UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

Proyecto Integrador, previo a la obtención del Título de Licenciado en Contabilidad y Auditoría

Tema:

"Diseño de controles de seguridad informática para el sistema de información en la empresa proveedora de internet Telpronet de la ciudad de Ambato"

Autor: Sánchez Acuña, William Alexis

Tutora: Dra. Jiménez Estrella, Patricia Paola

Ambato - Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella con cédula de ciudadanía No. 180293423-0, en mi calidad de Tutora del proyecto integrador sobre el tema: "**DISEÑO DE CONTROLES DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA DE INFORMACIÓN EN LA EMPRESA PROVEEDORA DE INTERNET TELPRONET DE LA CIUDAD DE AMBATO**", desarrollado por William Alexis Sánchez Acuña, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, Febrero 2024.

TUTORA

……..……..

Dra. Patricia Paola Jiménez Estrella

C.C. 180293423-0

AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, William Alexis Sánchez Acuña con cédula de ciudadanía No. 180483026-1, tengo a bien indicar que los criterios emitidos en el proyecto integrador, bajo el tema: "**DISEÑO DE CONTROLES DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA DE INFORMACIÓN EN LA EMPRESA PROVEEDORA DE INTERNET TELPRONET DE LA CIUDAD DE AMBATO**", así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autor de este Proyecto Integrador.

Ambato, Febrero 2024.

AUTOR

……..……..

William Alexis Sánchez Acuña

C.C. 180483026-1

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este proyecto integrador, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi proyecto integrador, con fines de difusión pública; además apruebo la reproducción de este proyecto integrador, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autor.

Ambato, Febrero 2024.

AUTOR

……..……..

William Alexis Sánchez Acuña

C.C. 180483026-1

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el proyecto integrador, sobre el tema**: "DISEÑO DE CONTROLES DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA DE INFORMACIÓN EN LA EMPRESA PROVEEDORA DE INTERNET TELPRONET DE LA CIUDAD DE AMBATO"**, elaborado por William Alexis Sánchez Acuña, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, Febrero 2024.

_____

Dra. Tatiana Valle Ph. D.

PRESIDENTE

_____ _____

Dr. Mauricio Arias — Ing. Alberto Luzuriaga

MIEMBRO CALIFICADOR — **MIEMBRO CALIFICADOR**

DEDICATORIA

El presente proyecto de titulación se lo dedico a mi familia, que han sido los que han estado siempre a mi lado en todo momento.

A mis padres, Geovanny Sánchez y Angelica Acuña, por estar conmigo en cada paso del camino, brindándome apoyo y siendo mi inspiración y ejemplo para alcanzar todos mis sueños.

A mi hermana Angelita que ha sido un gran apoyo y motivación en mi vida, enseñando a no rendirme y seguir con más fuerza hacia adelante.

A mi tía Isabel por su apoyo y cariño incondicional tanto en el ámbito personal como académico, siempre motivándome a mejorar y cumplir mis objetivos.

William Alexis Sánchez Acuña

AGRADECIMIENTO

Agradezco a Dios por darme la salud, la vida y la inteligencia, a mis padres y hermana por su apoyo incondicional en todo momento siendo la razón de este título profesional.

A la Universidad Técnica de Ambato, por darme la oportunidad de formar parte de esta reconocida institución. A los docentes de la Facultad de Contabilidad y Auditoría, de manera especial a mi tutora Dra. Patricia Jiménez por compartir su conocimiento en la ejecución de este proyecto.

A Telpronet por permitirme realizar mi proyecto de titulación, brindándome los datos y recursos necesarios.

William Alexis Sánchez Acuña

ÍNDICE GENERAL DE CONTENIDOS

CONTENIDO **PÁGINA**

A. PÁGINAS PRELIMINARES
PORTADA i
APROBACIÓN DEL TUTOR ii
AUTORÍA DEL TRABAJO DE TITULACIÓN iii
DERECHOS DE AUTOR iv
APROBACIÓN DEL TRIBUNAL DE GRADO v
DEDICATORIA vi
AGRADECIMIENTO vii
ÍNDICE GENERAL DE CONTENIDOS viii
ÍNDICE DE TABLAS xi
ÍNDICE DE ILUSTRACIONES xii
RESUMEN EJECUTIVO xiii
ABSTRACT xiv
B. CONTENIDOS
CAPÍTULO I 1
MARCO TEÓRICO 1
1.1. Introducción 1
1.1.1. Antecedentes del proyecto integrador 1
1.1.1.1. Historia de la empresa 1
1.1.1.2. Detalles estratégicos 2
1.1.1.3. Estructura organizacional 3
1.1.1.4. Detalles de operación 3
1.1.1.5. Detalles legales 4
1.1.1.6. Marcas y logos 4
1.1.1.7. Ubicación 5
1.1.2. Descripción del entorno 5
1.1.2.1. Importancia de la seguridad informática en América Latina 5

1.1.2.2. Ciberataques en las empresas del Ecuador y los controles en seguridad digital……. 6
1.1.2.3. Controles informáticos y seguridad de la información en Telpronet .. 8
1.1.3. Justificación 8
1.1.4. Objetivos 9
1.1.4.1. Objetivo general 9
1.1.4.2. Objetivos específicos 9
1.2. Revisión de la literatura 10
1.2.1. La teoría de sistemas de información y los riesgos en los activos de información 10
1.2.2. Concepto de auditoría 10
1.2.2.1. Importancia 11
1.2.3. Fases 11
1.2.4. Tipos de auditoría 12
1.2.4.1. De acuerdo con quién lo elabora 12
1.2.4.2. De acuerdo con la metodología 13
1.2.4.3. De acuerdo con el área a auditar 13
1.2.5. Tecnologías de la información 14
1.2.6. Sistemas de información 14
1.2.6.1. Seguridad informática 14
1.2.6.2. Seguridad física 15
1.2.6.3. Seguridad lógica 16
1.2.7. Sistema de Gestión de la Seguridad de la Información (SGSI) 16
1.2.8. Administración de riesgos 17
1.2.8.1. Tipos de riesgos 17
1.2.8.2. Tipos de vulnerabilidades 17
1.2.9. Definiciones básicas 19
1.2.10. Marco legal 19
1.2.10.1. Norma ISO 27000 19
1.2.10.2. Norma ISO 27001 20
1.2.10.3. Norma ISO 27002 21
1.2.10.4. Norma ISO 31000:2009 21

