeniería de Sistemas

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 el (la) ciudadano (a) **Ángel Enrique Gómez Ferrer**, cedulado con el número: **V.- 27.935.796**, para optar al Grado de *Ingeniero de Sistemas,* considero que dicho trabajo: *AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MUNDO SHOP C.A. UBICADA EN LA CALLE IGUALDAD, PORLAMAR, ESTADO NUEVA ESPARTA*, reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado Examinador que se designe.

Atentamente

Ing. Valentina Martínez Hernández
TUTOR

El Valle del Espíritu Santo, julio de 2022.

ÍNDICE

DEDICATORIA

Primeramente, a Dios y a la Virgen del Valle por bendecirme, guiarme y darme sabiduría durante los momentos más difíciles, superando todos los obstáculos para llegar a esta etapa tan importante.

A mis padres, Xenia Ferrer y Alexis Gómez por ser mi mayor motivación en los momentos más difíciles y brindarme la fortaleza necesaria para alcanzar todas mis metas.

A mis tíos, Roger Salazar y Saira Ferrer por apoyarme durante toda mi formación universitaria y velar siempre por mi educación.

A mis hermanos, abuelos, tíos y primos por estar siempre para mí, brindando sus mejores deseos desde la distancia.

A mi abuelo Manuel Ferrer, que desde el cielo me cuida y me bendice.

AGRADECIMIENTOS

A Dios y a la Virgen del Valle, por darme la dicha de vivir y guiarme siempre por el buen camino, permitiéndome cumplir todas mis metas.

A mis padres, por velar siempre por mi educación y darme los mejores consejos. Mama gracias por ser el motor que guía mi vida, apoyándome y motivándome cuando el camino se pone difícil. Papa gracias por tu apoyo incondicional y tu dedicación en todo momento. Gracias por todo el amor que me dan, sin ustedes no hubiera sido todo esto posible.

A mis tíos, Roger y Saira por brindarme todo su apoyo durante mis estudios.

A mi tutora Académica, Prof. Ing. Valentina Martínez, por brindarme todo el apoyo y empeño para la realización de esta investigación, encaminándome y guiándome con los mejores consejos y recomendaciones.

A la Prof. Yamnel Torcat, por velar cada paso de esta investigación, gracias por su dedicación y conocimiento, incentivándome en todo momento a dar lo mejor de mí.

A la Prof. Isis Rueda, por orientarme y guiarme con sus conocimientos en la culminación de esta investigación.

A la Universidad de Margarita, por recibirme y ser mi casa de estudios, formándome como profesional brindándome grandes experiencias y recuerdos.

A mis amigos, que durante toda esta etapa estuvieron conmigo ayudándome compartiendo todos sus conocimientos cuando lo requería y por todos los buenos momentos en clase.

A todos muchas gracias.

INDICE DE FIGURAS

INDICE DE GRÀFICOS

LISTA DE TABLAS

UNIVERSIDAD DE MARGARITA

SUBSISTEMA DE DOCENCIA

COORDINACIÓN DE INVESTIGACIÓN Y PASANTÍA

“AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MUNDO SHOP C.A. UBICADA EN LA CALLE IGUALDAD, PORLAMAR, ESTADO NUEVA ESPARTA”

Autor: Angel E. Gómez F.

Tutor Prof. Ing.: Valentina Martínez

Junio de 2022

RESUMEN

El presente trabajo de investigación comprende una auditoría de la seguridad de la información con el objetivo de proponer recomendaciones para mejorar la gestión de los activos de información de la empresa Mundo Shop C.A.. De esta manera, la investigación se llevó a cabo siguiendo una naturaleza cuantitativa con diseño de campo, lo que permitió recolectar la información directamente de los hechos, acompañado de un tipo de investigación descriptiva enmarcada en un proyecto factible. En este sentido, mediante el uso de la entrevista, cuestionarios de control, observación y revisión documental con las técnicas de análisis correspondientes, permitieron identificar y evidenciar la problemática, logrando definir las deficiencias y vulnerabilidades. Todo esto permitió formular las recomendaciones para garantizar el buen funcionamiento del manejo de la información a nivel de infraestructura, aplicaciones, control de acceso y definición de roles.

Descriptores: Seguridad de la información, Auditoría, Análisis de Riesgo, controles de seguridad.

INTRODUCCION

En la actualidad son muchos los avances tecnológicos que se han logrado, debido a ello, las empresas y el ser humano cuentan con miles de herramientas y experiencias que facilitan y benefician su día a día. Es por ello que las empresas implementan nuevas tecnologías de información basadas en una planificación estratégica que busca mejorar las competencias de la misma. En efecto, cada vez es de mayor importancia que se implementen normas y directrices que regulen el cumplimiento de los objetivos empresariales de la forma más eficiente.

De esta manera, las tecnologías de información asumen la gran responsabilidad de cumplir normas y estándares con el objetivo principal de garantizar la protección de los activos informáticos, a través de las mejores prácticas de la gestión de la información. Es por esto, que es de gran importancia la necesidad de implementar medidas para mantener y garantizar la seguridad de toda la información de la empresa; ya que la privacidad cumple un rol fundamental dentro de la tecnología de la información, donde solo las personas autorizadas puedan acceder a los datos, y con esto, poder garantizar credibilidad e integridad de la información almacenada.

En este sentido, las auditorías tienen como objetivo la evaluación de los métodos y mecanismos que utiliza una empresa para llevar a cabo sus actividades y servicios, examinando si se están llevando a cabo de la manera más eficiente. Así mismo, permite identificar los riesgos y vulnerabilidades presentes y, de acuerdo con los hallazgos encontrados, se generan las recomendaciones que mejor se adapten a los requerimientos de la organización.

En función de esto, en la ejecución de la auditoría de la seguridad de la información en la empresa Mundo Shop C.A., se evidenció que la misma no gestiona de la forma correcta sus activos de información; debido a que no cuentan con los controles necesarios para garantizar el manejo óptimo de la información.

Cabe resaltar que la presente investigación se encuentra estructurada por 5 partes, en las cuales se desenvuelve la auditoría de seguridad de información. Estas mismas son:

Parte I: Descripción General del Problema, donde se describe de manera detallada la problemática de estudio, las Interrogantes, Objetivo General, así como también los Objetivos Específicos y Valor Académico de la Investigación.

Parte II: Descripción Teórica, la cual se encuentra conformada por los Antecedentes de Investigación, las Bases Teóricas y Legales, al igual que la definición de términos, las cuales permiten sustentar y obtener una mayor comprensión del objeto de estudio.

Parte III: Descripción Metodológica, en la misma se establece de manera clara la metodología para llevar a cabo la investigación, donde se definen la Naturaleza, Tipo y Diseño de la investigación, la Población y Muestra, así como las Técnicas de Recolección y de Análisis de datos.

Parte IV: Análisis y Presentación de Resultados, donde se contemplan la ejecución de las técnicas definidas anteriormente, permitiendo evidenciar de manera puntual el alcance de cada objetivo de la investigación.

Para finalizar, se encuentra la Parte V: Conclusiones y Recomendaciones, donde se contempla el resultado de la investigación, además de las recomendaciones a los entes involucrados.

PARTE I

DESCRIPCION GENERAL DEL PROBLEMA

En este capítulo se argumenta la problemática con respecto a la seguridad de la información de manera detallada permitiendo conocer sus características y causas. Así mismo, se establecen los objetivos y el valor académico de la investigación.

1.1 Formulación del problema

Hoy en día el mundo está en constante evolución, la tecnología no se escapa de ello; son muchos los avances e innovaciones que se han logrado a través del tiempo y con esto las tecnologías de la información y comunicación han logrado mejorar con una rapidez increíble. Para las empresas cada vez es de más relevancia optimizar los procesos y tareas que realizan para su beneficio, es por esto que la retroalimentación cada vez es más importante, ya que gracias a ella se logran identificar los problemas en la menor cantidad de tiempo posible para poder tomar las decisiones que más convengan.

Así mismo, en una empresa la organización es sumamente importante, ya que de esto depende su crecimiento como entidad y, a su vez, permite tener un mayor crecimiento económico aprovechando el mínimo de sus recursos, con la finalidad de brindar mayores ganancias para la misma. La organización es un medio que permite establecer un buen funcionamiento de los recursos disponibles, aplicando estrategias con el fin de alcanzar los objetivos propuestos de toda la empresa, permitiendo obtener mejores resultados, disminuyendo los costos y mejorando los plazos de ejecución de los proyectos. Por esta razón es importante que toda entidad posea un sistema organizacional sólido y bien estructurado para una aplicación eficiente, sistemática, positiva y coordinada de los esfuerzos disponibles.

Además, las empresas ponen en práctica distintos modelos de estandarización, adoptando normas y reglas que logran que un procedimiento de trabajo se realice de forma óptima, con el objetivo de maximizar el ahorro en tiempo, dinero y esfuerzo en el mantenimiento de los mismos. En este sentido, Feher, F. (2007) explica que “Tener un

proceso estandarizado es una herramienta que da ventajas competitivas a emprendedores y empresas de todos los tamaños. No solo permite conocer a fondo el negocio, sino también a establecer indicadores que guiarán todas sus actividades".

No obstante, las empresas utilizan como herramienta las tecnologías de la información para llevar a cabo los procesos y servicios de la manera más eficaz y eficiente; estos mismos requieren ser supervisados por profesionales para mantenerlos actualizados y en óptimas condiciones de funcionamiento, basándose en normas y estándares informáticos que son de gran importancia en las empresas, ya que proveen el uso correcto de las tecnologías de la información con el fin de llevar a cabo las actividades de mejor manera, tomando en cuenta los parámetros establecidos para obtener la calidad que las normas establecen.

En este sentido, López, J. (2014:ii) explica que:

> Las normas y estándares informáticos se han convertido en un elemento de soporte vital a las organizaciones; a medida que se implementan los procesos del negocio, crece la necesidad de aplicarlas para asegurar que los procedimientos, diseños y productos y otras acciones cumplan con requisitos de calidad.

De igual forma, las normas y estándares informáticos garantizan que la gestión de activos y servicios logren tener mayor seguridad y confiabilidad para el desarrollo correcto de las actividades, minimizando los errores y aumentando la productividad; de esta manera se establece una implementación efectiva y un planteamiento estructurado para desarrollar servicios de tecnología de la información fiables, adoptando medidas y mecanismos para minimizar los riesgos en lo referente a la gestión de servicios de tecnología de la información de dicha empresa.

Por lo tanto, las auditorías cumplen un rol muy importante en las empresas, ya que permiten tomar acciones preventivas y correctivas para eliminar las fallas y vulnerabilidades que se detecten mediante la evaluación de la gestión de activos que realizan en su día a día. Dicha evaluación se encarga de inspeccionar la seguridad de los sistemas de información, planes de contingencia y medidas de prevención, con la finalidad de proteger y mantener la integridad de los equipos computacionales, bases de

datos y usuarios. Así mismo, comprobando que se realicen de la manera más eficiente, tomando en cuenta las normativas internacionales.

Del mismo modo, se ha demostrado que la información es uno de los recursos más importantes de las empresas, por lo cual los mecanismos que la involucran deben ser controlados y auditados de la misma manera que sus otros componentes. Es por esto que se debe garantizar que la información privada esté al alcance solo del personal autorizado para administrarla y manipularla. También Gómez, F. (s/f) comenta que, "Garantizar un máximo nivel de disponibilidad, integridad y confidencialidad de la información manejada diariamente en las organizaciones es un aspecto de gran importancia que se procura tener en cuenta dentro de las labores empresariales de hoy en día". En virtud a esto, para que una empresa pueda mantener su competitividad, rentabilidad y posicionamiento en el mercado, es necesario que la información cuente con disponibilidad, integridad y confidencialidad.

En efecto, la empresa Mundo Shop C.A., se caracteriza como una entidad sólida dedicada a la venta y comercialización de ropa para damas, caballeros y niños, brindando la mejor opción para aquellas personas que buscan prendas de vestir. Desde hace varios años dedica sus esfuerzos a satisfacer las necesidades de sus clientes en materia de moda y estilo, brindando productos de alta calidad y servicios garantizados a sus clientes en la calle Igualdad de la cuidad de Porlamar, ubicada en el Estado Nueva Esparta.

Cabe resaltar que la empresa Mundo Shop C.A., ofrece sus servicios de manera limitada y deficiente en cuanto a la gestión de la tecnología de la información. Esto se puede ver reflejado en la ausencia de políticas de seguridad, de un almacenamiento seguro y de ciclos de copia de seguridad. Por otro lado, tampoco poseen medidas de control y protocolos internos para proteger la integridad de la información. También la no restricción de permisos en equipos hace que existan riesgos y amenazas que puedan ocasionar la pérdida de la confidencialidad de la información.

Aunado a esto, los problemas mencionados son causados por distintos factores que influyen en la empresa, como lo son: la falta de controles en cuanto a contraseñas y acceso a equipos, así como también la falta de mantenimiento del software y hardware,

afectando en gran medida las actividades que desarrolla, generando como consecuencias que la información sea más fácil de vulnerar o se pueda perder de manera definitiva, ya que no cuentan con planes o manuales de prevención ante cualquier contingencia que se pueda presentar.

Es por esto que surge la necesidad de implementar una auditoría de la seguridad de la información en el departamento de administración, apoyándose en las normativas y protocolos internacionales; con el objetivo de evaluar los controles definidos para la seguridad de la información, para garantizar un mayor nivel de seguridad e integridad de la información y de esta manera brindarle a la empresa alternativas de crecimiento y de desarrollo empresarial que, a su vez, contribuyan de manera significativa en la disminución de riesgos y amenazas.

1.2 Interrogantes

1. ¿Cuál es la situación actual de los sistemas informáticos de la empresa Mundo Shop C. A.?
2. ¿Qué controles se aplican para la seguridad de la información en la empresa Mundo Shop C.A.?
3. ¿Cómo se valida el cumplimiento de las regulaciones para la seguridad de la información en la empresa Mundo Shop C.A.?
4. ¿Cómo elaborar el informe final de auditoria con las recomendaciones para el mejoramiento de la gestión de la información de la empresa Mundo Shop C.A.?

1.3 Objetivo General

Realizar una auditoría de la seguridad de la información para la empresa Mundo Shop C.A. ubicada en la calle Igualdad, Porlamar, Estado Nueva Esparta.

1.4 Objetivos específicos

1. Analizar la situación actual de los sistemas informáticos que se encuentran en la empresa Mundo Shop C.A.
2. Evaluar los controles definidos para la seguridad de la información de la empresa Mundo Shop C.A.

3. Validar el cumplimiento de las regulaciones para la seguridad de la información en la empresa Mundo Shop C.A.
4. Elaborar el informe final de auditoria con las recomendaciones para el mejoramiento de la gestión de la información de la empresa Mundo Shop C.A

1.5 Valor académico de la investigación

Hoy en día las empresas requieren ser cada vez más competitivas y para ello se deben buscar alternativas que permitan llevar de la mejor manera los mecanismos de gestión de información, con el fin de cumplir con los objetivos y metas propuestas. Por lo tanto, toda la información que recaban a través de los procesos y actividades, se convierten en su activo más valioso, de esta manera, si no se aplican medidas de seguridad, pueden suscitar ocasiones que generen grandes problemas y consecuencias para la empresa. Por ello, la seguridad de la información ha logrado convertirse en una práctica de gran relevancia dentro de cualquier organización.

Igualmente, la forma en la que se gestiona y aprovecha toda la información garantizará un desempeño eficiente y óptimo de la empresa, debido a ello, es fundamental que se adopten evaluaciones y estimaciones de riesgo que permitan formular estrategias para minimizar o eliminar las fallas y vulnerabilidades basadas en las normativas y protocolos internacionales que establecen el uso correcto de las mismas, con la finalidad de mejorar el funcionamiento de sus actividades.

En este sentido, la realización de una auditoría servirá como apoyo para lograr un mayor desempeño y la mejora constante de la gestión de la información, es por esto que la planificación es la primera fase del proceso de la auditoría y de ella depende la eficiencia y efectividad en el logro de los objetivos propuestos. Debido a ello, la finalidad de esta investigación es diagnosticar el estado actual de la empresa Mundo Shop C.A. y, a través de ello, formular medidas preventivas y correctivas que mitiguen las vulnerabilidades que puedan afectar la información de forma significativa.