CAPÍTULO II 22
METODOLOGÍA 22
2.1. Descripción del entorno 22
2.1.1. Unidad de análisis 22
2.1.2. Fuentes y técnicas de recolección de información 22
2.1.2.1. Fuentes de información primaria 22
2.1.3. Fases de desarrollo 26
CAPÍTULO III 30
DESARROLLO 30
3.1. Desarrollo de los controles de seguridad de la información 30
3.1.1. Análisis preliminar 31
3.1.2. Ejecución 35
3.1.2.1. Activos de información 35
3.1.2.2. Controles actuales de la empresa 39
3.1.2.3. Evaluación nivel de riesgo 42
3.1.3. Comunicación 46
3.1.3.1. Inventario de activos de información con base a las normas ISO 46
3.1.3.2. Normas generales de la empresa 49
3.1.3.3. Políticas por cada grupo de activos de información 51
3.1.3.4. Políticas y controles software contable 60
3.1.3.5. Políticas y controles hardware 64
3.1.3.6. Políticas y controles redes 66
3.1.3.7. Políticas y controles instalaciones 68
3.1.3.8. Políticas y controles personal 70
3.1.3.9. Matriz de seguimiento y monitoreo 72
CAPÍTULO IV 75
CONCLUSIONES Y RECOMENDACIONES 75
4.1. Conclusiones 75
4.2. Recomendaciones 77
C. MATERIAL DE REFERENCIA
REFERENCIAS BIBLIOGRÁFICAS 78

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

Tabla 1.-Auditorías en el área de sistemas 13
Tabla 2.-Principios de seguridad física..... 15
Tabla 3.-Tipos de vulnerabilidades..... 18
Tabla 4.-Definiciones básica 19
Tabla 5.- Beneficios ISO 27002 21
Tabla 6.-Personas entrevistadas y encuestadas..... 23
Tabla 7.- Preguntas del cuestionario y escalas 23
Tabla 8.- Preguntas de la entrevista y sus categorías 24
Tabla 9.- Fases de desarrollo del diseño de controles de seguridad informática..... 26
Tabla 10.- Criterios para los 3 principios de la información 27
Tabla 11.- Escala del nivel de tasación..... 28
Tabla 12.- Calificación de los controles 28
Tabla 13.- Niveles probabilidad e impacto..... 29
Tabla 14.- Calificación de los controles 29
Tabla 15.- Análisis de la entrevista 32
Tabla 16.- Análisis de la encuesta 34
Tabla 17.- Tasación de los activos de información..... 36
Tabla 18.- Controles actuales de la empresa 40
Tabla 19.- Probabilidad e impacto de los activos de información..... 43
Tabla 20.- Normas generales de Telpronet 50
Tabla 21.- Matriz de seguimiento y monitoreo de activos 73

ÍNDICE DE ILUSTRACIONES

CONTENIDO **PÁGINA**

Ilustración 1.- Organigrama estructural de la empresa Telpronet 3
Ilustración 2.- Logo de la empresa Telpronet 4
Ilustración 3.- Ubicación de la empresa 5
Ilustración 4.- Fases de la auditoría 11
Ilustración 5.- Clasificación de la auditoría 12
Ilustración 6.- Diferencia entre auditor interno y externo 12
Ilustración 7.- Diferencia de cumplimiento y técnicas 13
Ilustración 8.- Hardware y software 14
Ilustración 9.- Diferencia confidencialidad, integridad y disponibilidad 15
Ilustración 10.- Objetivos que se plantean en la seguridad lógica 16
Ilustración 11.- Ventajas del SGSI 16
Ilustración 12.- Clasificación de riesgos 17
Ilustración 13.- Ciclo deming o PDCA 20
Ilustración 14.- Relación entre el modelo PDCA y la ISO 27001 31
Ilustración 15.- Principio #1 “confidencialidad” 37
Ilustración 16.- Principio #2 “integridad” 38
Ilustración 17.- Principio #3 “disponibilidad” 38
Ilustración 18.- Controles Telpronet 41
Ilustración 19.- Mapa de calor 44
Ilustración 20.- Nivel de riesgo de los activos 45
Ilustración 21.- Pasos para la elaboración de un inventario de activos 46
Ilustración 22.- Logo del sistema contable 55
Ilustración 23.- Ventajas y desventajas 56

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "DISEÑO DE CONTROLES DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA DE INFORMACIÓN EN LA EMPRESA PROVEEDORA DE INTERNET TELPRONET DE LA CIUDAD DE AMBATO"

AUTOR: William Alexis Sánchez Acuña
TUTORA: Dra. Patricia Paola Jiménez Estrella
FECHA: Febrero 2024

RESUMEN EJECUTIVO

El objetivo principal del proyecto integrador fue diseñar controles de seguridad para el sistema de información de la empresa Telpronet de la ciudad de Ambato, cumpliendo con los principios básicos de disponibilidad, confidencialidad e integridad con base a la norma ISO 27000. Se realizó un diagnóstico previo a través de encuestas y entrevistas para la obtención de información sobre los activos relevantes en las operaciones de la empresa, realizando un inventario de los activos de información a los que se les asignó un nivel de importancia de acuerdo a las amenazas y vulnerabilidades expuestas. A través de una matriz de riesgos informáticos se determinó su nivel de criticidad. Por lo tanto, se diseñaron políticas y controles considerando las necesidades de la empresa, enfocándose principalmente en el software contable, ya que es, la herramienta de trabajo que permite el ingreso, procesamiento, almacenamiento y salida de información. Como resultado, se evidenció que los empleados carecen de capacitación en seguridad de la información y que los controles fueron aplicados de manera básica por lo que, la empresa debe tener una mejora continua en los procesos relacionados a la seguridad de información y hacer un seguimiento permanente del cumplimiento de los controles y políticas sugeridos.