Esta investigación busca demostrar que los análisis realizados mediante la aplicación de una auditoría de la seguridad de la información en el departamento de administración servirán de gran utilidad para formular recomendaciones más factibles, al tener un

enfoque de revisión sistemática organizada, a fin de garantizar que la empresa Mundo Shop C.A. posea mayor confidencialidad, disponibilidad e integridad de su activo más importante, que es la información que procesa.

De esta manera, el presente trabajo servirá de apoyo para futuras investigaciones relacionadas con la seguridad de la información; permitiendo llevar a cabo nuevos proyectos innovadores y relevantes que logren dejar aportes significativos en las empresas y, a su vez, expandir los conocimientos profesionales del ingeniero de sistemas.

Por esta razón, esta investigación representa una herramienta estratégica que provee una rentabilidad a la empresa Mundo Shop C.A, permitiendo mejorar la gestión de sus activos informáticos y otorgando una mayor productividad debido a que la información se encuentra resguardada de la mejor manera. Así mismo, logrando beneficios en grandes cualidades, donde el uso de las tecnologías de la información es muy importante como una estrategia competitiva.

PARTE II

DESCRIPCIÓN TEÓRICA

Este capítulo tiene como finalidad sustentar la investigación mediante estudios similares, así como a través de basamentos legales con el objetivo de crear un soporte para el desarrollo de la misma. De modo que, este capítulo contiene los antecedentes de la investigación, las referencias teóricas, las bases legales y la definición de términos, los cuales permiten una compresión más profunda del objeto de estudio.

2.1 Antecedentes

Dentro de la recopilación de información del proyecto, así como la búsqueda de trabajos de investigación similares que sirvieran de apoyo y referencia para el desarrollo de la presente investigación, se encontraron varios trabajos relacionados, tales como:

Blas y Pretell (2020) realizaron una tesis titulada: *"MODELO DE LA SEGURIDAD DE LA INFORMACION PARA MEJORAR LA GESTION INFORMATICA EN LA MUNICIPALIDAD DISTRITAL DE FLORENCIA DE MORA"*, cuya modalidad de investigación fue descriptiva. La finalidad de esta investigación fue mejorar la gestión tecnológica en los aspectos de seguridad informática, debido a la inadecuada gestión segura de sus activos. Por ello, se utilizó una metodología basada en el uso de los controles de seguridad a nivel operativo de la norma ISO 27002. Para este estudio se aplicaron once dominios que conforman las buenas prácticas de seguridad de la información de la norma ISO 27002.

Este trabajo de investigación resultó de gran importancia, ya que la aplicación de los controles de seguridad de la norma ISO 27002 permiten manejar la gestión de riesgos y aseguramiento de la información de la manera más óptima, y con ello poder aumentar la competitividad organizacional. La citada investigación, resultó de gran ayuda para establecer las técnicas de recolección de datos, y así, evidenciar de manera más exacta la problemática existente.

Así mismo, se presenta la tesis desarrollada por Vásquez y Delgado (2019) titulada*: "MODELO DE LA SEGURIDAD INFORMATICA APLICANDO LA NORMA ISO/IEC 27001*

PARA PROTEGER LOS ACTIVOS DE INFORMACION EN LA EMPRESA BERENDSON NATACIÒN S.R.L", la cual fue desarrollada dentro de un modelo de investigación aplicada. Dentro de los objetivos se tuvo implementar un modelo adaptado de la norma ISO/IEC 27001 como medida preventiva para minimizar y contrastar los riesgos identificados. Por lo cual, el autor concluyó, que la aplicación de la norma ISO 27001 en los procesos de la empresa, establece la base para acreditar y asegurar la disponibilidad de los servicios que ofrece.

Este trabajo se ajusta en relación a la presente investigación, tomando en cuenta que la gestión de riesgos en una empresa debería considerarse como un proceso esencial, debido a que si no se conocen los riesgos a los que se encuentra expuesta la información y sus activos, no se podrán evitar posibles fallas o ataques que generen grandes consecuencias. Esta investigación fue de gran aporte para estructurar el enfoque de la prevención de riesgos.

De igual modo, Mina (2015) realizó un trabajo de investigación titulado: "*AUDITORIA DE LA SEGURIDAD DE LA INFORMACIÒN E INFRAESTRUCTURA DE TI, AL ÀREA DE TI DE LA EMPRESA DE ENERGÌA DE ARAUCA ENELAR E.S.P. DEL DEPARTAMENTO DE ARAUCA".* El objetivo de esta investigación fue realizar una auditoría de la seguridad de la información para identificar los riesgos a los que se encuentran expuestos los activos de información a causa de factores humanos, ambientales, internos, externos, deliberados e involuntarios. La modalidad de investigación fue cuantitativa y cualitativa, de esta manera, gracias a los resultados que se obtuvieron en el análisis de riesgos y la evaluación de los controles de la norma ISO/IEC 27002, se elaboraron políticas de seguridad de la información en las cuales se establecieron una serie de controles que permitieron mitigar los riesgos y, a su vez, gestionar adecuadamente sus activos de información.

La citada investigación constituye un referente importante, puesto que permitió evidenciar que la puesta en práctica de la norma ISO/IEC 27002 es de gran beneficio para las empresas, pues se utiliza como estrategia para mantener la competitividad y lograr manejar adecuadamente la información. Esta investigación sirvió de aporte para seleccionar la metodología MAGERIT de análisis y gestión de riesgo.

2.2 Bases teóricas

2.2.1 Auditoría

2.2.1.1 Definición

Meing, W. (1983) define la auditoria como:

> Un proceso sistemático para obtener y evaluar de forma objetiva, las evidencias relacionadas con informes sobre actividades económicas y otras situaciones que tienen una relación directa con las actividades que se desarrollan en una entidad pública o privada. El fin del proceso consiste en determinar el grado de precisión del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso.

Según esta afirmación de Meing, las auditorías son un tipo de estudio que busca evaluar los niveles de eficacia y eficiencia que se llevan a cabo en todos los procesos de la empresa, con la finalidad de formular recomendaciones y alternativas que permitan tomar decisiones para corregir los errores existentes y mejorar la puesta en práctica de los procesos.

Paralelamente, Noguez, V. (2016) menciona que:

> El proceso de auditoría, más que ser un requisito a cumplir, debe convertirse en uno de los motores de la mejora del Sistema de Gestión de Calidad (u otros Sistemas de Gestión), que permita la evaluación del desempeño y el logro de los objetivos de Calidad (objetivos del Sistema de Gestión).

En este sentido, según esta afirmación de Noguez, esta herramienta evaluativa busca mejorar continuamente los procesos de una organización para cumplir con las metas propuestas y brindar la mejor calidad de los productos y servicios que ofrecen.

Así mismo, Mendívil, V. (2002) explica que “el objetivo de la auditoria consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades. Para ello la auditoria les proporciona análisis, evaluaciones, recomendaciones, asesorías e información concerniente a las actividades realizadas”.

2.2.1.2 Fases de la auditoría

Las auditorias buscan el cumplimiento de un objetivo específico mediante un proceso sistemático de recolección de información, el cual tiene que pasar distintas fases. Es así como, según Uriarte, J. (2021) sostiene que toda auditoría se lleva a cabo siguiendo un plan de acción o fases que es importante respetar y cumplir. Estas fases son:

- Planeación, en la primera etapa de la auditoría se establece el propósito de este proceso y el alcance que tendrá. Además, se determina la duración, quiénes la llevarán a cabo y los detalles y actividades que se desarrollarán dentro del procedimiento.
- Ejecución, se ponen en marcha todos los procedimientos detallados en la etapa de planeamiento. Aquí se toma nota, se analizan documentos y archivos, se entrevista a las personas necesarias, se revisan y controlan procesos, entre otros.
- Informe, con todo el material reunido durante la auditoría, el auditor redacta un informe que incluye todos los datos relevados en el proceso. En esta presentación en forma escrita queda asentado todo el trabajo del auditor en la empresa y se detallan las falencias y los logros del área analizada.

De acuerdo con Uriarte, para llegar a las conclusiones y recomendaciones de la auditoría es necesario el cumplimiento de cada una de las fases, por ello se requiere de una planeación adecuada de las actividades que se emplearán, de modo que permita su realización de manera eficiente y eficaz.

2.2.1.3 Tipos de auditoría

En la actualidad, existen distintos tipos de auditorías, entre los enfoques más importantes se encuentran:

2.2.1.3.1 Auditoría Financiera

Sánchez, F. (2006), plantea que la auditoría financiera consiste en el examen, evaluación de los documentos, operaciones, registros y estados financieros de la entidad, para determinar si ellos reflejan razonablemente su situación financiera, así como, los resultados de sus operaciones, además del cumplimiento de las disposiciones económico-financiero y el control interno. Es decir, es un análisis de los procesos

financieros de una empresa, que tiene el objetivo final de generar un informe detallado con las irregularidades detectas que puedan afectar las actividades económicas y financiares de la misma.

2.2.1.3.2 Auditoría de Gestión

Redondo, R. (1996:2) explica que la auditoría de gestión es una técnica relativamente nueva de asesoramiento que ayuda a analizar, diagnosticar y establecer recomendaciones a las empresas, con el fin de conseguir con éxito una estrategia. Uno de los motivos principales por el cual una empresa puede decidir emprender una auditoría de gestión es el cambio que se hace indispensable para reajustar la gestión o la organización de esta. De este modo, este tipo de auditoría cumple un rol importante en gestión empresarial, la cual tiene como finalidad evaluar que los procesos y sus resultados cumplen de manera eficiente y eficaz con los objetivos propuestos y los recursos asignados.

2.2.1.3.3 Auditoría Administrativa

Franklin, E. (2007:11) sostiene que la auditoría administrativa “es la revisión analítica total o parcial de una organización con el propósito de precisar su nivel de desempeño y perfilar oportunidades de mejora para innovar valor y lograr una ventaja competitiva sustentable”. En este sentido, es la evaluación de toda la estructura organizativa de una empresa en la forma como lleva a cabo sus planes y métodos.

2.2.1.3.4 Auditoría informática de sistemas

Bajares, B. (2009) afirma que “su finalidad es el examen y análisis de los procedimientos administrativos y de los controles internos de la compañía auditada. Al finalizar el trabajo realizado, los auditores exponen en su informe aquellos puntos débiles que hayan podido detectar, así como las recomendaciones sobre los cambios convenientes a introducir, en su opinión, en la organización de la compañía”. De modo que, este tipo de auditoria sirve para analizar la manera en que se lleva a cabo los procedimientos en una empresa, con la finalidad de identificar si se está llevando a cabo de la manera más óptima y, si no, generar las recomendaciones más favorables.

2.2.1.3.5 Auditoría Interna

Fabián, L. (2020) sostiene que la auditoría interna “es una actividad diseñada para observar, investigar, cuestionar, verificar y proponer cambios y procedimientos. Es un control administrativo, cuya función es evaluar la eficiencia y la eficacia de otros controles”. De esta manera, este tipo de auditoria se utiliza para evaluar el desempeño de las distintas áreas de una empresa con la finalidad de evaluar la operatividad de los procesos.

2.2.1.3.6 Auditoría Externa

Sánchez, J. (2020) establece que la auditoría externa “es una práctica común en empresas e instituciones, donde profesionales auditores procedentes del exterior evalúan que una empresa funciona correctamente en relación a los procesos que asume y su marco normativo”. Por lo tanto, es un análisis objetivo de todos los procesos y métodos de una empresa, el cual es llevado a cabo mediante un profesional que no pertenece a la empresa.

2.2.2 Auditoría de la Seguridad de la Información

En el sitio web de Ambit-bts.com (2021) explica que:

> Es la herramienta principal para poder conocer el estado de seguridad en que se encuentra una empresa en relación con sus sistemas informáticos, de comunicación y acceso a internet. Estas auditorías permiten mejorar los sistemas e incrementar la ciberseguridad, siendo fundamentales para poder garantizar el funcionamiento del negocio y proteger la integridad de la información que manejan.

En este sentido, esta herramienta permite evaluar la seguridad y confiabilidad de la gestión de la información de una empresa, de esta manera determinando el estado actual de todos los sistemas informáticos con el fin de formular recomendaciones y medidas preventivas para mejorar la gestión de seguridad de la información.

Cabe destacar, que las auditorías abarcan muchos campos de aplicación para garantizar una buena gestión en las organizaciones, estas mismas se diferencian entre sí, debido a las técnicas que utilizan para el análisis y el tipo de estudio en el que se enfoca para medir el grado de cumplimiento de las normas establecidas.

2.2.3 Plan de Auditoría

Cole, B. (2021) puntualiza que “es un plan de acción que documenta qué procedimientos seguirá un auditor para validar que una organización cumple con las regulaciones de cumplimiento”. De acuerdo con el autor Cole, el plan de auditoría busca la creación de un informe con toda la información detallada de los procesos que se van a evaluar y medir, con el fin de identificar si la empresa está gestionando sus controles de manera adecuada.

2.2.4 Sistemas informáticos

Uriarte, J. (2020) define a los sistemas informáticos como “un sistema automatizado de almacenamiento, procesamiento y recuperación de datos, que aprovecha las herramientas de la computación y la electrónica para llevar a cabo su serie compleja de procesos y operaciones”. Según esta definición de Uriarte, son un conjunto de elementos dinámicos relacionados entre sí, que reúnen y procesan datos de manera organizada para realizar distintas tareas con el fin de ayudar en la toma de decisiones empresariales.

2.2.5 Normas y estándares informáticos

2.2.5.1 Norma

En el sitio web de concepto.de.com (2020) se afirma que “son reglas que se establecen con el propósito de regular comportamientos para mantener un orden determinado, y son articuladas para establecer las bases de un comportamiento aceptado dentro de una sociedad u organización”.

De modo que, esta afirmación sostiene que son todos aquellos dictámenes específicos que buscan lograr beneficios óptimos a partir de distintos criterios establecidos para que los procesos de las organizaciones cumplan con los objetivos propuestos.

2.2.5.2 Estándares

Borbón, J (2018) describe que “es un documento con contenido técnico-legal que establece un modelo o norma que refiere lineamientos a seguir para cumplir una actividad

o procedimientos. (…) Busca que los procesos y actividades de organizaciones y sus personas sean repetibles, organizados, y estructurados".

Esta afirmación de Borbón, refiere que son un modelo de condiciones y especificaciones a seguir para realizar un determinado procedimiento, así mismo, establecen los parámetros de controles a implementar para garantizar la mejor calidad y mejora constante de los servicios.

2.2.5.3 ISO/IEC 27001

En el sitio web de Iso.org.com (2022) señala que:

> Es ampliamente conocido y proporciona requisitos para un sistema de gestión de seguridad de la información (…). Su uso permite a las organizaciones de cualquier tipo gestionar la seguridad de los activos, como la información financiera, la propiedad intelectual, los detalles de los empleados o la información confiada por terceros.

De acuerdo con lo anterior, esta norma describe cómo gestionar la seguridad de la información, permitiendo evaluar todos los posibles riesgos que pudiesen afectar el desempeño de los procesos y a partir de ello formular las recomendaciones que mejor convengan para minimizarlos con la finalidad de garantizar confidencialidad, integridad y disponibilidad.

2.2.5.4 ISO/IEC 27002

Montoya, J. (2009) sugiere que "este estándar internacional va orientado a la seguridad de la información en las empresas u organizaciones. De modo, que las probabilidades de ser afectados por robo, daño o perdida de información se minimicen al máximo". De este modo, según Montoya, son lineamientos de buenas prácticas de la seguridad de la información con las mejores recomendaciones de los controles a implementar basados en la evaluación previa de los activos de información, con la finalidad de brindar el mayor nivel de seguridad posible de los datos de una organización.

2.2.5.5 ITIL

Donoso, F. y Ramírez, P. (2006:88) explique que ITIL "es una 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". En este sentido, son un grupo de las mejores prácticas con lineamientos para planificar y dar soporte, que se deben seguir para mejorar la gestión de los servicios de información según los requerimientos de la empresa.

2.2.5.6 CMMI

Huayta, M. (2006) explica que:

> Es un modelo de mejora de procesos que se provee a las empresas de requisitos esenciales para ejecutar procesos eficaces. Además, puede ser usado para la guía de implementación de procesos a través de una organización. (…) establece un conjunto de buenas prácticas para el desarrollo de productos y servicios cubriendo ciclo de vida desde la creación hasta su entrega, gestionando así sus incidencias, pero a menor escala.

De esta manera, esta herramienta permite un conjunto de buenas prácticas de los procesos dirigida a lograr mayor efectividad y eficiencia, permitiendo identificar en que estado de madurez se encuentra la empresa de acuerdo a la evaluación previa.

2.2.6 Gestión de la tecnología de la información

Pérez, L. (2021) señala que:

> Es el proceso de supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información dentro de una organización de TI. Este proceso de gestión asegura que todos los recursos tecnológicos y los empleados asociados son utilizados correctamente y de una manera que proporciona valor para la organización.

De acuerdo con Pérez, la gestión de la tecnología de la información consiste en la planificación y desarrollo de nuevas estrategias de soluciones tecnológicas, siendo entonces una pieza fundamental en las organizaciones para aumentar la productividad.

2.2.7 Metodología MAGERIT

Sandoval, J. (2017) sostiene que "es un método formal para investigar los riesgos que soportan los sistemas de información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos". De este modo, es una metodología que

permite analizar y gestionar los riesgos y vulnerabilidades de los sistemas informáticos con la finalidad de formular las medidas preventivas y correctivas para que toda la información se mantenga su confidencialidad, integridad y seguridad. Así mismo, Amaya, C. (2013) explica que "está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza".

2.3 Bases Legales

2.3.1 Constitución de la República Bolivariana de Venezuela

Art. 110.- El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para las mismas. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía.

2.3.2 Ley Especial Contra Los Delitos Informáticos

Art. 1.- Objeto de la Ley. La presente Ley tiene como objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes, o de los delios cometidos mediante el uso de dichas tecnologías, en los términos previstos de esta Ley.

Art. 2.- (…) Se entiende por Tecnología de la Información, rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el

desarrollo y uso del “hardware”, “firmware”, “software”, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

Art. 6.- Acceso indebido. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Art. 7.- Sabotaje o daño a sistemas. Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión intencional, por cualquier medio, de un virus o programa análogo.

Art. 10.- Posesión de equipos o prestación de servicios de sabotaje. Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Art. 11.- Espionaje informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación

de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

Art. 12.- Falsificación de documentos. Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Art. 17.- Apropiación de tarjetas inteligentes o instrumentos análogos. Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Art. 20.- Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

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.

Art. 22.- Revelación indebida de data o información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

En este sentido, esta ley es importante porque se encarga de prevenir y sancionar los delitos informáticos que pueden llegar a ser cometidos a una empresa por personas internas o externas, por lo cual esta ley busca proteger los activos informáticos y de información. De modo que, los citados artículos de la presente ley permitieron mostrar algunos de los distintos riesgos que podrían suscitar, atentar, menoscabar y violentar contra los sistemas informáticos, y con ello causar diferentes daños a la información que posee la empresa. Por lo tanto, es fundamental que las empresas conozcan esta ley que se encarga de regular y prevenir estos tipos de delitos mencionados para garantizar un buen funcionamiento.

2.3.3 Ley Orgánica de Ciencia, Tecnología e Innovación

Art. 3.- Forman parte del Sistema Nacional de Ciencia, Tecnología e Innovación, Las instituciones Públicas o Privadas que generen u desarrollen conocimientos científicos y tecnológicos y procesos de innovación, y las personas que se dediquen a la planificación, administración y ejecución y aplicación de actividades que posibiliten la vinculación entre la ciencia, la tecnología y la sociedad.

Cabe destacar, que el desarrollo de la presente investigación se basa en lo contemplado en las prescritas leyes citadas como respaldo para llevar a cabo una auditoria de la seguridad de la información. De modo, que todas las empresas deben cumplir con los lineamientos expuestos para garantizar la legalidad de sus procesos. De la misma forma, estos basamentos legales permiten que la realización de este proyecto se desarrolle de manera ética y legal.

2.4 Definición de términos

Activo:

Son los recursos que forman parte del sistema de la empresa como el hardware, software, datos, infraestructura y personas. (Mifsud, E. 2012)

Amenaza:

Incidente nuevo o recién descubierto que tiene el potencial de dañar un sistema o una empresa en general. (Tamayo, S. 2021)

Análisis:

Estudio exhaustivo de las diversas partes de un elemento con el objetivo de caracterizarlo y comprenderlo. (Bembibre, V. 2009)

Confidencialidad:

Los datos son accesibles solamente por aquellos usuarios y procesos autorizados. (Fernández, L. 2020)

Contingencia:

Es la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos, como: equipos informáticos y de comunicación, software, datos, instalaciones, programas de cómputo, entre otras. (Casas, F. 2017)

Disponibilidad:

La información debe encontrarse a disposición para quienes quieran acceder a ella, incluidos personas, aplicaciones, operaciones, entre otros. Este acceso debe ejecutarse solo para personas autorizadas en cada caso. (DocuSing.com, 2021)

Evaluación:

Proceso mediante el cual se intenta determinar el valor de una cosa o persona o el grado de cumplimiento de determinados objetivos. (Salazar, H. 2015)

Información:

Es un conjunto de datos acerca de algún suceso, hecho o fenómeno, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo. (Thompson, I. 2008)

Integridad:

Cualidad de los activos de información donde se asegura que la información y sus métodos de proceso se manejan exactos y completos. (Instituto Nacional de Tecnología de la Comunicación de España, 2013)

Riesgo:

Se considera la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él causando daños a la organización. (Instituto Nacional de Tecnología de la Comunicación de España, 2013)

Sistema de información:

Conjunto de componentes que interactúan entre sí con el propósito de alcanzar un objetivo determinado, el cual debe satisfacer las necesidades de información de dicha empresa. (García, I. 2018)

Vulnerabilidad:

Son las debilidades que tienen los activos o grupos de activos que pueden ser aprovechadas por una amenaza. (Instituto Nacional de Tecnología de la Comunicación de España, 2013)

PARTE III

DESCRIPCIÓN METODOLÓGICA

En este capítulo se definirán de manera detallada las distintas herramientas que se emplearán en la investigación para facilitar su desarrollo. En este sentido, de acuerdo con Balestrini, M. (2006:125), se destaca que “El marco metodológico es la instancia referida a los métodos, las diversas reglas, registros, técnicas, y protocolos con los cuales una teoría y su método calculan las magnitudes de lo real”. De este modo, se establecen las técnicas y métodos necesarios para la investigación.

3.1 Naturaleza de la investigación

Los enfoques de investigación buscan cumplir objetivos particulares que engloban todo el proceso investigativo, asimismo Mata, L. (2019) explica que la naturaleza de la investigación “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”. De esta manera, la presente investigación está enfocada en el modelo de investigación cuantitativo, ya que se basa en cuantificar la recopilación y análisis de los datos con la finalidad de comprenderlos y explicarlos, permitiendo medir el grado de efectividad de los controles definidos para la seguridad de la información.

En este sentido, Tamayo, M. (2007) afirma que la investigación cuantitativa:

> Consiste en el contraste de teorías ya existentes a partir de una serie de hipótesis surgidas de la misma, siendo necesario obtener una muestra, ya sea en forma aleatoria o discriminada, pero representativa de una población o fenómeno objeto de estudio.

De este modo, según Tamayo este enfoque es una herramienta para obtener y analizar los datos recopilados, con la finalidad de convertirlos en información cuantificable a través de diferentes técnicas y llevar a cabo conclusiones. Así mismo, Sampieri, R. Fernández, C. y Baptista, P (2004) explican que “el enfoque cuantitativo se fundamenta en un esquema deductivo y lógico que busca formular preguntas de investigación e hipótesis para posteriormente probarlas”

3.1.1 Tipo de Investigación

Los tipos de investigación establecen la modalidad de estudio que se llevará a cabo, así mismo, rigen la forma en la que se recolectarán los datos, de esta manera Tamayo y Tamayo, M. (2007) explica que la investigación descriptiva “comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos”. Por lo que, la investigación descriptiva se enfoca en especificar de forma precisa y clara las características de los procesos de la investigación partiendo del diagnóstico. Este método permitirá recopilar y describir toda la información de los procesos actuales para la seguridad de la información que utiliza la empresa Mundo Shop C.A. y a partir de esto generar las recomendaciones que más convengan.

Así mismo, esta investigación se encuentra enmarcada dentro de un proyecto factible, que de acuerdo con la UPEL (1998:7) se define como un estudio “que consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales”. Por lo tanto, este tipo de investigación consiste en la creación y diseño de recomendaciones que sirvan para resolver problemas previamente identificados, la cual permitirá alcanzar los objetivos establecidos en función de los requerimientos de una organización.

De esta manera, el objetivo de la presente investigación se ajusta de acuerdo al tipo de investigación de tipo proyecto factible, ya que busca proponer las mejores recomendaciones para la seguridad de los sistemas informáticos a través de una auditoría de la seguridad de la información.

3.1.2 Diseño de la investigación

En esta etapa de la investigación se establecen los lineamientos de trabajo para llevar a cabo dicha investigación, por lo tanto, Arias, F. (1999:30) define el diseño de la investigación como “la estrategia que adopta el investigador para responder al problema planteado”. De modo que, constituye el plan que el investigador utiliza para dar respuestas a sus interrogantes.

En este sentido, Palella, S. y Martins, F. (2008:88) definen que:

> La investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables. Estudia los fenómenos sociales en su ambiente natural. El investigador no manipula variables debido a que esto hace perder el ambiente de naturalidad en el cual se manifiesta.

En tal efecto, este proceso permite recopilar los datos de manera sistemática y exacta a fin de describirlos e interpretarlos para determinar el estado actual de la situación problema. Así mismo, la presente investigación emplea el diseño de la investigación de campo para lograr una recolección directa de toda la información y así evaluar niveles de riesgo y vulnerabilidad de los sistemas informáticos de la empresa Mundo Shop C.A.

3.1.3 Población y muestra

Según Arias, F. (2006:81) la población es “un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el problema y por los objetivos de estudio”. Por lo tanto, son todos los elementos de los que se puede recopilar y extraer información del objetivo de estudio. Es por esto que, para fines de esta investigación, la población estará constituida por todo el personal del departamento de administración que cumplen distintos roles como: gerente de tienda, encargado de administración, asistente administrativo, encargado de ventas y dos (2) cajeros.

Por otro lado, Tamayo y Tamayo, M. (2006:176) definen la muestra como "el conjunto de operaciones que se realizan para estudiar la distribución de determinados caracteres en totalidad de una población universo, o colectivo partiendo de la observación de una fracción de la población considerada". En tal efecto, para el desarrollo de esta investigación la muestra es la totalidad de la población establecida, la cual corresponde a seis (6) personas.

3.2 Técnicas de recolección de datos

Existen distintas técnicas que permiten recopilar toda la información necesaria para la investigación que sirven para dar respuestas a las interrogantes. En este sentido, Razo, C. (2011:119) define que:

> Son las herramientas utilizadas por el investigador en la recopilación de los datos, las cuales se seleccionan conforme a las necesidades de la investigación en función de la muestra elegida, y se aplican tanto para hacer la recolección, la observación y/o la experimentación.

De acuerdo con Razo, es un proceso sistemático para recabar información sirviendo de base para sustentar el desarrollo de la investigación que se está llevando a cabo, así mismo permitirá alcanzar los objetivos propuestos. De esta manera, se utiliza técnicas de recolección de datos, tales como:

En primer lugar, se va a emplear la observación, la cual consiste en visualizar los comportamientos de las personas involucradas con el fin de describirlos y comprenderlos. De modo que, según Arias, F. (2006:69) la observación es "una técnica que consiste en visualizar o captar mediante la vista, en forma sistemática, cualquier hecho, fenómeno o situación que se produzca en la naturaleza o en la sociedad, en función de unos objetivos de investigación preestablecidos". Por lo tanto, se aplicará con la finalidad de conocer cuál es la situación actual que presentan los sistemas informáticos. El instrumento que se empleará será el block de nota.

Así mismo, se utilizará la entrevista, esta técnica consiste en obtener la información a través de preguntas y respuestas para saber las actitudes y opiniones de las personas involucradas en la investigación. Por lo tanto, Sabino, C. (1992:116) explica que:

> La entrevista desde el punto de vista del método es una forma específica de interacción social que tiene por objeto recolectar datos para una investigación. El investigador formula preguntas a las personas capaces de aportarles datos de interés, estableciendo un dialogo peculiar, asimétrico, donde una de las partes busca recoger informaciones y la otra es la fuente de esas informaciones.

De esta manera, se aplicará una entrevista estructurada a la encargada de administración de la empresa Mundo Shop C.A. El instrumento de que se utilizará será la guía de entrevista.

Seguidamente, se empleará la encuesta, esta técnica que consiste en obtener información mediante preguntas sistemáticas de los datos que desea obtener para luego evaluarlos. Así mismo, de acuerdo con García, M (1993), se define como:

> Es una investigación realizada sobre una muestra de sujetos representativa de un colectivo más amplio, que se lleva a cabo en el contexto de la vida cotidiana, utilizando procedimientos estandarizados de interrogación, con el fin de obtener mediciones cuantitativas de una gran variedad de características objetivas y subjetivas de la población.

En tal sentido, es un procedimiento de investigación que recopila la información a través de preguntas sobre de algún suceso en una determinada población, permitiendo obtener la opinión y el punto de vista de los trabajadores, así como el grado de cumplimiento de los dominios de la norma ISO 27001 en la empresa Mundo Shop C.A. El instrumento para la encuesta que se utilizará será el cuestionario de control.

Por último, Hurtado, J (2008) explica que el análisis crítico es “el proceso mediante el cual el investigador recopila, revisa, analiza, selecciona y extrae información de diversas fuentes, acerca de un tema en particular, con el propósito de llegar al conocimiento y compresión más profundos del mismo”. De este modo, esta técnica permite analizar de manera más amplia el objeto de estudio, por ello, se utilizará es técnica de recolección que provee un marco de referencia para elaborar las recomendaciones partiendo de las normativas internacionales ISO/IEC 27001 e ISO/IEC27002. El instrumento para esta técnica será el bloc de notas.

3.3 Técnicas de análisis de datos

Estas técnicas permiten organizar y modelar los datos recolectados con la finalidad de tener una mayor comprensión de los mismos. De este modo, según Arias, F. (2006:119) “en este punto se describen las distintas operaciones a las que serán sometidos los datos que se obtengan”. En tal sentido, con estas técnicas se logra sintetizar la información para generar conclusiones significativas y poder cumplir los objetivos propuestos.

Para el análisis de los datos obtenidos a través de la observación se empleará el diagrama de causa y efecto, el cual permite clasificar y ordenar las causas de un determinado problema, analizando todos los elementos que involucra

En este sentido, González, R. (2012) define que un diagrama causa-efecto:

> Es una forma de organizar y representar las diferentes teorías propuestas sobre las causas de un problema. (…) permite, por tanto, representar gráficamente el conjunto de causas que dan lugar a una consecuencia, o bien el conjunto de factores y sub-factores que contribuyen a generar un efecto común.

De este modo, con esta técnica se podrá sintetizar toda la información recolectada a través del instrumento bloc de notas y así, evidenciar los problemas que presentan los procesos informáticos con la finalidad de identificar las causas que lo generan.

Por otro lado, como técnica de análisis para las entrevistas se utilizará el flujograma que, de acuerdo con Sánchez, A. (2021) se define como “un esquema que muestra un proceso o sistema paso por paso, utilizado en numerosas áreas, ya sea para planificar, documentar, mejorar, etc. Estos utilizan una serie de símbolos con los cuales se indica cada uno de los pasos que se llevan a cabo”. De este modo, esta técnica permite representar de manera gráfica y secuencial los procesos para evaluar los controles definidos para la seguridad de la información.

Además, para el análisis de los cuestionarios de control se utilizará la matriz de vulnerabilidad que, según Medina, P. (s/f) se define como “la medida o grado de debilidad o sensibilidad de ser afectados por amenazas o riesgos, en función de la frecuencia y severidad de los mismos (…) con el fin de formular planes de acción, para su protección o mejora”. Esta técnica permitirá evaluar cada uno de los dominios donde se obtendrá una visión de forma gráfica de cada situación evaluada.

Por último, para el análisis de la revisión documental se utilizará el análisis crítico que, según Sabino, C. (2006) consiste en “la revisión de un conjunto de informaciones a partir de las cuales se realizan inferencias, razonamientos, comparaciones, argumentaciones, deducciones, criticas, estimaciones y explicaciones”. De esta manera, es un tipo de análisis que determina que un objeto de estudio cumpla con ciertos parámetros. Esta técnica se utilizará para analizar las normativas internacionales y a partir de ello formular las recomendaciones de auditoría que más convengan.