PALABRAS DESCRIPTORAS: CONTROL, INFORMACIÓN, SEGURIDAD, VULNERABILIDAD, POLÍTICAS.

TECHNICAL UNIVERSITY OF AMBATO
FACULTY OF ACCOUNTING AND AUDITING
ACCOUNTING AND AUDITING CAREER

TOPIC: "DESIGN OF COMPUTER SECURITY CONTROLS FOR THE INFORMATION SYSTEM IN THE INTERNET PROVIDER COMPANY TELPRONET IN THE CITY OF AMBATO".

AUTHOR: William Alexis Sánchez Acuña
TUTOR: Dra. Patricia Paola Jiménez Estrella
DATE: February 2024

ABSTRACT

The main objective of the integration project was to design security controls for the information system of the company Telpronet in the city of Ambato, complying with the basic principles of availability, confidentiality and integrity based on the ISO 27000 standard. A preliminary diagnosis was made through surveys and interviews to obtain information about the relevant assets in the company's operations, making an inventory of the information assets to which a level of importance was assigned according to the threats and vulnerabilities exposed. Their level of criticality was determined through a computer risk matrix. Therefore, policies and controls were designed considering the needs of the company, focusing mainly on the accounting software, as it is the working tool that allows the entry, processing, storage, and output of information. As a result, it was evidenced that the employees lack training in information security and that the controls were applied in a basic way; therefore, the company must have a continuous improvement in the processes related to information security and make a permanent follow-up of the compliance with the suggested controls and policies.

KEYWORDS: CONTROL, INFORMATION, SECURITY, VULNERABILITY, POLICIES.

CAPÍTULO I

MARCO TEÓRICO

1.1.Introducción

1.1.1. Antecedentes del proyecto integrador

1.1.1.1.Historia de la empresa

Conforme lo comentado por la representante legal de la empresa Telpronet Tannia Castillo (2023) la empresa comenzó sus actividades en agosto de 2010. En ese momento, los señores Patricio Molina y Tannia Castillo se unieron para formar Telpronet, con el objetivo de brindar servicio de internet asequible a la ciudadanía de Pujilí, donde en ese momento era limitado.

El esfuerzo, la iniciativa y el empuje de los fundadores se reflejan en la gestión de la empresa, que se caracteriza por una fuerte filosofía de reinversión. Gracias a esto, Telpronet ha logrado evolucionar, mantenerse en el mercado de telecomunicaciones inalámbricas, generar empleo y conectar a las personas con el mundo. El talento humano ha sido fundamental en estos más de diez años, construyendo credibilidad en el campo de las telecomunicaciones sin perder de vista los valores que caracterizan a la empresa.

Telpronet es un proveedor de internet y equipos terminales, cuya reputación ha sido forjada con esfuerzo, ética, eficiencia y atención constante. Esto le ha permitido ganar reconocimiento tanto en la población de Cotopaxi como en la de Ambato. El éxito alcanzado se debe al trabajo diario de un valioso equipo humano compuesto por empleados, técnicos y profesionales debidamente preparados para atender las demandas y requerimientos de los clientes.

Actualmente, Telpronet tiene cobertura en la zona central del país, con oficinas en Ambato y Pujilí, además de un punto de pago autorizado en Salcedo. La empresa ofrece un servicio de internet de alta calidad que utiliza tecnología de fibra óptica. Cuenta con los mejores planes disponibles en la zona, los cuales garantizan un servicio confiable y seguro.

1.1.1.2.Detalles estratégicos

Los detalles estratégicos fueron recolectados de la página oficial de la empresa (Telpronet, 2023):

Misión

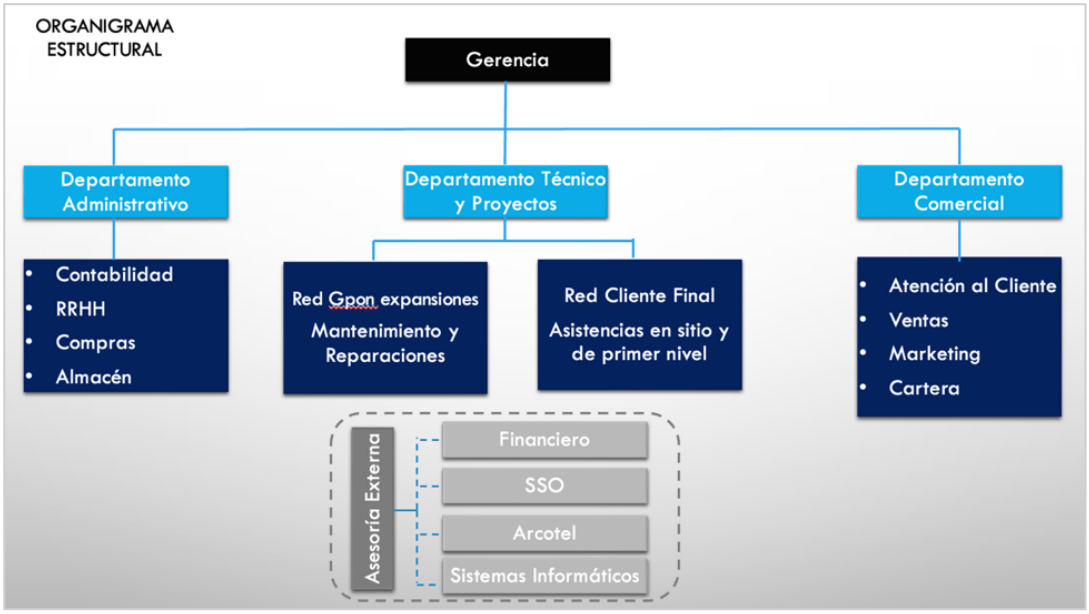
Somos una empresa dinámica y en constante mejora e innovación, siempre en busca de brindar soluciones de alta calidad a todos nuestros clientes.