PARTE IV

ANALISIS Y PRESENTACION DE RESULTADOS

Este capítulo tiene como objetivo procesar la información recabada con las técnicas de recolección de información descritas en la parte anterior, y así mostrar el alcance de los objetivos de investigación. De esta manera, permitiendo interpretar de forma más clara los resultados obtenidos y con ello generar las conclusiones y recomendaciones que sirvan para mejorar los procesos de la empresa Mundo Shop C.A.

4.1 Análisis de la situación actual de los sistemas informáticos que se encuentran en la empresa Mundo Shop C.A.

La empresa Mundo Shop C.A. se dedica la venta y comercialización de ropa para damas, caballeros y niños, ofreciendo el mejor servicio y calidad. Esta misma, cuenta con una estructura jerárquica simple. En este sentido, para conocer de manera clara la situación actual de los sistemas informáticos, mediante un recorrido por las instalaciones en compañía del encargado, se logró observar y recopilar información, a través del instrumento bloc de notas, de distintos factores que son causantes de que la información se encuentre más vulnerable.

En efecto, se procedió al análisis de todos los apuntes del bloc de notas, para identificar los factores que inciden o afectan la seguridad de la información de la empresa Mundo Shop C.A.. De esta manera, podemos decir que el departamento de administración es el que maneja la mayor cantidad de información sensible, donde uno de los factores con mayor riesgo es la inexistencia de controles de acceso, por lo que cualquier personal tiene acceso a manipular los equipos y toda la información que se almacena en ellos. De la misma forma, no cuentan con una estructura adecuada a los requerimientos de la empresa; y poseen una disposición inadecuada del cableado, además del desconocimiento de medidas de control que garanticen la seguridad de la información por parte del personal, siendo estos factores determinantes al momento de gestionar cualquier tipo de información.

De este modo, mediante la aplicación de una auditoría de la seguridad de la información, se podrán dar las mejores recomendaciones para mitigar los riesgos y vulnerabilidades presentes en los activos de la empresa, y así, llevar a cabo las mejores prácticas para proteger la información de mejor manera.

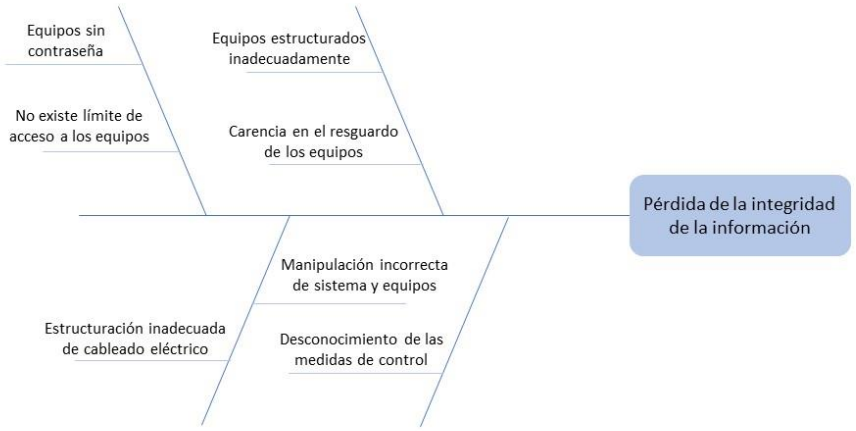

Figura 1. Diagrama de Causa y Efecto: perdida de la integridad de la información.
Fuente: Elaboración Propia, 2022.

Aunado a esto, la implementación de las normativas y estándares garantiza a las empresas que un procedimiento de trabajo se realice de la manera óptima, con el objetivo aprovechar al máximo los recursos y aumentar la competitividad. Por lo cual, se buscó conocer si están alineados a una normativa internacional mediante la aplicación de un cuestionario a la encargada de administración, la cual permitió identificar qué controles aplican para la seguridad de la información de la infraestructura y aplicaciones. De esta manera, la escala de valores para evaluar los resultados obtenidos se encuentra conformada por:

INFRAESTRUCTURA		
No cumple	0	No cumplen con los estándares internacionales aplicables a las áreas de gestión de información.

Deficiente	1	Conocen los estándares, pero no lo aplican en todos los procesos de gestión de información.
Suficiente	2	Cumplen con las políticas y controles de seguridad para la protección áreas de gestión de información.
Excelente	3	Se implementan estándares en la ejecución de sus procesos.

Tabla 1. Ponderación de Infraestructura, Fuente: Elaboración Propia 2022.

Segmento/ Rubros	*Infraestructura, controles y Gestiones*						
Objetivo de Control							
Detallar la infraestructura de las áreas de manejo de información y examinar la aplicación de estándares y normativas, para los controles y gestiones							
Preguntas	**(0) No cumple**	**(1) Deficiente**	**(2) Suficiente**	**(3) Excelente**	**Resultados Obtenidos**	**Resultados Esperados**	**%**
¿Conocen alguna normativa internacional aplicable al manejo de la información?		**1**			**6**	**18**	**33%**
¿Se rigen por algún estándar internacional, para la gestión de información?	**0**						
¿Las TIC y el equipo relacionado al manejo de información se encuentran en áreas adecuadamente protegidas?		**1**					
¿Existen controles para minimizar los riesgos de amenazas físicas?		**1**					
¿Se realiza mantenimiento periódico de los equipos de modo a asegurar la continua disponibilidad e integridad?			**2**				

¿Tienen políticas y controles definidos para la gestión y control de la seguridad de la información?		**1**					
Total		**4**	**2**				

Tabla 2. Cuestionario realizado al departamento de Administración de la empresa Mundo Shop, Fuente: Elaboración Propia 2022.

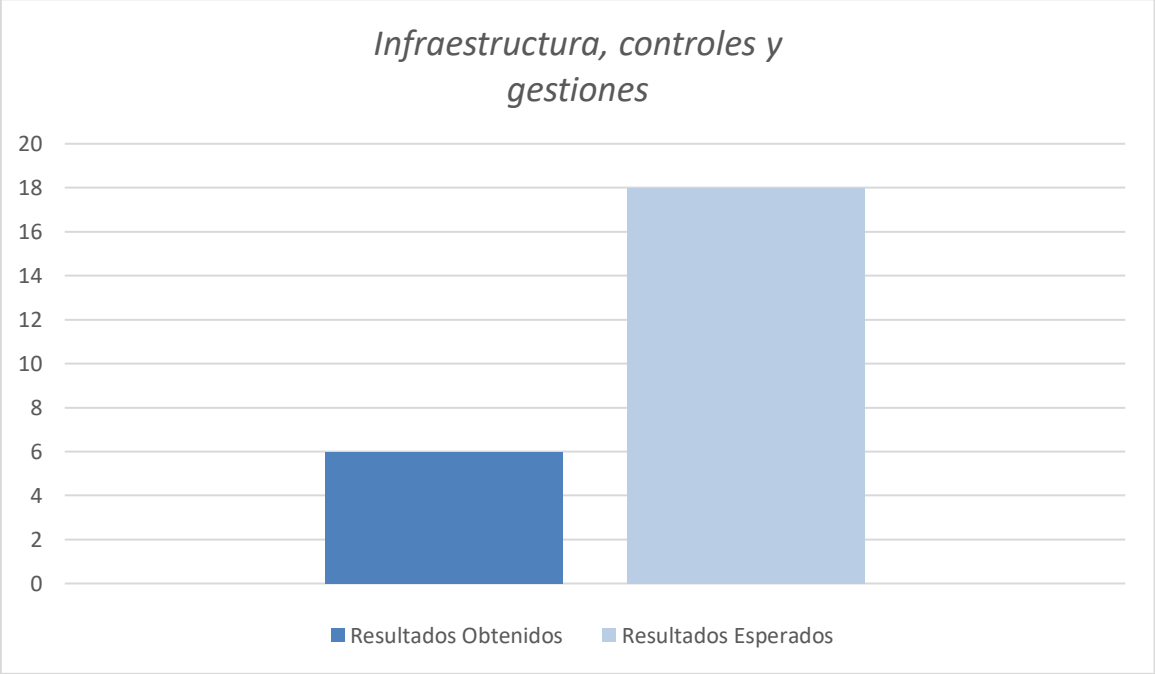

Gráfico 1: Descripción de la infraestructura, controles y gestiones, Fuente: Elaboración Propia 2022.

De esta manera, gracias a los resultados obtenidos se logró determinar que la empresa no se rige por ningún estándar internacional que garantice un buen funcionamiento de las tecnologías de la información; siendo punto de partida para la evaluación exhaustiva de técnicas que midan los niveles de riegos que pueden tener el no cumplir parámetros para el manejo de la información.

De igual forma, se buscó conocer si las aplicaciones que utiliza la empresa Mundo Shop C.A. manejan las políticas de seguridad y estándares que garanticen el buen funcionamiento de la gestión de la información que se maneja en ellas.

APLICACIONES		
No cumple	0	No se cuenta con ningún de parámetros con respecto al uso de aplicaciones.
Deficiente	1	Cuenta con ciertos niveles de usuarios, pero no se especifica responsable.
Suficiente	2	Posee estándares con respecto al uso de aplicaciones, que le permiten desempeñar sus funciones.
Excelente	3	Cumple con todos los lineamientos y estándares para el uso de aplicaciones.

Tabla 3. Ponderación de aplicaciones, Fuente: Elaboración Propia 2022.

Segmento/ Rubros	*Aplicaciones*
Aplicación	*MySQL*
Objetivo de Control	
Identificar las incidencias con respecto al uso de aplicaciones para la gestión y procesamiento de información	

Preguntas	**(0) No cumple**	**(1) Deficiente**	**(2) Suficiente**	**(3) Excelente**	**Resultados Obtenidos**	**Resultados Esperados**	**%**
¿Existen manuales para el uso correcto de la aplicación?			**2**		**6**	**24**	**25%**
¿Se presentan fallas en la ejecución de aplicaciones?			**2**				
¿Se definen responsables para solventar fallas de aplicaciones?	**0**						
¿Se realizan pruebas periódicas y después de cambios importantes?	**0**						

¿Existen controles de accesos definidos?		**1**					
¿Se cambian las contraseñas por defecto del fabricante?	**0**						
¿Con frecuencia se revisan si las contraseñas utilizadas son débiles?		**1**					
¿Hacen uso de controles técnicos para el acceso de la información, como longitud mínima de contraseña, reglas de complejidad, contraseñas compartidas, entre otros?	**0**						
Total		**2**	**4**				

Tabla 4. Cuestionario realizado al departamento de Administración de la empresa Mundo Shop, Fuente: Elaboración Propia 2022.

Segmento/ Rubros		*Aplicaciones*					
Aplicación		*Sistema D3xD Gisin3*					
Objetivo de Control							
Identificar las incidencias con respecto al uso de aplicaciones para la gestión y procesamiento de información							
Preguntas	**(0) No cumple**	**(1) Deficiente**	**(2) Suficiente**	**(3) Excelente**	**Resultados Obtenidos**	**Resultados Esperados**	**%**
¿Existen manuales para el uso correcto de la aplicación?		**1**					

¿Se presentan fallas en la ejecución de aplicaciones?			**2**		**6**	**24**	**25%**
¿Se definen responsables para solventar fallas de aplicaciones?	**0**						
¿Se realizan pruebas periódicas y después de cambios importantes?	**0**						
¿Existen controles de accesos definidos?		**1**					
¿Se cambian las contraseñas por defecto del fabricante?	**0**						
¿Con frecuencia se revisan si las contraseñas utilizadas son débiles?		**1**					
¿Hacen uso de controles técnicos para el acceso de la información, como longitud mínima de contraseña, reglas de complejidad, contraseñas compartidas, entre otros?		**1**					
Total		**4**	**2**				

Tabla 5. Cuestionario realizado al departamento de Administración de la empresa Mundo Shop, Fuente: Elaboración Propia 2022.

Segmento/ Rubros	*Aplicaciones*
Aplicación	*SAP*
Objetivo de Control	
Identificar las incidencias con respecto al uso de aplicaciones para la gestión y procesamiento de información	

Preguntas	(0) No cumple	(1) Deficiente	(2) Suficiente	(3) Excelente	Resultados Obtenidos	Resultados Esperados	%
¿Existen manuales para el uso correcto de la aplicación?		**1**					
¿Se presentan fallas en la ejecución de aplicaciones?			**2**				
¿Se definen responsables para solventar fallas de aplicaciones?	**0**						
¿Se realizan pruebas periódicas y después de cambios importantes?	**0**						
¿Existen controles de accesos definidos?			**2**		**7**	**24**	**29%**
¿Se cambian las contraseñas por defecto del fabricante?		**1**					
¿Con frecuencia se revisan si las contraseñas utilizadas son débiles?		**1**					
¿Hacen uso de controles técnicos para el acceso de la información, como longitud mínima de contraseña, reglas de complejidad, contraseñas compartidas, entre otros?		**1**					
Total		**3**	**4**				

Tabla 6. Cuestionario realizado al departamento de Administración de la empresa Mundo Shop, Fuente: Elaboración Propia 2022.

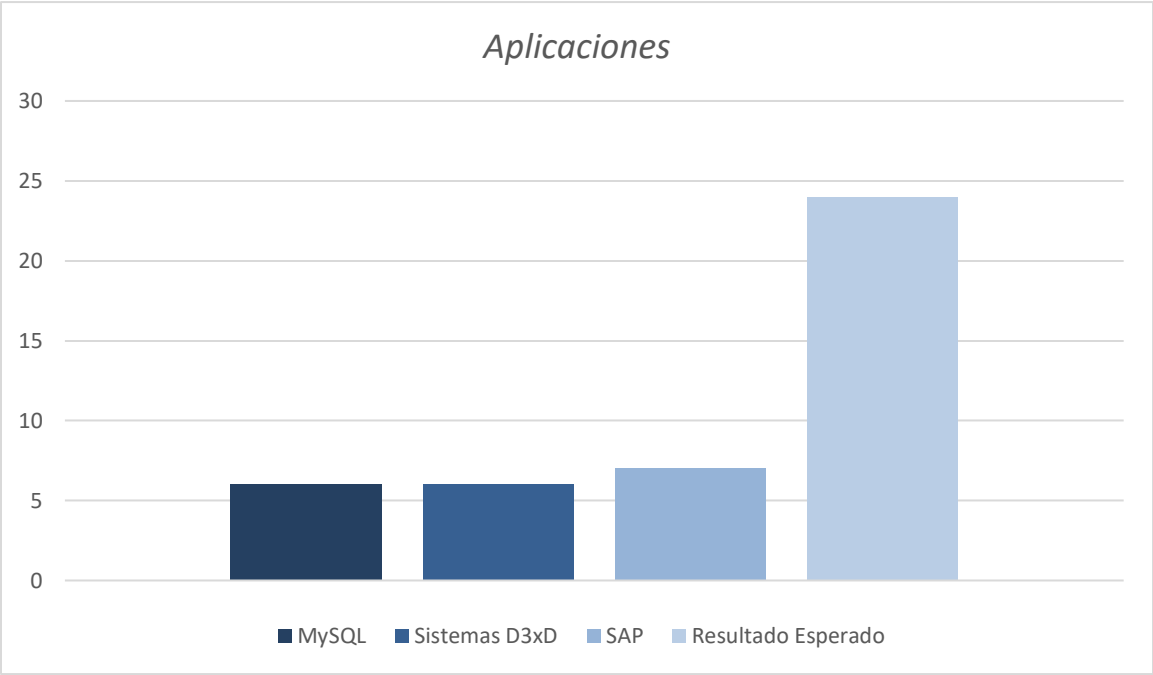

Gráfico 2: incidencias con respecto al uso de aplicaciones para la gestión y procesamiento de información, Fuente: Elaboración Propia 2022.

En este sentido, gracias a los resultados obtenidos se logró evidenciar que las aplicaciones que utilizan para el manejo de la información en el departamento de administración no se implementan políticas de resguardo y seguridad adecuadas que garanticen la integridad y credibilidad de la misma. Dando paso así, a una evaluación exhaustiva mediante una auditoria de la seguridad de la información.

4.2 Evaluación de los controles definidos para la seguridad de la información de la empresa Mundo Shop C.A.

En este punto se busca conocer si la información resguardada se encuentra almacenada correctamente y si se está aprovechando al máximo, para ello se aplicó una entrevista a la administradora mediante una guía de entrevista, la cual estuvo conformada por 8 preguntas puntuales para obtener y recopilar información sobre los datos de los clientes, logrando saber de qué manera están siendo utilizados. Debido a ello, permitió ordenar e interpretar toda la información obtenida a través de la representación mediante un flujograma de procesos, y así conocer el procedimiento que utiliza la empresa para recabar los datos de los clientes al momento de realizar una compra.

El proceso de registro de clientes está definido de tal forma que se ingresan las credenciales para acceder al sistema, seguidamente se abre el módulo de ventas, luego de ello se introducen los datos del cliente, se verifica si es un cliente nuevo, si no existe se ingresan los datos solicitados y se procede a guardar los datos.

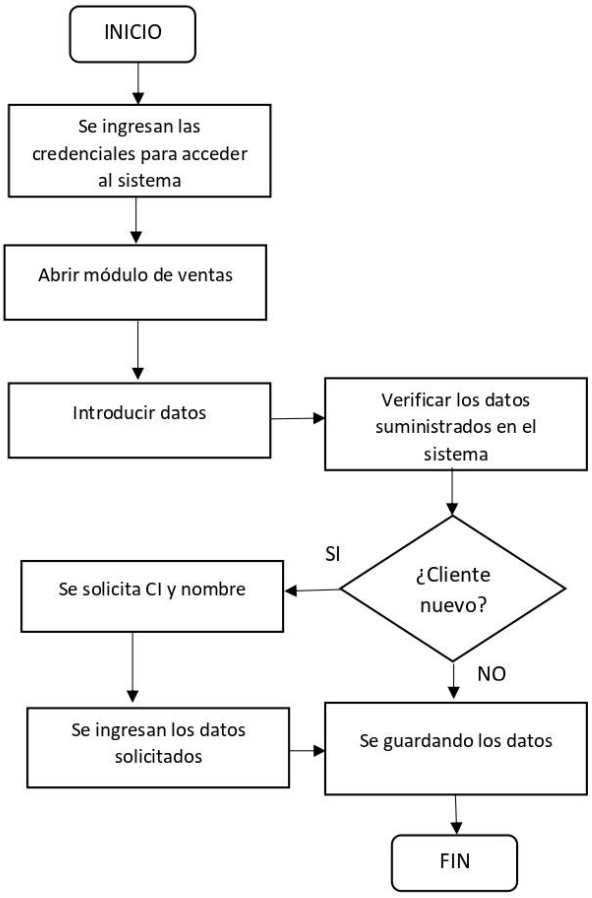

Figura 2. Flujograma proceso de registros de cliente.
Fuente: Elaboración Propia, 2022.

De esta manera, se pudo evidenciar que el proceso de recopilación de datos de los clientes no se lleva de la mejor manera, debido a que no se tiene un control exhaustivo de la información de los clientes, por lo que los datos tienden a duplicarse y a poseer errores, ya que no se realiza una validación de los mismos con la cédula del cliente. Además, no se registra un número de teléfono y dirección que proporcione más información de los clientes y sirvan de apoyo para incrementar las ventas mediante estrategias de publicidad.

En este sentido, una vez obtenidos estos resultados y los del objetivo anterior, se procedió a elaborar el plan de auditoría con las especificaciones, enfoque y alcance de la misma, en donde se plasman todos los pasos a seguir. De esta manera, se obtuvo un documento comprendido por los planes formales a desarrollar, así como los tiempos de ejecución del cumplimiento de los objetivos, incluyendo los recursos utilizados para cada actividad. Dicho plan se encuentra comprendido por:

4.2.1 Clasificación de la Auditoría

La presente investigación se calificó como una auditoría externa, debido a que el investigador no guarda ningún tipo de relación con la empresa Mundo Shop C.A.. De esta manera, se logrará un dictamen independiente, confiable y transparente, que dé validez a la información obtenida.

4.2.2 Tipo de Auditoría

El tipo de auditoría que se implementó se basó en una auditoría de la seguridad de la información, debido a que analiza la forma en la que operan los sistemas de información y los controles internos utilizados en la empresa Mundo Shop C.A., para la formulación de sugerencias que coadyuven en el mejoramiento de la seguridad de la información y la reducción de los riesgos en dichos sistemas.

4.2.3 Alcance de la Auditoría

Una vez establecidos los criterios preliminares para la realización de la auditoría, se procedió a determinar los puntos que serían evaluados, en este caso el departamento de administración, debido a que maneja la mayor cantidad de información vulnerable. Es por ello, que se consideraron varios aspectos, muy específicos, en el desenvolvimiento de la auditoría de seguridad de información, tales como:

4.2.3.1 Recursos para la Realización de la Auditoría

Para la ejecución de la auditoría de seguridad de la información en la empresa Mundo Shop C.A., se requirió de recursos de carácter humano, informático, materiales de oficina y documentación.

Humano

- Personal para la auditoría: La auditoría se llevó a cabo por el investigador Br. Angel Gómez.
- Personal del área auditada: Este estuvo conformado por el personal que labora en la empresa Mundo Shop C.A., cubriendo todos los niveles organizacionales.
- Personal de la Universidad: Lo integraron la tutora académica, Coordinación de Investigación y Pasantías y profesores especialistas en el área.

Informático

- Hardware: dispositivos de almacenamiento, teléfono inteligente y dispositivos periféricos.
- Software: Herramientas para la recolección de información y herramientas de Office
- Laptop

Materiales de Oficina

- Hojas Blancas
- Cuaderno
- Lápices
- Bolígrafos
- Resaltadores

Documentación

- ISO/IEC 27001
- ISO/IEC 27002
- MAGERIT V3.0

4.2.3.1.2 Programa de Auditoría

Esta se determinó de acuerdo con la normativa y dominios aplicados al diseño de los instrumentos de recolección de información. Para el desarrollo de la presente investigación, se hizo uso del estándar internacional ISO 27001:2013, del cual fueron

seleccionados los dominios y sub-dominios que se consideraron necesarios y oportunos para la ejecución de la auditoría, siendo estos:

- **A.5 Políticas de seguridad de la información**
    - A.5.1 Directrices de gestión de la seguridad de la información:
        - A.5.1.1 Políticas para la seguridad de la información
        - A.5.1.2 Revisión de las políticas para la seguridad de la información
- **A.6 Controles de seguridad de la información**
    - A.6.1 Organización interna
        - A.6.1.1 Roles y responsabilidades en seguridad de la información.
        - A.6.1.4 Revisión de las políticas para la seguridad de la información.
- **A.8 Gestión de activos**
    - A.8.1 Responsabilidad sobre los activos
        - A.8.1.1 Inventario de activos
        - A.8.1.3 Uso aceptable de los activos
- **A.9 Control de acceso**
    - A.9.1 Requisitos de negocio para el control de acceso:
        - A.9.1.2 Acceso a las redes y a los servicios de red
    - A.9.2 Gestión de acceso de usuario
        - A 9.2.4 Gestión de la información secreta de autenticación de los usuarios.
- **A.11 Seguridad física y del entorno**
    - A.11.1 Requisitos de negocio para el control de acceso:
        - A.11.1.1 Perímetro de seguridad física.
        - A.11.1.2 Controles físicos de entrada.
        - A.11.1.4 Protección contra las amenazas externas y ambientales.
    - A.11.2 Seguridad de los equipos.
        - A.11.2.1 Emplazamiento y protección de equipos.
        - A 11.2.2 Instalaciones de suministro.
        - A 11.2.3 Seguridad del cableado.

- A 11.2.4 Mantenimiento de los equipos.
- A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia.

- **A.12 Seguridad de las operaciones.**
  - A.12.2 Protección contra el software malicioso (Malware)
    - A.12.2.1 Controles contra el código malicioso.
  - A.12.3 Copias de Seguridad.
    - A.12.3.1 Copias de seguridad de la información.

4.2.3.3 Cronograma de auditoría

Actividades		SEMANAS											
		1	2	3	4	5	6	7	8	9	10	11	12
FASE I: CONOCIMIENTO	Conocer el área a auditar												
	Realizar un recorrido para recopilar información y determinar el estado de la empresa												
FASE II: PLANEACIÓN	Elaborar el plan a llevar a cabo en el desarrollo de la auditoría												
	Analizar las medidas de control, seguridad y políticas de la empresa												
FASE III: EJECUCIÓN	Recolectar información mediante de los instrumentos definidos												
	Revisión los hallazgos conseguidos a largo de la auditoría												
	Identificar los riesgos y vulnerabilidades encontrados en la empresa												
FASE VI: RESULTADOS	Formular las recomendaciones												

Tabla 7. Cronograma de Auditoría, Fuente: Elaboración Propia 2022.

4.3 3. Validación del cumplimiento de las regulaciones para la seguridad de la información en la empresa Mundo Shop C.A.

El cuestionario para el desarrollo de la auditoría de seguridad de la información estuvo dirigido a la gerencia, a la encargada del departamento de Administración y al asistente administrativo. En estas se abordan temas de importancia para la investigación, tocando puntos como:

- Control de Acceso
- Control y monitoreo de la Tecnologías de la Información
- Copias de Seguridad
- Gestión de la Información
- Manuales y procesos de contingencia
- Políticas de Seguridad
- Infraestructura tecnológica.
- Mantenimientos de equipos informáticos.
- Identificación y categorías de los activos de información.
- Incidentes o eventos de seguridad.
- Concientización en temas de seguridad de la información.
- Conocimiento acerca de tema de seguridad informática y de la información.

Los cuestionarios de control fueron diseñados para evaluar cada uno de los dominios, representados en forma de pregunta. Los mismos, permitieron tener una apreciación más clara de las vulnerabilidades que presenta el área auditada; facilitando así el análisis y dictamen de resultados, pudiendo obtener los niveles de riesgo por cada dominio.

De esta forma, los cuestionarios de control cuantitativo permiten dar una calificación numérica a un requerimiento dentro de los procesos que se estén auditando para determinar su nivel de vulnerabilidad. El puntaje de los procesos a auditar se mide en una escala de 1 a 5; donde 1 significa que no se requiere intervención inmediata para controlar el suceso y el 5 es catalogado como estado crítico que requiere corrección inmediata. Como último paso, se suma el puntaje obtenido de las encuestas dicotómicas.

El cálculo del porcentaje de riesgo, se realiza aplicando las siguientes fórmulas matemáticas:

- $Porcentaje\ de\ riesgo\ parcial$ = ($Total\ SI$∗100) $Total$
- $Porcentaje\ de\ riesgo$ = 100 – $porcentaje\ de\ riesgo\ parcial$

Una vez obtenido el porcentaje de riesgo, se va a tomar en cuenta la siguiente escala para determinar el riesgo total:

- Riesgo Bajo = 1% - 30%

- Riesgo medio = 31% -70%
- Riesgo alto = 71% - 100%

4.3.1 Evaluación y Gestión de los Riesgos

El nivel de riesgo es una estimación de lo que puede ocurrir y se valora de forma cuantitativa, como el producto del impacto, asociado a un suceso, por la probabilidad de la misma. En esta técnica, se realiza el cálculo para obtener el riesgo según las debilidades encontradas en el cuestionario de control.

Para obtener el riesgo, se debe utilizar la siguiente formula:

$$Riesgo = Impacto * Probabilidad$$

Al explicar la fórmula anterior, podemos definir el impacto, el cual viene dado como la consecuencia que puede causar la amenaza en caso de materializarse y, por otro lado, la probabilidad, es la posibilidad que existe de que la amenaza se presente, al tener los dos términos anteriores, se puede decir que el riesgo que se está calculando, se refiere a la probabilidad de que un evento se materialice y tenga un impacto negativo.

Para determinar la probabilidad y el impacto, se utilizó una escala numérica del 1 al 5, como lo determina la metodología MAGERIT v3.0, como se muestra a continuación:

IMPACTO	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

PROBABILIDAD	
1	Muy Raro
2	Poco Probable
3	Posible
4	Probable
5	Muy Probable

Tabla 8. Escalas para Análisis de Riesgos.
Fuente: MAGERIT V3.0

Una vez otorgada una puntuación a cada debilidad, de acuerdo con la escala de impacto y probabilidad, se procede a hacer uso de la fórmula de riesgo mencionada

anteriormente, la cual permitirá generar una matriz de riesgo donde se puede apreciar la ubicación de cada una de las vulnerabilidades, según su impacto y probabilidad.

A continuación, se mostrará la matriz que se utilizará en el presente trabajo:

MATRIZ DE RIESGO		PROBABILIDAD				
		1	2	3	4	5
IMPACTO	5					
	4					
	3					
	2					
	1					

Tabla 9. Modelo Matriz de Riesgo.
Fuente: Elaboración Propia, 2022.

Los colores que se pueden apreciar en la matriz de riesgo, corresponden a los Niveles de Aceptabilidad de Riesgos, estos niveles fueron clasificados de la siguiente manera:

Nivel	Aceptabilidad
Extremo	No Aceptable. Ya que por su nivel de probabilidad de ocurrencia e impacto entra en una escala donde se le tiene que dar atención inmediata, ya sea para evitar, prevenir o mitigar el daño en la empresa.
Alto	
Moderado	
Bajo	Aceptable, el riesgo puede ser asumido por la empresa.

Tabla 10. Nivel de Aceptabilidad del Riesgo.
Fuente: Elaboración Propia, 2022.

4.3.2 Evaluación de dominios

A.5 Políticas de seguridad de la información

Para el primer dominio seleccionado, se evalúan los siguientes subdominios:

- A5.1.1. Políticas para la Seguridad de la Información.
- A5.1.2. Revisión de las Políticas para la Seguridad de la Información.

Al evaluar el Dominio A.5 se presentaron una serie de inconvenientes debido a que la empresa carecía de ciertas políticas indispensables para la aplicación de cuestionarios de control. Los ítems planteados para verificación no aplicaron por la razón anteriormente expuesta. Por lo tanto, no se pudo realizar una evaluación de riesgos en el presente dominio, por falta de la documentación que debía ser cotejada.

Dominio A6. Aspectos Organizativos de la Seguridad de la Información

Se procedió a evaluar el dominio a A6 Organización de la Seguridad de la Información del cual se tomaron los siguientes subdominios:

- A.6.1 Organización interna:
    - A.6.1.1 Roles y responsabilidades en seguridad de la información
    - A.6.1.4 Revisión de las políticas para la seguridad de la información

A continuación, se reflejan los resultados obtenidos de los ítems evaluados mediante el cuestionario CC-A6 y la sumatoria de los puntajes del mismo. Los puntajes obtenidos fueron:

Si=9

No=12

Total=21

Con los resultados obtenidos se da paso a la obtención del porcentaje de riesgo:

Porcentaje Parcial de Riesgo=42,86 %

Porcentaje de Riesgo=57,14 %

Desde una perspectiva general, el Dominio A6. “Aspectos Organizativos de la Seguridad de la Información” se sitúa en un nivel de riesgo Medio, por la ausencia de controles y por el impacto que genera la materialización de las amenazas.

En base a las vulnerabilidades encontradas, se realiza una valoración de las consecuencias que podrían generar las vulnerabilidades y las probabilidades de que el evento ocurra.

Al evaluar el subdominio mencionando anteriormente, se encontraron vulnerabilidades como:

- Carencia de controles de seguridad para el manejo adecuado
- No se le da énfasis al tema de seguridad y al riesgo de la información, por lo que el conocimiento de este tema es escaso.
- Se carece de conocimiento entorno a la seguridad de la información y al impacto que podría tener la materialización de las amenazas.

Ref.	VULNERABILIDADES	IMPACTO	PROBABILIDAD	RIESGO
V001	Carencia de controles de seguridad para el manejo adecuado	4	4	**16**
V002	No se le da énfasis al tema de seguridad y al riesgo de la información, por lo que el conocimiento de este tema es escaso.	5	4	**20**
V003	Se carece de conocimiento entorno a la seguridad de la información y al impacto que podría tener la materialización de las amenazas	3	3	**9**

Tabla 11. Análisis de Riesgos en el Dominio A6.
Fuente: Elaboración Propia, 2022.

Los resultados obtenidos en el cálculo de riesgos del Dominio A.6 se encuentran relacionados a la ausencia de las Políticas de Seguridad de la Información. Como resultado de los acontecimientos anteriores, se representan de forma gráfica las vulnerabilidades encontradas a través de la matriz de riesgo.