Valores Corporativos

- **Honestidad:** Mantener una conducta ética y cumplir con altos estándares de comportamiento tanto hacia los clientes como hacia los empleados y demás partes interesadas.
- **Calidad:** Cumplir con altos estándares en términos de velocidad, estabilidad de la conexión y atención al cliente.
- **Orientación al cliente:** Actitud completamente disponible tanto para los clientes internos como externos, resolviendo sus necesidades desde el primer contacto, con el fin de cumplir con la promesa de valor y generar una experiencia de servicio excepcional.
- **Trabajo en equipo:** Colaborar de manera efectiva y coordinada con los demás miembros de la empresa para alcanzar objetivos compartidos.

1.1.1.3.Estructura organizacional

Ilustración 1.- Organigrama estructural de la empresa Telpronet



—— Relación de autoridad y subordinación (indican comunicación).

···· Relación de coordinación y relaciones funcionales.

Fuente: Telpronet (2023)

1.1.1.4.Detalles de operación

Telpronet (2023) brinda acceso a Internet de acuerdo con los siguientes planes:

- Plan Bronze 80 MB
- Plan Platimun 100 MB
- Plan Gold 150 MB
- Plan Diamond 200 MB
- Plan Home Plus 25 MB
- Plan Home Premium 30MB
- Home Ultra-Premium

1.1.1.5.Detalles legales

Telpronet (2023) lleva a cabo sus actividades conforme la siguiente base legal:

- Reglamento de los Abonados
- Reglamento General Ley Orgánica de Telecomunicaciones
- Calidad de Servicio del Abonado
- Ley Orgánica de Telecomunicaciones
- Ley Orgánica de Discapacitados
- Reglamento Ley Orgánica de los Adultos Mayores
- Guía de Seguridad Informática
- Guía Control Parental
- Ley de Protección de Datos
- Ley de Seguridad Social
- Ley de Régimen Tributario Interno

1.1.1.6.Marcas y logos

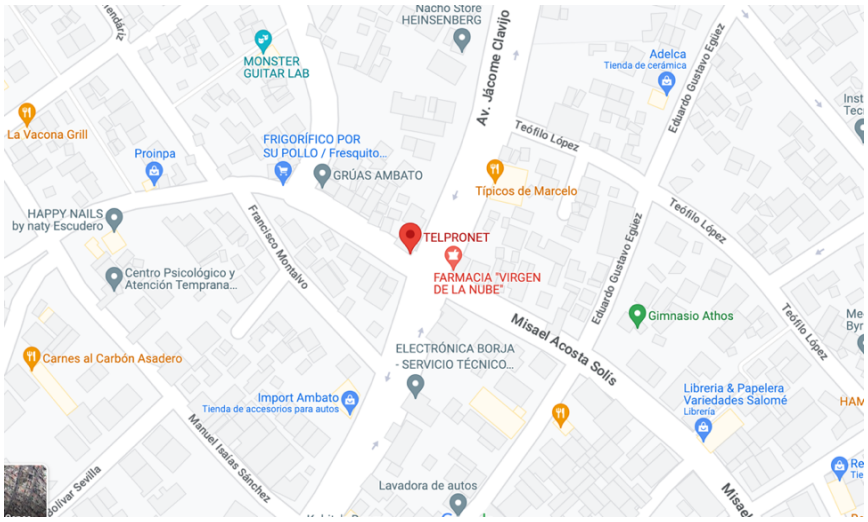
Ilustración 2.- Logo de la empresa Telpronet

Fuente: Telpronet (2023)

1.1.1.7.Ubicación

Telpronet se encuentra ubicada en la Av. Jácome Clavijo y Misael Acosta Solís (esquina).

Ilustración 3.- Ubicación de la empresa



Fuente: Google maps (2023)

1.1.2. Descripción del entorno

1.1.2.1.Importancia de la seguridad informática en América Latina

Es fundamental reconocer que las empresas deben resguardar los datos y asegurar su integridad, confidencialidad y disponibilidad, de ahí la importancia de la seguridad informática. Según Guerra et al. (2021) indican que las políticas implementadas en la empresa a veces pueden generar confusión, ya que la seguridad informática implica más que solo un usuario y una contraseña. Se requiere cumplir con las normativas, estrategias de privacidad y protección de datos impuestas por las leyes vigentes. A lo que, Sánchez et al. (2021) sostienen que es importante contar con la herramienta computacional llamada UdeCEscaner que permita fortalecer las estrategias de seguridad y así evaluar las posibles vulnerabilidades de la empresa para anticiparse a posibles ataques informáticos (Franco et al., 2013). En definitiva, la evaluación de las vulnerabilidades informáticas es un proceso que tiene un gran impacto en el sistema de información, sistemas contables, procesos contables automatizados de todas las organizaciones de América Latina.

En una investigación realizada por Kosevich (2020) se menciona que en los últimos 5 años ha habido un incremento del 40% en la cantidad de ataques cibernéticos en la región, lo que representa a más de 700 millones de ataques en un solo año. Los ciberdelitos en América Latina han causado graves daños económicos, alcanzando una suma total de $90 mil millones de dólares americanos. Entre los países más afectados se encuentran Brasil que representa el 55% de los ataques en la región, seguido por México con el 17% y Colombia con el 9%. De este modo, Camargo & Pinzon (2022) destacan que la mitad de las naciones del Caribe y América Latina carecen de la capacidad necesaria para defenderse eficazmente contra los ataques cibernéticos. Por consiguiente, los países elaboran políticas, estrategias y planes de seguridad para abordar este tipo de problemas.

Guaña (2023) menciona que en Colombia el riesgo en la seguridad informática es muy común debido a que no se valora la información y no se incluye la instalación de un antivirus en los planes de Internet. Es por eso por lo que este país ratifica la importancia de utilizar mecanismos de ciberseguridad para proteger los datos en todas las instituciones y organizaciones tanto públicas como privadas. Por lo tanto, hoy en día la información se ha transformado en un recurso de gran valor para todas las organizaciones, lo que ha llevado a la necesidad de invertir recursos para mantenerla, administrarla y crearla (Altamirano, 2019).