MATRIZ DE RIESGO		PROBABILIDAD				
		1	2	3	4	5
IMPACTO	5				V002	
	4				V001	
	3			V003		
	2					
	1					

Tabla 12. Matriz de Riesgo para el Dominio A6.
Fuente: Elaboración Propia, 2022.

En virtud de las vulnerabilidades evaluadas en el Dominio A6. “Aspectos Organizativos para la Seguridad de la Información” se clasifica como extremo o inadmisible al riesgo V002, el cual debe ser intervenido de forma inmediata. Por otra parte, tenemos en el nivel medio el riesgo V001 y, por último, en el nivel moderado al riesgo V003. Los riesgos anteriormente mencionados requieren ser intervenidos para llevarlos al nivel de aceptabilidad mínimo.

Dominio A8. Gestión de Activos

Siguiendo con la evaluación de dominios, se tomaron en cuenta los subdominios:

- A.8.1 Responsabilidad sobre los activos:
  - *A.8.1.1 Inventario de activos*
  - *A.8.1.3 Uso aceptable de los activos*

La ejecución de este dominio permitió valorar la Gestión de Activos, así como también la aplicación de modelos para el manejo de la información existente en la empresa. La evaluación de los ítems establecidos en el cuestionario de control CC-A8 dio como resultados:

Si= 7

No= 11

Total= 18

Una vez obtenidos los resultados del cuestionario de control CC-A8, se procede a llevar a cabo las fórmulas para determinar el Porcentaje Riesgo Parcial y el Porcentaje de Riesgo, teniendo como resultado que:

Porcentaje Parcial de Riesgo= 38,89 %

Porcentaje de Riesgo= 61,11 %

Una vez obtenidos los resultados, se determinó que el dominio A8. Gestión de Activos, se encuentra en un Riesgo Medio en relación a la situación evaluada. Es por ello, que se procede a definir las vulnerabilidades encontradas con la aplicación de los cuestionarios de control CC-A8:

- Falta de conocimientos técnicos para la gestión adecuada de equipos donde se procese la información.
- Carencias de criterios para la clasificación y manejo de la información. Por consiguiente, los departamentos no cuentan con una manual para la clasificación de la información que les permita determinar si la información es de carácter confidencial o de uso interno.
- Insuficiencia de gestión periódica a los inventarios que posee la empresa.
- No se efectúan copias de seguridad de la información.
- No se llevan a cabo los debidos procedimientos para el manejo de la información.
- Ausencia de normativas que garanticen el buen uso de los equipos para la seguridad de la información.

Como resultado de las vulnerabilidades encontradas, se realiza una valoración de las consecuencias que podrían generar y las probabilidades de que el evento ocurra.

Ref.	VULNERABILIDADES	IMPACTO	PROBABILIDAD	RIESGO

V004	Falta de conocimientos técnicos para la gestión adecuada de equipos donde se procese la información.	4	3	**12**
V005	Carencias de criterios para la clasificación y manejo de la información. Por consiguiente, los departamentos no cuentan con una manual para la clasificación de la información que les permita determinar si la información es de carácter confidencial o de uso interno.	5	4	**20**
V006	Insuficiencia de gestión periódica a los inventarios que posee la empresa	4	4	**16**
V007	No se efectúan copias de seguridad de la información.	5	5	**25**

V008	No se llevan a cabo los debidos procedimientos para el manejo de la información.	3	3	**9**
V009	Ausencia de normativas que garanticen el buen uso de los equipos para la seguridad de la información.	4	4	

Tabla 13. Análisis de Riesgos en el Dominio A8.
Fuente: Elaboración Propia, 2022.

Los resultados obtenidos en el cálculo de riesgos son trasladados a una matriz, con el objetivo de representar de forma gráfica la ubicación de las vulnerabilidades y la clasificación de las mismas. De este modo se facilita su comprensión.

MATRIZ DE RIESGO		**PROBABILIDAD**				
		1	**2**	**3**	**4**	**5**
IMPACTO	**5**				**V005**	**V007**
	4			**V004**	**V006 V009**	
	3			**V008**		
	2					
	1					

Tabla 14. Matriz de Riesgo para el Dominio A8.
Fuente: Elaboración Propia, 2022.

Luego de representar los resultados mediante la matriz de riesgo, se ha determinado que el que posee mayor criticidad es el V007 y V005, sobre el cual se deben aplicar controles inmediatos para erradicarlos. Sucesivamente tenemos que, las vulnerabilidades V004, V006 y V009 se encuentran en un nivel intermedio, que requieren implementación de controles a corto plazo para llevarlas a un nivel aceptable. Por último, tenemos la vulnerabilidad V008 en un nivel bajo o de riesgos asumibles.

Dominio A9. Control De Accesos

Para la evaluación del Dominio A9. Control de Accesos, se analizan los subdominios:

- A9.1. Requisitos de Negocio para el Control de Accesos.
    - A9.1.1. Política de Control de Accesos.
- A9.2 Gestión de acceso de usuario.
    - A.9.2.4 Gestión de la información secreta de autenticación de los usuarios

Por consiguiente, se presentan los resultados obtenidos de los ítems evaluados mediante el cuestionario CC-A9, el cual mide el control de acceso; dando como resultado:

Si= 6

No= 15

Total= 21

Arrojó como resultado del porcentaje de riesgo:

Porcentaje Parcial de Riesgo= 28,57%

Porcentaje de Riesgo= 71,43%

En función de los valores obtenidos, se puede definir que el Dominio A9. “Control de Accesos” se sitúa en un nivel de riesgo bajo con referencia al impacto que tendría la materialización de las amenazas.

Al ser evaluados los subdominios anteriormente mencionados, se tuvo como resultado que la empresa presenta una serie de vulnerabilidades, tales como:

- No existen políticas que establezcan el debido control de accesos a los equipos informáticos ni a la información que se manejan en los distintos departamentos que conforman la empresa, tales como: facturas, datos de clientes y proveedores, estados de cuentas, entre otros.
- El área donde se almacena la información no cuenta con la seguridad física necesaria, ya que esta se encuentra expuesta a factores que quieran atentar contra su integridad.
- No se desarrollan acciones de monitoreo y control ante posibles vulnerabilidades técnicas de los sistemas de información, que permitan darle el trato adecuado a los riesgos surgentes.

Ya establecidas las vulnerabilidades, se procede a realizar la valoración de las consecuencias que podrían generar y las probabilidades de que el evento pueda materializarse.

Ref.	VULNERABILIDADES	IMPACTO	PROBABILIDAD	RIESGO
V010	No existen políticas que establezcan el debido control de accesos a los equipos informáticos ni a la información que se manejan en los distintos departamentos que conforman la empresa tales como, facturas, datos de cliente y proveedores, estados de cuentas, entre otros.	4	5	**20**
V011	El área donde se almacena la información no cuenta con la seguridad física necesaria, ya que la información se encuentra expuesta a factores que quieran atentar contra su integridad.	5	5	**25**
V012	No se desarrollan acciones de monitoreo y control ante posibles vulnerabilidades técnicas de los sistemas de información, que permitan darle el trato adecuado a los riesgos surgente.	4	3	**12**

Tabla 15. Análisis de Riesgos en el Dominio A9.
Fuente: Elaboración Propia, 2022.

Los resultados obtenidos en el cálculo de riesgos son trasladados a una matriz, con el objetivo de representar de forma gráfica la ubicación de las vulnerabilidades y la clasificación de las mismas.

MATRIZ DE RIESGO		PROBABILIDAD				
		1	2	3	4	5
IMPACTO	5				V010	V011
	4			V012		
	3					
	2					
	1					

Tabla 16. Matriz de Riesgos para el Dominio A9.
Fuente: Elaboración Propia, 2022.

De acuerdo con la matriz de riesgo se clasifica a la vulnerabilidad V010 y V011 en un nivel de impacto extremo, esto demuestra el grado de importancia que se le debe de dar a la misma debido al impacto que podría generar a la empresa, de esta forma, es prudente la aplicación de medidas a corto plazo y así evitar que se materialicen. Por otro lado, se tiene la vulnerabilidad V012 como un riesgo alto, el cual debe ser controlado para evitar pérdidas o daño de la información.

Dominio A11. Seguridad Física y del Entorno

Para la evaluación del Dominio A11. que engloba la Seguridad Física y del Entorno, se tomaron los siguientes subdominios:

- A.11.1 Requisitos de negocio para el control de acceso
  - A11.1.1 Perímetros de seguridad física
  - A.11.1.2 Controles físicos de entrada
  - A11.1.4 Protección contra las amenazas externas y ambientales
- A11.2 Seguridad de los equipos
  - A11.2.1 Emplazamiento y protección de equipos
  - A11.2.2 Instalaciones de suministros
  - A11.2.4 Mantenimiento de los equipos

- A11.2.9 Política de puesto de trabajo despejado y pantalla limpia

La aplicación de este dominio permitió evaluar la Seguridad Física y del Entorno, de la misma forma la implementación de medidas y protocolos para el manejo de estas. Una vez obtenidos los resultados por cada ítem evaluado en el cuestionario de control CC-A11, se tiene que:

Si= 28

No= 29

Total= 57

En efecto, se procede a aplicar las fórmulas para conocer el Porcentaje Riesgo Parcial y el Porcentaje de Riesgo, el cual tuvo como resultado:

Porcentaje Parcial de Riesgo= 49,12%

Porcentaje de Riesgo= 50,88%

De esta manera, se determinó que el dominio A11. Seguridad Física y del Entorno, se encuentra en un Riesgo Medio en relación a la situación evaluada; dando como resultado, un conjunto de vulnerabilidades arrojadas mediante los cuestionarios de control CC-A11:

- No existe una adecuada gestión de mantenimientos preventivos y correctivos a los equipos informáticos con los que cuenta la empresa.
- No existen mecanismos internos ni documentación en formato físico o digital para los procedimientos de recuperación ante catástrofes, desastres y eventualidades, tales como: robo, incendio, humo, agua, polvo, interferencia en el suministro eléctrico, interferencia en las comunicaciones y vandalismo.
- Las pantallas de los equipos de trabajo donde se maneja información susceptible, no están ubicadas o protegidas para evitar la visualización no autorizada.
- No existen normas para el uso de los equipos y medios electrónicos.
- No se establecen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas de claves o cualquier otra información de carácter confidencial.

- Falta de formación y conciencia sobre la seguridad de la información.
- No están definidos espacios físicos que cuenten con los niveles de seguridad necesarios para el área de equipos, estaciones de trabajos, repositorios y almacenamientos.

Definidas las vulnerabilidades, se procede a realizar la valoración del impacto por la probabilidad, en relación a sus probabilidades de materializarse. Por ello, se efectúa el análisis de riesgo por cada una de las vulnerabilidades:

Ref.	VULNERABILIDADES	IMPACTO	PROBABILIDAD	RIESGO
V013	No existe una adecuada gestión de mantenimientos preventivos y correctivos a los equipos informáticos con los que cuenta la empresa.	3	3	**9**
V014	No existen mecanismos internos ni documentación en formato físico o digital para los procedimientos de recuperación ante catástrofes, desastres y eventualidades tales como robo, incendio, humo, agua, polvo, interferencia en el suministro eléctrico, interferencia en las comunicaciones y vandalismo.	4	4	**16**

V015	Las pantallas de los equipos de trabajo donde se maneja información susceptible, no están ubicados o protegidos para evitar la visualización no autorizada.	4	3	**12**
V016	No existen normas para el uso de los equipos y medios electrónicos.	3	4	**12**
V017	No se establecen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas de claves o cualquier otra información de carácter confidencial.	4	4	**16**
V018	Falta de formación y conciencia sobre la seguridad de la información.	4	3	**12**
V019	No están definidos espacios físicos que cuenten con los niveles de seguridad necesaria para el área de equipos, estaciones de trabajos, repositorios y almacenamientos.	5	4	**20**

Tabla 17. Análisis de Riesgo Dominio A11.
Fuente: Elaboración Propia 2022.

Siguiendo con el análisis del dominio, se procede a trasladar todos los resultados obtenidos en el cálculo de riesgos a una matriz para, de esta forma, observar gráficamente los resultados obtenidos para el Dominio A11. Seguridad Física y del Entorno.

MATRIZ DE RIESGO		PROBABILIDAD				
		1	2	3	4	5
IMPACTO	5				V019	
	4			V015 V018	V014 V017	
	3			V013	V016	
	2					
	1					

Tabla 18. Matriz de Riesgo para el Dominio A11.
Fuente: Elaboración Propia 2022.

En conformidad con los resultados obtenidos de la matriz de riesgo, se aprecia que la vulnerabilidad V019 está en un nivel de riesgo extremo, al cual se deben aplicar controles de forma inmediata que incluyan recomendaciones adaptadas a la dimensión de la problemática y del área auditada. Por otra parte, las vulnerabilidades V014, V015, V016, V017 y V018 se catalogan como riesgo alto, es por ende que se recomienda la ejecución de medidas a corto plazo una vez atacada la vulnerabilidad crítica. Por último, se tiene la vulnerabilidad V013, la cual se encuentra en un riesgo bajo y deben aplicarse medidas correctivas.

Dominio A12. Seguridad de Operaciones

Para el análisis del Dominio a A12. Seguridad de las Operaciones, se toman en cuenta los subdominios mencionados a continuación:

- A12.2 Protección contra el software malicioso (malware)
    - A12.2.1 Controles contra el código malicioso
- A12.3 Copias de seguridad
    - A12.3.1 Copias de seguridad de la información

A continuación, se muestran los resultados obtenidos de los ítems evaluados mediante el cuestionario CC-A12 y la sumatoria de los puntajes del mismo, los cuales fueron:

Si= 26

No= 7

Total= 33

Con los resultados obtenidos se da paso a la obtención del porcentaje de riesgo:

Porcentaje Parcial de Riesgo= 78,79%

Porcentaje de Riesgo= 21,21 %

Ya obtenidos los porcentajes de riesgos del Dominio A12. Seguridad de la Operaciones, se sitúa en un nivel de riesgo Medio; esto se debe a la ausencia de controles y normativas que garanticen la seguridad de las operaciones. Por consiguiente, se procede a nombrar las vulnerabilidades encontradas con la aplicación de los cuestionarios de control CC-A12

- No se cuenta con políticas ni procedimientos asociados a controles de riesgos informáticos (malware, ciberataques, robo de información).
- No se establecen políticas asociadas a copias de seguridad de información y software de forma periódica.
- No existe un conocimiento apropiado referente a la detección, evaluación y mitigación de riesgos informáticos.
- No se verifica el estado de los sistemas operativos.
- No existen políticas ni procedimientos que enmarquen controles asociados a la aplicación antimalware para salvaguardar la información.
- No existe documentación de antecedentes de ataques y riesgos, que sirvan como precedente para futuros casos.

A continuación, se efectúa el análisis de riesgo en relación con el dominio A12. Seguridad de las Operaciones, por cada una de las vulnerabilidades encontradas:

Ref.	VULNERABILIDADES	IMPACTO	PROBABILIDAD	RIESGO

V020	No se cuenta con políticas ni procedimientos asociados a controles de riesgos informáticos (malware, ciberataques, robo de información).	4	4	**16**
V021	No se establecen políticas asociados a copias de seguridad de información y software de forma periódica.	5	4	**20**
V022	No existe un conocimiento apropiado referente a la detección, evaluación y mitigación de riesgos informáticos	3	3	**9**
V023	No se verifica el estado de los sistemas operativos.	4	3	**12**
V024	No existen políticas ni procedimientos que enmarquen controles asociados a la aplicación antimalware para salvaguardar la información.	3	4	**12**
V025	No existe documentación de antecedentes de ataques y riesgos, que sirvan como precedente para futuros casos.	2	3	**6**

Tabla 19. Análisis de Riesgos en el Dominio A12.
Fuente: Elaboración Propia, 2022.

Ya obtenidos los resultados en el cálculo de riesgos son trasladados a una matriz, con el objetivo de representar de forma gráfica.

MATRIZ DE RIESGO		PROBABILIDAD				
		1	2	3	4	5
IMPACTO	5				V021	
	4			V023	V020	
	3			V022	V024	
	2			V025		
	1					

Tabla 20. Matriz de Riesgos para el Dominio A12.
Fuente: Elaboración Propia, 2022.