1.1.2.2. Ciberataques en las empresas del Ecuador y los controles en seguridad digital

Según el informe anual número 14 del CSI (Competer Security Institute) sobre delitos informáticos en Ecuador, se estima que se han registrado pérdidas de miles de dólares, que oscilan entre los 289.000 dólares y los 234.244 dólares (Jordán et al., 2013). De la misma forma Zúñiga et al. (2020) mencionan que en la actualidad existen diversos riesgos asociados a los equipos y sistemas de información. Se destaca que las empresas que no cuentan con controles de seguridad son las más propensas a correr riesgos.

La falta de capacitación del personal en las empresas es la principal razón del incremento de los ataques cibernéticos en el país. Según Maino (2022) en un estudio realizado se menciona que, las empresas todavía no han podido adaptar una cultura de

seguridad digital con las mejores prácticas para sus colaboradores. Por otra parte Pérez (2022) indica que si bien existen leyes, normas y reglamentos que ayudan a mejorar la seguridad informática, es necesario contar con personal específico en el ámbito para disminuir el riesgo en la empresa. De este modo las organizaciones del Ecuador enfrentan grandes desafíos relacionados con las personas, la orientación al cliente, la empresa, la privatización y la creatividad (Rivera, 2013).

De acuerdo con Ponce (2016) las empresas privadas en el Ecuador han mostrado un mayor interés en adquirir servicios de ciberseguridad para enfrentar las amenazas constantes que intentan comprometer la seguridad de sus datos. La principal limitación que enfrentan estas organizaciones es el presupuesto asignado a invertir en seguridad informática. A pesar de tener ciertas restricciones en cuanto a invertir en protección de la información Valencia et al. (2023) indican que las empresas en la actualidad asignan más recursos de su presupuesto a esta área. Esta tendencia es motivada por los profesionales de la ciberseguridad que se fundamentan en los ataques informáticos en continua transformación.

Las auditorías y los enfoques metodológicos han permitido conocer las diversas dificultades que las organizaciones han enfrentado a lo largo de los años. En el año 2019 se registraron ciberataques a los sitios web de instituciones muy conocidas en Ecuador. Entre los organismos públicos y privados afectados se encontraban la embajada, el Banco Central, la Presidencia, Corporación Nacional de Telecomunicaciones (CNT), Banco del Pichincha, el Servicio Rentas Internas (SRI), entre otras (Toapanta et al., 2019).

A si mismo Ramos (2020) menciona que, a través de la Ley de Comercio Electrónico se puede dar seguimiento a las infracciones informáticas clasificadas en dos tipos, una con carácter administrativo y la segunda relacionada con los delitos en el código penal. Es decir, en Ecuador se manifiesta la falta de preparación y conciencia sobre la importancia de la ciberseguridad.

1.1.2.3.Controles informáticos y seguridad de la información en Telpronet

De acuerdo con la gerente de Telpronet Tannia Castillo (2023) la empresa se encuentra realizando sus operaciones por más de 10 años, en un entorno dinámico y complejo debido a que presentan desafíos únicos en términos de seguridad de la información. Un aspecto que complica la protección de datos en la empresa proveedora de servicios de internet, es la diversidad de amenazas a la que están expuesto, como ciberataques, malware, phishing, spam y robo de identidad, entre otros.

Durante la pandemia se observó cómo los ciberataques afectaron a la empresa, debido a la transición masiva al trabajo remoto y la reciente dependencia de la tecnología digital crearon nuevas oportunidades para los ciberdelincuentes. Es decir, la pandemia actuó como un catalizador para aumentar la cantidad y la sofisticación de los ataques cibernéticos, en donde la empresa no estaba preparada para esta situación.

Por lo tanto, es adecuado realizar un estudio profundo sobre el cuidado, manejo de los recursos informáticos, como un plan para así dar mejora continua que provean medidas de control siendo fundamental realizar un control de la seguridad informática en la empresa, para así determinar posibles amenazas y evaluar los riesgos para sugerir un tratamiento adecuado para la mitigación, seguimiento y monitoreo de los controles de seguridad.

1.1.3. Justificación

Estrada et al. (2021) mencionan que los ciberataques se han vuelto muy comunes a nivel general, ya que pueden afectar tanto a aplicaciones como a sistemas empresariales. Durante la pandemia se ha observado un aumento considerable en la probabilidad de ser víctima de ataques, pasando de 33 a 41 modalidades de ciberataques. Esto se debe a que, durante ese tiempo se utilizaban en gran medida dispositivos tecnológicos para comunicarse o realizar teletrabajo (Carvajal, 2020). En este contexto, las organizaciones optaron por priorizar la protección de la seguridad de sus clientes, ya que es un activo importante (Hernández et al., 2019).

En este proyecto integrador, se llevó a cabo una investigación bibliográfica documental debido a que se obtuvieron datos de fuentes secundarias consultadas sobre

los controles de seguridad informática. Además, se utilizaron datos de fuentes primarias de la empresa, obtenidos a través de encuestas y entrevistas (técnicas) realizadas a las personas responsables de la seguridad informática y el sistema de información, lo que permitió tener un contexto más amplio. Posteriormente se identificaron y evaluaron las vulnerabilidades presentes en la empresa. A continuación, con la identificación de los riesgos se determinó el nivel de severidad y se conoció si los activos eran críticos o no.

Como resultado de este proyecto integrador, la empresa Telpronet tuvo un impacto significativo después de determinar las vulnerabilidades y amenazas, ya que se diseñó una guía práctica de controles preventivos, detectivos y correctivos, según el caso. Esto permitió establecer políticas de seguridad que, en conjunto, proporcionaron una gestión óptima y eficiente. Además, se aplicaron las normativas estándar según la ISO 27000 y 31000, lo que garantizó y facilitó la ejecución del trabajo tanto para los empleados como para el gerente. Finalmente, se proporcionaron recomendaciones detalladas para la organización. Por lo tanto, la realización del proyecto integrador fue factible.

1.1.4. Objetivos

1.1.4.1.Objetivo general

Diseñar políticas de control para el sistema de gestión de la seguridad de la información en la empresa Telpronet en la ciudad de Ambato.