Conforme a los resultados obtenidos mediante la matriz de riesgo y evaluaciones anteriores, se determina que el riesgo con mayor criticidad es el V021, sobre el cual se deben implementar controles inmediatos para eliminarlo. Además, se encuentran las vulnerabilidades V020, V023 y V024, clasificadas como un riesgo de nivel alto, que requieren de la aplicación de controles a corto plazo para llevarlas a un nivel aceptable. Y por último tenemos en niveles bajos o de riesgos asumibles a las vulnerabilidades V022 y V025.

4.4 Elaboración del informe final de auditoría con las recomendaciones para el mejoramiento de la gestión de la información de la empresa Mundo Shop C.A

Una vez establecidos los criterios para la evaluación de la auditoría, se procedió a realizar los distintos análisis preliminares, los cuales sirvieron para la elección de las normativas internacionales que se adapten al área auditada, es por ello que se eligió la ISO/IEC 27001, la cual tiene como finalidad, realizar una valoración de los riesgos. De esta manera, se determinaron los controles que se deben aplicar, las medidas y acciones a mejorar, y los procedimientos que hay que cumplir. De igual forma, se encuentra la ISO/IEC 27002, que se encarga de las buenas prácticas para la gestión de la seguridad de la información, describiendo cómo se pueden establecer los controles con la finalidad de garantizar la vigencia y el mantenimiento de los procesos de seguridad.

Esto nos permitió tener unos lineamientos y parámetros a seguir para medir los riesgos y vulnerabilidades existentes dentro del área auditada, ya que en la empresa no se cuenta con un control necesario para el manejo de la información, poniendo en riesgo la integridad de la organización en general; al no existir ningún tipo de parámetro en cuanto al manejo de la información, gestión de activos, control de acceso, planes de contingencia en cuanto a catástrofes o planes de resguardo de la información como ciclos de copias de seguridad. Es por ello que estas distintas situaciones y vulnerabilidades ponen en riesgo la permanencia de la información, ya que no se le da el debido cuidado. Así mismo, estos lineamientos y parámetros sirven como línea de partida para formular las recomendaciones de los cambios y medidas con los que se mejoraría la gestión de la seguridad de la información.

Este punto viene dado por los análisis preliminares que se han realizado mediante la revisión documental apoyada en el instrumento del bloc de notas, la cual permite formular las recomendaciones más convenientes. Además, si se considera su implementación, ayudaría a la empresa con la gestión de los procesos que involucra la información.

En conformidad con los resultados obtenidos dadas las evaluaciones realizadas, se procede a emitir las recomendaciones pertinentes por cada dominio, lo cual funcionará como mecanismo para la mejora de los procesos de gestión de los activos de información.

Dominio A5. "Políticas de Seguridad de la Información":

Para el dominio A5. "Políticas de Seguridad de la Información" se generaron las siguientes recomendaciones:

- Definir objetivos que involucren la seguridad de la información, priorizando, la data sensible en relación a las estaciones de trabajo.
- Elaborar un manual de Políticas de Seguridad de la información, donde se detallen los controles implementados en la empresa Mundo Shop C.A., incluyendo los nuevos controles de seguridad acorde a las necesidades emergentes. El manual de Políticas de seguridad de la información debe contemplar los siguientes aspectos:

- Ámbitos de Aplicación.
- Objetivos.
- Alcances.
- Asignación de Roles.
- Clasificación y control de los activos informáticos.
- Gestión de Accesos.
- Seguridad física y del entorno.
- Identificación, Revisión y Mantenimiento de Equipos.
- Copias de Seguridad y recuperación de la información.
- Eliminación de Programas maliciosos.

- Participar al personal de las políticas y cambios significativos para su adecuación, eficacia y cumplimiento.
- Establecer métodos de contingencia que contemplen las normas, procedimientos y acciones básicas de respuestas oportunas, adecuadas y efectivas ante eventualidades que se puedan suscitar en la empresa Mundo Shop C.A., siendo este un mecanismo para garantizar la continuidad de las funciones en la empresa.

Dominio A6. "Organización de la Seguridad de la Información":

Una vez valorada la situación de la empresa con respecto a este dominio que engloba la "Organización de la Seguridad de la Información", se recomienda instituir los roles y responsabilidades en cuanto a la seguridad e integridad de la información. Es por ello que se emiten las siguientes recomendaciones:

- Implantar medidas y responsabilidades con respecto al uso indebido de los activos de la empresa.

- Establecer políticas o normativas sobre el uso de los recursos tecnológicos con los que cuenta la empresa, tales como equipos de cómputos y la utilización de dispositivos personales.
- Instaurar la aplicación de un documento de categorización de la información de la empresa Mundo Shop C.A., el mismo estará constituido por:
    - Niveles de Información
    - Medidas de Control de la Información por Nivel
    - Riesgo en cuanto al manejo de la información por labor desempeñada por el personal.
- Precisar los mecanismos con respecto al uso de copias de seguridad y recuperación de la información, este debe indicar el contenido del respaldo y la clasificación de la información almacenada, puesto que las categorías de clasificación de la información serían: la información pública, la información reservada e información clasificada.

Dominio A8. "Gestión de Activos":

Para el dominio A8. "Gestión de Activos" se emitieron las siguientes recomendaciones:

- Implementar inventarios que contengan el registro de los equipos y licencias de propiedad de la empresa.
- Crear cronogramas para la actualización de inventarios, que contemplen los registros de reemplazo de equipos y las razones por las que fue reemplazado, para tener un control de la no usabilidad de los equipos y evitar el reemplazo injustificado de aquellos que podrían seguir siendo utilizados.
- Clasificar la información en función del valor, criticidad y susceptibilidad a modificaciones no autorizadas.
- Proteger los sistemas o medios que contienen información contra accesos no autorizados.
- Elaborar un documento que contenga las políticas sobre el uso de los recursos tecnológicos del departamento, así como también el uso de correos corporativos y el manejo de la información.

- Implementar mecanismos para la realización de copias de seguridad donde se plasmen el responsable de desarrollar este proceso y los criterios mínimos para su realización.
- Verificar el cumplimiento de la realización de las copias de seguridad, para evitar la aparición de problemas o errores que pongan en riesgo la integridad de la empresa
- Implementar mecanismos para el monitoreo del uso del internet.

Dominio A9. "Control de Accesos":

Siguiendo con el establecimiento de las recomendaciones, tenemos para el dominio A9. "Control de Acceso" las siguientes:

- Establecer una política de control de accesos a los equipos informáticos y a la información, en base a los requerimientos de seguridad por parte de la empresa.
- Implementar controles de uso de contraseñas que contemplen su usabilidad, asignación y periodo de vigencia.
- Establecer controles internos para el monitoreo del acceso a las tecnologías de la información por parte de empleados y la manera en la que estos le dan uso a la información.

Dominio A11. "Seguridad Física y del Entorno":

La ejecución de modelos que garanticen la seguridad e integridad física y del entorno de la empresa, es catalogada pieza fundamental, debido al impacto que generaría si las amenazas llegaran a materializarse, dificultando así el desarrollo de las laborales cotidianas de la empresa y afectando de esta manera la continuidad de sus operaciones. Por los motivos anteriormente mencionados, se realizan las siguientes recomendaciones:

- Instaurar cronogramas de revisiones periódicas de las condiciones del entorno y del ambiente de las áreas de procesamiento de información; para prevenir cualquier eventualidad, en caso de que suceda alguna incidencia.

- Crear procesos internos y documentación en formato físico o digital para los procedimientos a seguir para la recuperación ante catástrofes, eventualidades y desastres naturales.
- Revisar periódicamente el estado del cableado, realizar su identificación y documentación correspondiente.
- Establecer políticas para la ejecución de mantenimientos preventivos y de control de los equipos de cómputos utilizados en la empresa, con el fin de optimizar los recursos y prevenir fallos.
- Implantar controles para la protección de los equipos enviados fuera de las instalaciones de la empresa y que poseen información susceptible, con el fin de delimitar el riesgo que conlleva esta acción.
- Identificar y documentar controles que permitan monitorizar, controlar, planificar y coordinar los equipos tecnológicos que se usan en la empresa para llevar a cabo las labores diarias.

Dominio A12. "Seguridad de las Operaciones":

Para el dominio A12. "Seguridad de las Operaciones", se emitieron las siguientes recomendaciones:

- Capacitar al personal en relación a la seguridad de la información sobre cómo actuar ante una incidencia y la ejecución de copias de seguridad, con el fin de que se adquiera conciencia de la misma.
- Establecer políticas y procedimientos que abarquen controles ante riesgos informáticos.
- Implementar controles periódicos de revisión de antivirus en todos los dispositivos con los que cuenta la empresa, tales como servidores, portátiles y ordenadores de escritorio.
- Implantar cronogramas de revisión de la información que se gestiona mediante las copias de seguridad, para evitar duplicidad de información, archivos dañados o ausencia de los mismos.

- Almacenar copias de seguridad en ubicaciones adecuadas, protegidas contra desastres físicos y acceso indebido.
- Documentar antecedentes de ataques y riesgos suscitados en el área, para que sirvan como precedente para la toma de acciones rápida y apropiada para minimizar efectos de futuros casos.

PARTE V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

5.1.1 Conclusiones de los objetivos

La puesta en práctica de una auditoría de la seguridad de la información desarrollada en la empresa Mundo Shop C.A., permitió evaluar la validación de cada uno de los procedimientos que involucran el manejo de información; cerciorándose del cumplimiento de regulaciones adaptadas al área de trabajo. En efecto, se logró determinar el estado en el que se encontraba la organización en cuanto a los aspectos de seguridad de la información y así dictar las recomendaciones pertinentes cumpliendo con los estándares de integridad, confiabilidad y disponibilidad de los procesos que se llevan a cabo diariamente dentro de la misma.

De esta manera, para lograr una evaluación óptima mediante una auditoría de la seguridad de la información, se siguieron una serie de parámetros que fundamentan el desarrollo de la misma. Los hallazgos obtenidos, fueron como resultado de la aplicación de cuestionarios de control, las cual se consideró como la herramienta más apropiada para la recolección de información que muestran las deficiencias en cuanto a la seguridad de la información. El estándar ISO 27001, fue el idóneo para evaluar la seguridad de la información, ya que el mismo plantea dominios que se adaptan al área auditada, siendo este proyecto, dirigido a la parte de seguridad de los sistemas informáticos. En este sentido, mediante la aplicación de análisis de riesgo a cada dominio evaluado, se obtuvieron las amenazas y vulnerabilidades que presentaban la empresa y cuál es la probabilidad de que estas se materialicen, y cuál sería el nivel de impacto que ocasionaría.

Por otro lado, una vez obtenidas las deficiencias como resultado de la auditoría realizada, se puede decir que, fue factible lograr el trabajo planteado mediante la evaluación y recomendaciones ante las vulnerabilidades encontradas. Las recomendaciones que se plantearon en el presente trabajo, permitirán mejorar de una

manera eficiente y confiable la calidad de los servicios que se brindan y la seguridad de los mismos.

En efecto, una vez obtenidos todos los resultados se procedió a identificar en qué nivel de madurez organizacional se encuentra la empresa Mundo Shop C.A. con respecto al uso a las normativas ISO, teniendo como resultado que la empresa se encuentra en un nivel 0: proceso incompleto, puesto que no está definida ninguna política de seguridad de la información. De esta manera, si se implementan las recomendaciones de esta investigación se obtendrán cambios favorables a largo plazo.

5.1.2 Conclusión general

La puesta en práctica de un trabajo de investigación que involucre la ejecución de una auditoría enfocada en la evaluación de vulnerabilidades y la seguridad de la información en la empresa Mundo Shop C.A., permitió evidenciar las debilidades relacionadas a la ausencia de políticas y normativas con respecto a la seguridad y resguardo de su activo más importante, aunado a la inexistencia de políticas para control de incidentes. Por lo que, se hace indispensable la necesidad de implementar un plan para la prevención y corrección de riesgos que permita la disminución de estos.

Es importante resaltar que el análisis de estos aspectos, sirvió para la detección de amenazas, riesgos y vulnerabilidades que presenta la empresa, además de la inadecuada gestión de los procesos informáticos y deficiencias en el manejo de la información. Lo cual permite la aplicación de mecanismos para la gestión de seguridad de la información, en función de establecer procedimientos y buenas prácticas para el manejo óptimo de las actividades que desarrolla la empresa.

La realización de este proyecto de investigación con enfoque en el desarrollo de una auditoría, permitió tener una apreciación clara del estado actual de los equipos informáticos con los que cuenta la empresa auditada y de esta manera verificar su rendimiento en relación a los fallos y seguridad de los dispositivos, tomando en cuenta los inconvenientes o amenazas que pudieran dificultar el desarrollo de las actividades diarias. Es por ello, que se realizó una inspección de la seguridad de la información, abarcando puntos de procedimientos, controles, seguridad y gestión de datos.

De esta forma podemos concluir, que la ejecución de esta auditoría tuvo como objetivo el dictamen de recomendaciones de control y políticas de seguridad para la gestión de incidentes, que garanticen el buen uso de la información, sirviendo como mecanismo para la mitigación en lo posible de los riesgos que puedan generarse al realizar cualquier tipo de procesos y la manera más conveniente de actuar si se llegaran a presentar.

5.2 Recomendaciones

A continuación, se generan una serie de recomendaciones ordenadas por importancia según porcentaje general de riesgo de cada dominio evaluado, para el cual se obtiene:

5.2.1 Recomendaciones para la empresa Mundo Shop C.A.

En busca de garantizar el buen funcionamiento de los procesos diarios que lleva a cabo la empresa y que la misma no continúe presentando deficiencias en el procesamiento y gestión de la información, es necesario que se implementen las siguientes recomendaciones:

1. Gestión de Incidentes de Seguridad de la Información:
    - Establecer campañas de concientización dirigidas al personal para evitar la reincidencia de eventualidades que se puedan presentar a futuro y así tener unas mejores prácticas de Seguridad de la Información.
2. Seguridad de las Operaciones:
    - Efectuar la realización de copias de seguridad, periódicamente, priorizando la información dependiendo de su clasificación.
    - Garantizar que la información, así como también los recursos tecnológicos, se encuentren actualizados, evitando la aparición de códigos maliciosos que puedan poner en riesgo su integridad.
3. Organización de la Seguridad de la Información:
    - Establecer parámetros que definan el uso indebido de los activos de la organización
4. Gestión de Activos:

- Crear inventarios de forma periódica donde se registren los equipos con los que cuenta la empresa y licencias de propiedad de la empresa.
- Clasificar la información en función del valor, criticidad, susceptibilidad a divulgación o a modificaciones no autorizadas.

5. Seguridad Física y del Entorno:
    - Monitorear y revisar de manera periódica el estado de los componentes de soportes físicos, eléctricos y ambientales, con el fin de prevenir fallas ante cualquier eventualidad.
    - Efectuar mantenimientos preventivos y de control de los equipos de cómputos utilizados por la empresa, con el propósito de optimizar los recursos y prevenir fallos.
6. Control de Accesos:
    - Realizar cambios de forma periódica de claves de acceso para aumentar la seguridad y evitar vulnerabilidades en equipos.
    - Crear parámetros para gestionar contraseñas seguras.
7. Seguridad de la Información:
    - Implementar políticas que abarquen la seguridad de la información aplicables a todos los procesos que ejecuta la empresa; las cuales deben ser aprobadas por la gerencia de la organización y, posterior a ello, publicadas y comunicadas a todos los empleados

Mediante la aplicación de las recomendaciones anteriormente expuestas, se garantiza que la empresa Mundo Shop C.A., tendrá cambios circunstanciales con grandes mejoras en los niveles de eficiencia, productividad y operatividad.

ANEXOS

Cuestionarios de control

EVALUACIÓN AL MANEJO LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA MUNDO SHOP C.A.

Elaborado por:	Br. Angel Gómez	**Referencia**	
Respondido por:		**Fecha**	
CUESTIONARIO DE CONTROL			
Dominio	**A.5 Políticas de seguridad de la información**		
Subdominios	**A.5.1 Directrices de gestión de la seguridad de la información:** - A.5.1.1 Políticas para la seguridad de la información - A.5.1.2 Revisión de las políticas para la seguridad de la información		

La política de seguridad acerca de "Políticas para la seguridad de la información" y "Revisión de las políticas para la seguridad de la información " según la normatividad, tiene las siguientes especificaciones:				
N°	**Pregunta**	**SI**	**NO**	**Observación**
1	¿Existe una definición de los niveles jerárquicos razonablemente diseñado y administrado?			
2	¿Las políticas implementadas están bien definidas y cubren todos los riesgos en cuanto al manejo de la información?			
3	¿Los trabajadores y empleados están formalmente obligados a cumplir estos acuerdos?			
4	¿Están las políticas bien escritas, legible, razonable y viable?			

5	¿Cuán madura es la organización en este aspecto?			

EVALUACIÓN AL MANEJO LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA MUNDO SHOP C.A.

Elaborado por:	Br. Angel Gómez	**Referencia**	
Respondido por:		**Fecha**	

CUESTIONARIO DE CONTROL	
Dominio	**A.6 Controles de seguridad de la información**
Subdominios	**A.6.1 Organización interna:** - A.6.1.1 Roles y responsabilidades en seguridad de la información - A.6.1.4 Revisión de las políticas para la seguridad de la información

La política de seguridad acerca de "Roles y responsabilidades en seguridad de la información" y "Revisión de las políticas para la seguridad de la información " según la normatividad, tiene las siguientes especificaciones:

N°	Pregunta	SI	NO	Observación
1	¿Se le da la debida importancia a la seguridad y al riesgo de la información?			
2	¿Existe un personal encargado de analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad?			
3	¿Posee una definición clara de los roles y las responsabilidades asignados a personas adecuadamente capacitadas?			

4	¿Tiene cada rol responsabilidad específica con respecto al riesgo y a la seguridad de la información?			
5	¿Se participa información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?			
6	¿Se definen y documentan los niveles de autorización dentro de la organización?			
7	¿Posee presupuesto para la aplicación de actividades con respecto a la seguridad de la información?			

EVALUACIÓN AL MANEJO LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA MUNDO SHOP C.A.

Elaborado por:	Br. Angel Gómez	**Referencia**	
Respondido por:		**Fecha**	
CUESTIONARIO DE CONTROL			
Dominio	**A.8 Gestión de activos**		
Subdominios	**A.8.1 Responsabilidad sobre los activos:** - A.8.1.1 Inventario de activos - A.8.1.3 Uso aceptable de los activos		

La política de seguridad acerca de “Inventario de activos”, “Uso aceptable de los activos ", " Gestión de soportes extraíbles ", tiene las siguientes especificaciones:				
N°	**Pregunta**	**SI**	**NO**	**Observación**
1	¿Hay un inventario de activos de la información?			
2	¿Contiene la siguiente información? -Información empresa -Software -Infraestructura -Seguridad física -Equipos electrónicos y características			
3	¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada?			

4	¿Existe una política sobre el uso de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.?			
5	¿Cubre el comportamiento del uso en Internet y en las redes sociales?			
6	¿Se especifica el uso inapropiado?			

EVALUACIÓN AL MANEJO LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA MUNDO SHOP C.A.

Elaborado por:	Br. Angel Gómez	**Referencia**	
Respondido por:		**Fecha**	

CUESTIONARIO DE CONTROL	
Dominio	**A.9 Control de acceso**
Subdominios	**A.9.1 Requisitos del negocio para el control de acceso:** - A.9.1.1 Política de control de acceso **A.9.2 Gestión de acceso de usuarios:** - A.9.2.4 Gestión de la información secreta de autenticación de los usuarios

La política de seguridad acerca de "Control de acceso", tiene las siguientes especificaciones:				
N°	**Pregunta**	**SI**	**NO**	**Observación**
1	¿Posee políticas que establecen el control de acceso?			
2	¿Hacen uso de controles técnicos para el acceso de la información, como longitud mínima de contraseña, reglas de complejidad, contraseñas compartida, entre otros?			
3	¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada?			

4	¿Con frecuencia se revisan si las contraseñas utilizadas don débiles?			
5	¿Se cambian las contraseñas por defecto del fabricante?			
6	¿Se almacenan en forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?			
7	¿Existen controles de accesos definidos?			

EVALUACIÓN AL MANEJO LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA MUNDO SHOP C.A.

Elaborado por:	Br. Angel Gómez	**Referencia**	
Respondido por:		**Fecha**	

CUESTIONARIO DE CONTROL	
Dominio	**A.11 Seguridad física del entorno**
Subdominios	**A.11.1 Requisitos de negocio para el control de acceso:** - A.11.1.1 Perímetro de seguridad física - A.11.1.2 Controles físicos de entrada - A.11.1.4 Protección contra las amenazas externas y ambientales **A.11.2 Seguridad de los equipos** - A.11.2.1 Emplazamiento y protección de equipos - A 11.2.2 Instalaciones de suministro - A 11.2.4 Mantenimiento de los equipos A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia

La política de seguridad acerca de “Perímetro de seguridad física”, “Controles físicos de entrada ", " Protección contra las amenazas externas y ambientales ", “Emplazamiento y protección de equipos ”, “Instalaciones de suministro”, “Seguridad del cableado”, “Mantenimiento de los equipos” y “Política de puesto de trabajo despejado y pantalla limpia” según la normatividad, tiene las siguientes especificaciones:

N°	Pregunta	SI	NO	Observación
1	¿Los equipos destinados para el manejo de la información se encuentran en una zona de riesgo?			

2	¿Están definidos los parámetros de seguridad tales como edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, entre otros?			
3	¿El techo exterior, las paredes el suelo son de construcción solida?			
4	¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado?			
5	¿Se monitorea los puntos de acceso con cámaras?			
6	¿Se cuenta con sistema de detección de intrusos y este ha sido sometido a pruebas?			
7	¿Existen sistemas de protección contra cualquier eventualidad como fuego, humo, inundaciones, rayos, intrusos, vándalos, entre otros?			
8	¿Existe un procedimiento de recuperación de desastre?			
9	¿Existe un registro de todas las entradas y salidas?			
10	¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas?			

11	¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada?			
12	¿Existen controles para minimizar los riesgos de amenazas físicas?			
13	¿Existen pruebas periódicas y después de cambios importantes?			
14	¿Se realiza mantenimiento periódico de los equipos de modo a asegurar la continua disponibilidad e integridad?			
15	¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad.)?			
16	¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas?			
17	¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos?			

18	¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?			
19	¿Existen controles implementados con respecto a que ningún equipo, información y software sea sacado de la organización sin la autorización respectiva?			

EVALUACIÓN AL MANEJO LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA MUNDO SHOP C.A.

Elaborado por:	Br. Angel Gómez	**Referencia**	
Respondido por:		**Fecha**	

CUESTIONARIO DE CONTROL	
Dominio	**A.12 Seguridad de operaciones**
Subdominios	**A.12.2 Protección contra el software malicioso (Malware):** - A.12.2.1 Controles contra el código malicioso **A.12.3 Copias de Seguridad:** - A.12.3.1 Copia de seguridad de la información

La política de seguridad acerca de "Seguridad de la Operaciones", tiene las siguientes especificaciones:				
N°	**Pregunta**	**SI**	**NO**	**Observación**
1	¿Existen políticas y procedimientos asociados a controles antimalware?			
2	¿Se implementan controles de antivirus en todos los dispositivos relevantes, tales como portátiles y ordenadores de escritorio?			
3	¿Se actualiza el software antivirus de forma automática?			

4	¿Se generan alertas accionables tras una detección?			
5	¿Se toma acción de forma rápida y apropiada para minimizar sus efectos?			
6	¿Existe una política acerca de la instalación de software?			
7	¿Existen políticas y procedimientos asociados a las copias de seguridad?			
8	¿Las copias de seguridad cubren los datos relevantes de la empresa, tales como datos, sistemas y programas de aplicación?			
9	¿Los medios de respaldo están físicamente protegidos y asegurados?			
10	¿Las copias de seguridad se almacenan en lugares protegidos contra desastres físicos y accesos indebidos?			
11	¿Existen acuerdos de confidencialidad, integridad y disponibilidad?			

REFERENCIAS

Ambit-bts (2021). *¿Qué es una auditoria de seguridad informática? Tipos y Fases*. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases#:~:text=Una%20auditor%C3%ADa%20de%20seguridad%20inform%C3%A1ti,pol%C3%ADticas%20de%20seguridad%20se%20cumplen.

Arias, F. (2006). El Proyecto de Investigación. Introducción a la metodología científica. (6ª Edición). Caracas: Editorial Episteme.

Balestrini, M. (2006). Como se elabora el proyecto de Investigación. Recuperado el 16 de marzo de 2021, de: https://issuu.com/sonia_duarte/docs/como-se-elabora-el-proyecto-de-inve

Bembibre, V. (2009). *Definición de análisis.* Definicionabc. Recuperado 03 de marzo de 2022, de https://www.definicionabc.com/ciencia/analisis.php

Borbón, J (2018). *Buenas prácticas, Estándares y Normas*. Recuperado 27 de febrero de 2022, de https://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas#:~:text=Pues%20bien%2C%20un%20est%C3%A1ndar%20es,cumplir%20una%20actividad%20o%20procedimientos.

Casas, F. (2017). *Contingencia Informática*. Slideshare. Recuperado 06 de marzo de 2022, de https://es.slideshare.net/Indiana_1969/contingencia-informatica#:~:text=Es%20la%20incertidumbre%20existente%20por,Instalaciones%20Programas%20de%20computo%2C%20etc.

Chávez, N. (2007), *Introducción a la Investigación Educativa.* (3 ª edición). Maracaibo.

Cole, B. (2021). *Programa de Auditoria o plan de auditoría*. Recuperado 09 de febrero de 2022, de https://www.computerweekly.com/es/definicion/Programa-de-auditoria-o-plan-de-auditoria

Concepto.de (2020). *Norma,* Definicion.de*.* Recuperado 22 de febrero de 2022, de https://concepto.de/que-es-norma/

DocuSing.com, (2021). *Disponibilidad de la información: ¿Por qué es importante contar con opciones seguras?.* Recuperado 15 de marzo de 2022, de https://www.docusign.mx/blog/disponibilidad-de-la-informacion

Donoso, F. y Ramírez, P., (2006). *Descripción, funcionamiento y aplicaciones.* Recuperado 23 de junio de 2022, de https://repositorio.uchile.cl/handle/2250/108405

Fabián, L. (2020). *ISO/IEC 27001. Todos los tipos de auditoría*. Disponible en: https://eladminis.com/todos-los-tipos-de-auditoria/

Feher, F. (2017). *Importancia de estandarizar operaciones en tu empresa.* Recuperado 28 de enero de 2022, de https://www.google.com/amp/s/salesup.com/crm-online/amp/cc-importancia-de-estandarizar-operaciones-en-tu-empresa.html

Fernández, L. (2020). *Triangulo CIA: conceptos fundamentales para la seguridad informática*. Recuperado 24 de marzo de 2022, de https://www.google.com/amp/s/www.redeszone.net/tutoriales/seguridad/triangulo-cia-seguridad-informatica/amp/

Franklin, E. (2007). *Auditoria administrativa*. Gestión estratégica del cambio. (2ª edición).

García, F. (1993). *La encuesta*. Recuperado el 30 de marzo de 2021, de: http://metodos-comunicacion.sociales.uba.ar/wp-content/uploads/sites/219/2020/09/Garc%C3%ADa-Ferrando.pdf

Gómez, F. (s/f). *Importancia de implementar un SGSI en nuestra organización.* https://www.safesociety.co/blogitem/4/la-importancia-de-implementar-un-sgsi-en-nuestra-organizacion

González, R. (2012). *Diagrama de Ishikawa: Análisis causa-efecto de los problemas.* Recuperado 14 de febrero de 2022, de https://www.pdcahome.com/diagrama-de-ishikawa-2/

https://diposit.ub.edu/dspace/bitstream/2445/13223/1/Auditoria%20de%20gesti%C3%B3n.pdf

Instituto Nacional de Tecnología de la Comunicación de España, (2013). *Implantación de un SGSI en la empresa*. INCIBE. Recuperado 12 de marzo de 2022, de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

Iso.org (2022). *ISO/IEC 27001, Gestión de la Seguridad de la información*. Disponible en: https://www.iso.org/isoiec-27001-information-security.html

López, J., (2014), Tesis pregrado: *Normas y estándares informáticos. Recuperado 30 de enero de 2022, de https://repositorio.unapiquitos.edu.pe/handle/20.500.12737/4504*

Mata, L. (2021). *El enfoque de la investigación: la naturaleza del estudio*. Recuperado 25 de marzo de 2022, de https://investigaliacr.com/investigacion/el-enfoque-de-investigacion-la-naturaleza-del-estudio/

Meing, W. (1983). *Princicios de Auditoria* (2ª ed.) Editorial Diana.

Mendívil, V. (2002). *Elemento de Auditoria*. (7 ª edición). Cengage Learning Editors.

Mifsud, E. (2012). *Vulnerabilidades de un sistema informático*. Introducción a la seguridad informática. Recuperado 08 de febrero de 2022, de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

Montoya, J. (2009). *Estándar Internacional ISO/IEC 27002.* Recuperado 01 de marzo de 2022, de https://www.monografias.com/trabajos67/estandar-internacional/estandar-internacional2

Noguez, V. (2016). *Cuál es el objetivo de una auditoría.* Recuperado 25 de febrero de 2022, de https://www.escuelaeuropeaexcelencia.com/2016/02/objetivo-de-una-auditoria/

Palella, S. y Martins, F. (2008). Población, Metodología de la Investigación Cuantitativa (2ª Edición). Caracas: FEDUPEL. Recuperado el 16 de marzo de 2021, de: http://investigacionmetodologicaderojas.blogspot.com/2017/09/poblacion-y-muestra.html

Pérez, L (2021), *Gestión de TI.* Recuperado 16 de febrero de 2022, de https://www.computerweekly.com/es/definicion/Gestion-de-TI

Razo, C. (2011:119). *Cómo elaborar y asesorar una investigación de tesis*. Recuperado el 24 de marzo de 2022, de: http://www.indesgua.org.gt/wp-content/uploads/2016/08/Carlos-Mu%C3%B1oz-Razo-Como-elaborar-y-asesorar-una-investigacion-de-tesis-2Edicion.pdf

Recuperado 05 de febrero de 2022, de https://cucjonline.com/biblioteca/files/original/la85f884ealf890592bdd5f94lf5b715

Redondo, R. (1996) *Auditoria de gestión.* Recuperado 02 de febrero de 2022, de

República Bolivariana de Venezuela (1999). *Constitución de la República Bolivariana de Venezuela.* Gaceta oficial N°36.860, diciembre 30. Caracas.

República Bolivariana de Venezuela (2001). Ley especial contra los Delitos Informáticos. Gaceta oficial N°37.313, octubre 30. Caracas.

Sabino, C. (1992). El proceso de la investigación. Recuperado el 16 de marzo de 2021, de: http://paginas.ufm.edu/sabino/ingles/book/proceso_investigacion.pdf

Salazar, H. (2015). *Definición de evaluación*. Definicionmx. Recuperado 19 de marzo de 2022, de https://definicion.mx/evaluacion/

Sampieri, Fernández y Baptista. (2004). *Metodología de la investigación*. (6 ª edición). México https://sites.google.com/site/practicadocenteimatematica/la-entrevista

Sánchez, A. (2021). *Diagrama de flujo.* ConceptoDefinicion. Disponible en: https://conceptodefinicion.de/diagrama-de-flujo/

Sánchez, F. (2006). Contabilidad financiera para PYMES. Colombia, Editorial TRILLAS.

Sánchez, J. (2020). *Auditoría externa*. Economipedia. Recuperado 06 de febrero de 2022, de https://economipedia.com/definiciones/auditoria-externa.html

Tamayo y Tamayo, M. (2006). Muestra, Técnicas de Investigación. (2ª Edición). México: Editorial Mc Graw Hill. Recuperado el 27 de marzo de 2022, de: file:///C:/Users/USUARIO/Downloads/Dialnet-SignificatividadDelMarcoMetodologicoEnElDesarrollo-7062667.pdf

Thompson, I. (2008). *Definición de Información*. Promonegocios. Recuperado 22 de marzo de https://www.promonegocios.net/mercadotecnia/definicion-informacion.html

Universidad Pedagógica Experimental Libertador (1998). *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Caracas.

Uriarte, J. (2021). *Definición y características de Auditoria.* Recuperado 09 de febrero de 2022, de https://www.caracteristicas.co/auditoria/

Uriarte, J. (2021). *Definición y características de Sistema Informático.* Recuperado 14 de febrero de 2022, de https://www.caracteristicas.co/sistema-informatico/