1.1.4.2.Objetivos específicos

- Realizar el inventario de activos de información de la empresa, identificando amenazas, vulnerabilidades y riesgos que se encuentren expuestos, para su respectivo nivel de tasación.
- Evaluar las amenazas y riesgos para la identificación de los posibles impactos que provoque la deficiencia en los controles de SGSI.
- Establecer las políticas para el SGSI conforme la norma ISO/IEC 27000 para la seguridad informática y los controles a aplicarse.

1.2.Revisión de la literatura

1.2.1. La teoría de sistemas de información y los riesgos en los activos de información

La teoría de sistemas de información se refiere al estudio de los sistemas que procesan, almacenan y transmiten información dentro de una organización. De acuerdo con Brien & Marakas (2006) esta teoría busca comprender cómo los componentes de un sistema interactúan entre sí para lograr los objetivos organizacionales. En este sentido, el sistema permite analizar los componentes como hardware, software, redes de telecomunicaciones y el procesamiento de datos para así verificar que la información sea segura. Es por esta razón, que se deben implementar directrices y protocolos que ayuden a minimizar las posibles amenazas. Asimismo, los autores señalan que el riesgo de los activos de información se debe en gran mayoría a la ausencia de aplicación de normativas de seguridad informática. De esta manera, el enfoque desde la cual se estudia y comprende el funcionamiento de los sistemas de información es examinar su diseño, implementación y uso con la finalidad de que la eficiencia y efectividad de las organizaciones tenga una mejora continua. Bajo este criterio, se considera que la aplicación del estándar ISO/IEC es de vital importancia en cualquier sistema de información. En resumen, la teoría de sistemas de información busca evaluar el riesgo y, a su vez, implementar controles que ayuden a cumplir las metas de la compañía.

1.2.2. Concepto de auditoría

Es un proceso de revisión y evaluación sistemática de las cuentas, registros y controles financieros e informáticos de una compañía u organización para cerciorarse de que se practiquen los estándares y prácticas contables, legales y éticas (Baca, 2016).

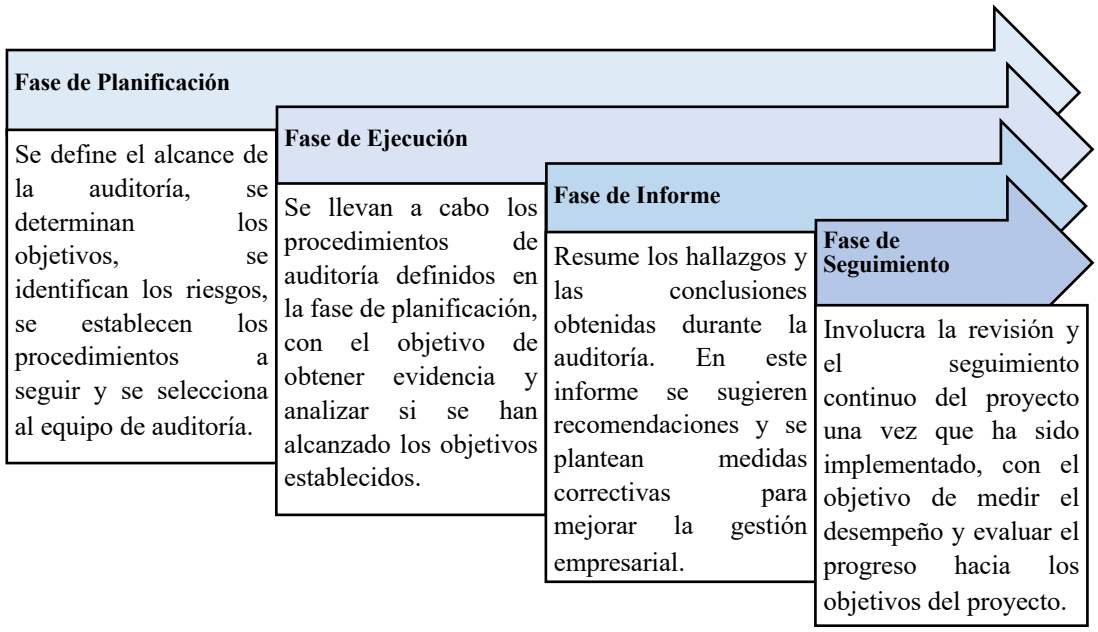
1.2.2.1.Importancia

La auditoría es primordial para todas las empresas porque permite evaluar y controlar su situación financiera y operativa, optimizar procesos internos, proteger las finanzas, identificar áreas de mejora y cumplir con normas internacionales de auditoría. Además, las auditorías regulares permiten detectar posibles fraudes y errores contables antes de que se transformen en situaciones más graves (Meljem, 2018).

1.2.3. Fases

Según Pelanzas (2022) las fases de auditoría se dividen en las siguientes:

Ilustración 4.- Fases de la auditoría



Elaborado por: Sánchez (2023)
Fuente: Pelanzas (2022)

1.2.4. Tipos de auditoría

Según Menéndez (2022) la clasificación de la auditoría se la realiza de acuerdo con quién lo elabora, la metodología y de acuerdo con el área a auditar.

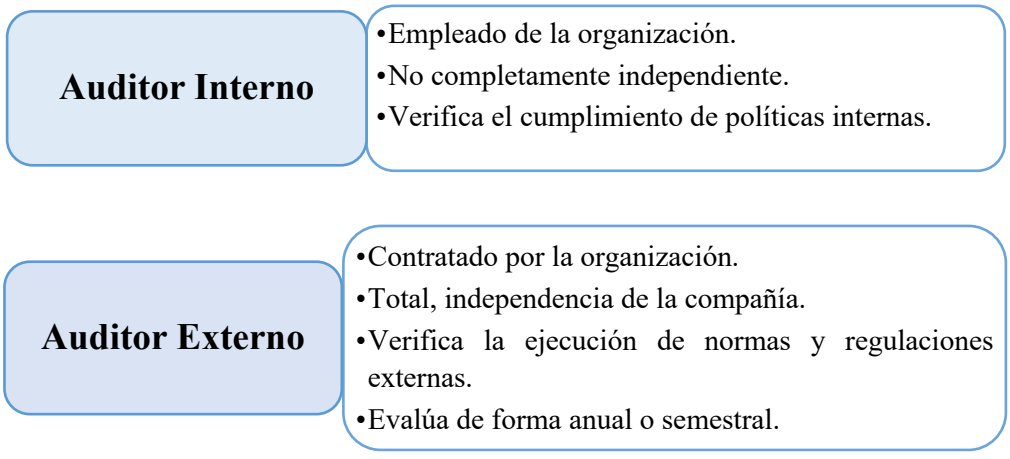
Ilustración 5.- Clasificación de la auditoría

De acuerdo con quién lo elabora	De acuerdo con la metodología	De acuerdo con el área a auditar (Sistemas)
•Interna •Externa	•De Cumplimiento •Técnicas	•De Redes de telecomunicaciones •De Sistemas Operativos •De Aplicaciones •De Vulnerabilidades •De seguridad, lógica, física •Web

Elaborado por: Sánchez (2023)
Fuente: Menéndez (2022)

1.2.4.1.De acuerdo con quién lo elabora

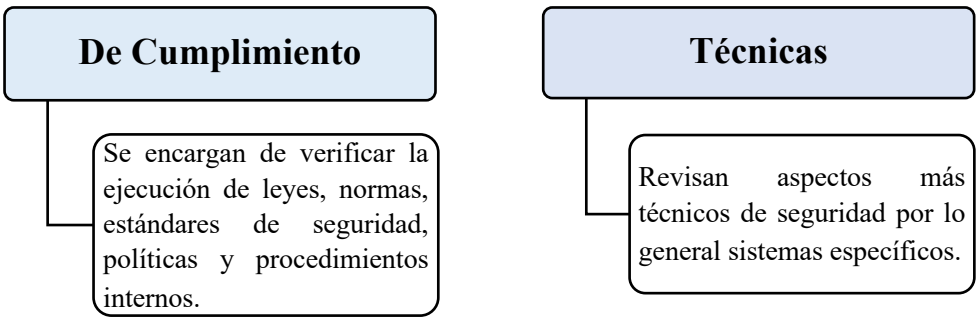
Ilustración 6.- Diferencia entre auditor interno y externo



Elaborado por: Sánchez (2023)
Fuente: Menéndez (2022)

1.2.4.2.De acuerdo con la metodología

Ilustración 7.- Diferencia de cumplimiento y técnicas



Elaborado por: Sánchez (2023)
Fuente: Menéndez (2022)

1.2.4.3.De acuerdo con el área a auditar

Tabla 1.-Auditorías en el área de sistemas

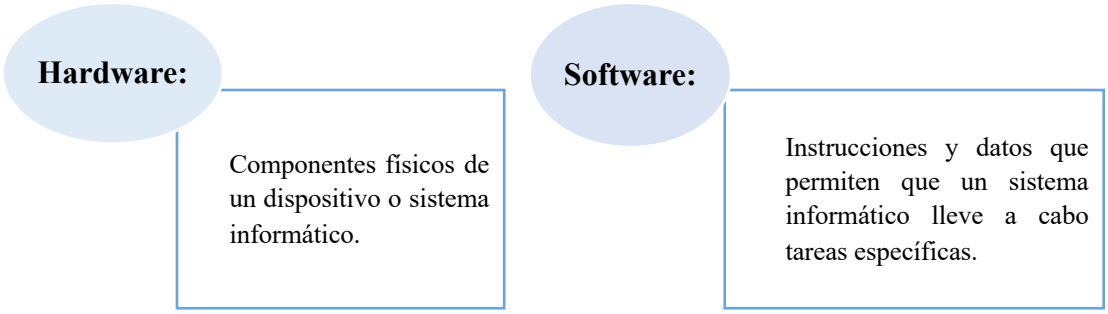
Auditoría de redes y comunicaciones	**Auditoría de Aplicaciones**
Proceso de evaluaciones y análisis para conocer la situación actual de los sistemas de información en: rendimiento, seguridad, capacidades del sistema, cumplimiento de políticas y estándares.	Evaluación diseñada para identificar vulnerabilidades, errores o riesgos relacionados con la protección y el desempeño de las aplicaciones informáticas. El objetivo es detectar fallas en los sistemas de software.
Auditoría de Vulnerabilidades	**Auditoría de seguridad, lógica, física**
Se trata de un proceso enfocado en identificar y evaluar posibles debilidades y riesgos en la infraestructura y en el software de una organización. El objetivo es detectar las vulnerabilidades antes de que sean explotadas por terceros.	Proceso de evaluar y analizar la protección de los recursos físicos de la organización, como equipos, infraestructura e instalaciones, así como también la salvaguardia de los datos digitales de la compañía, incluyendo datos, sistemas informáticos y de red.
Auditoría Web	**Auditoría en Sistemas**
Es un proceso de análisis y evaluación exhaustiva de un sitio web con el objetivo de detectar los factores que afectan al rendimiento.	Implica examinar y evaluar los sistemas operativos de una organización para determinar su nivel de seguridad y confiabilidad.

Elaborado por: Sánchez (2023)
Fuente: Menéndez (2022)

1.2.5. Tecnologías de la información

Son el grupo de herramientas, recursos, equipos, programas y aplicaciones utilizados para crear, almacenar, procesar, recuperar, transmitir y gestionar la información. Pueden incluir hardware, software, redes de comunicaciones, internet, bases de datos, seguridad informática, entre otros. En la era digital, los sistemas de procesamiento de información son fundamentales y juegan un rol crucial en la manera en que las empresas se comunican y se relacionan con la sociedad y los negocios (Alias & Cebrian, 2019).

Ilustración 8.- Hardware y software



Elaborado por: Sánchez (2023)
Fuente: Madrigal (2019)

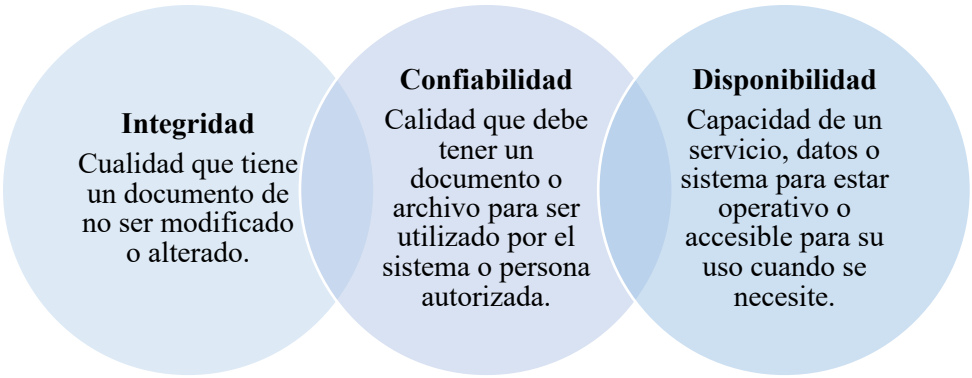
1.2.6. Sistemas de información

Se trata de un grupo de componentes interconectados que colaboran en conjunto para recolectar, procesar, guardar y compartir información, con el propósito de respaldar la voluntad de la alta gerencia, la coherencia y el control en la empresa (Dussan, 2020).

1.2.6.1.Seguridad informática

De acuerdo con Costas (2010) la seguridad informática se fundamenta en un conjunto de principios elementales que ayudan a proteger los datos ante posibles amenazas, entre ellos tenemos:

Ilustración 9.- Diferencia confidencialidad, integridad y disponibilidad



Elaborado por: Sánchez (2023)
Fuente: Costas (2010)

1.2.6.2.Seguridad física

De acuerdo con Gómez (2011) la seguridad física se centra en la aplicación de barreras físicas teniendo como principios los siguientes:

Tabla 2.-Principios de seguridad física

Control de acceso	**Sistemas biométricos**
Son procedimientos que limita la entrada a los medios de los sistemas de información con la intención de evitar el paso no autorizado.	Tipo de control de acceso que utiliza características físicas (reconocimiento facial) de una persona para autenticar su identidad y autorizar el acceso a los recursos.
Ciberseguridad	**Protección datos**
Conjunto de prácticas destinadas a resguardar los sistemas informáticos, redes, dispositivos y datos contra posibles ataques, perjuicios o ingresos no autorizados	Son las medidas y estrategias de seguridad electrónica (sensores conectados a alarmas) implementadas para proteger los datos y sistemas de información.
Condiciones ambientales	
Se refiriere al entorno físico donde se encuentran los recursos y sistemas de información, como la humedad, temperatura, iluminación, ruido, entre otros.	
Incendios	**Inundaciones**
Causados por el uso inadecuado de combustible o por el fallo en instalaciones eléctricas.	Invasión de agua por exceso, en donde la principal causa es los terrenos planos o la falta de drenaje.

Elaborado por: Sánchez (2023)
Fuente: Gómez (2011)

1.2.6.3.Seguridad lógica

Se refiere a la implementación de medidas y protocolos para proteger el acceso a los datos, permitiendo únicamente al personal autorizado acceder a ella. Para Menéndez (2022) los objetivos para tener en cuenta son los siguientes:

Ilustración 10.- Objetivos que se plantean en la seguridad lógica

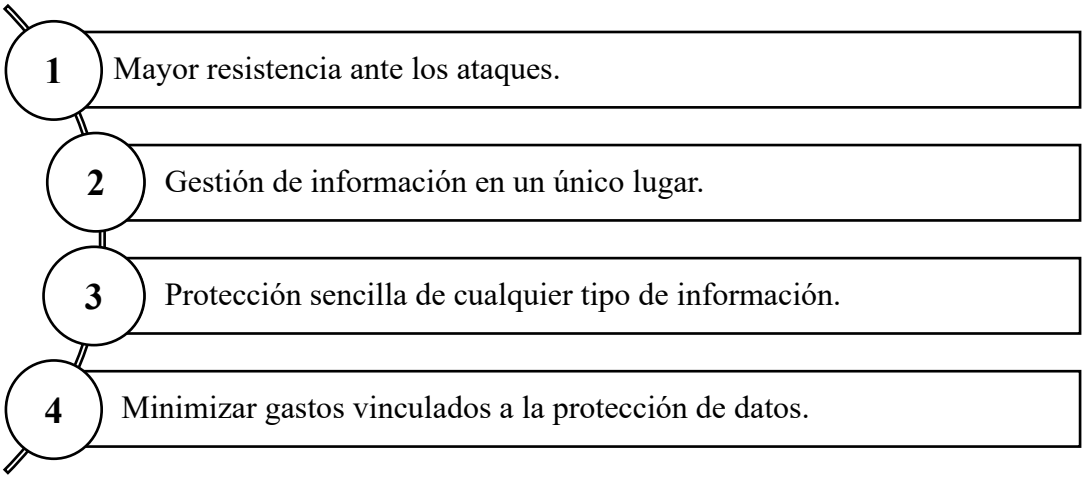
Limitar el acceso al inicio (desde la BIOS), al sistema operativo, a los programas y a los archivos.	Garantizar que los usuarios puedan trabajar sin una supervisión detallada.	Garantizar el uso de datos, archivos y programas adecuados.

Elaborado por: Sánchez (2023)
Fuente: Menéndez (2022)

1.2.7. Sistema de Gestión de la Seguridad de la Información (SGSI)

Es un método estructurado para administrar los datos privados o sensibles de una compañía de manera que se mantenga protegida. Esto implica a los individuos, los sistemas de TI y los procedimientos mediante el empleo de un método para la gestión de riesgos. Con el aumento de las violaciones de datos en el entono digital, el SGSI se vuelve fundamental para fortalecer la ciberseguridad de una organización. Según Fletcher (2019) algunas de las ventajas del SGSI son las siguientes:

Ilustración 11.- Ventajas del SGSI



Elaborado por: Sánchez (2023)
Fuente: Fletcher (2019)

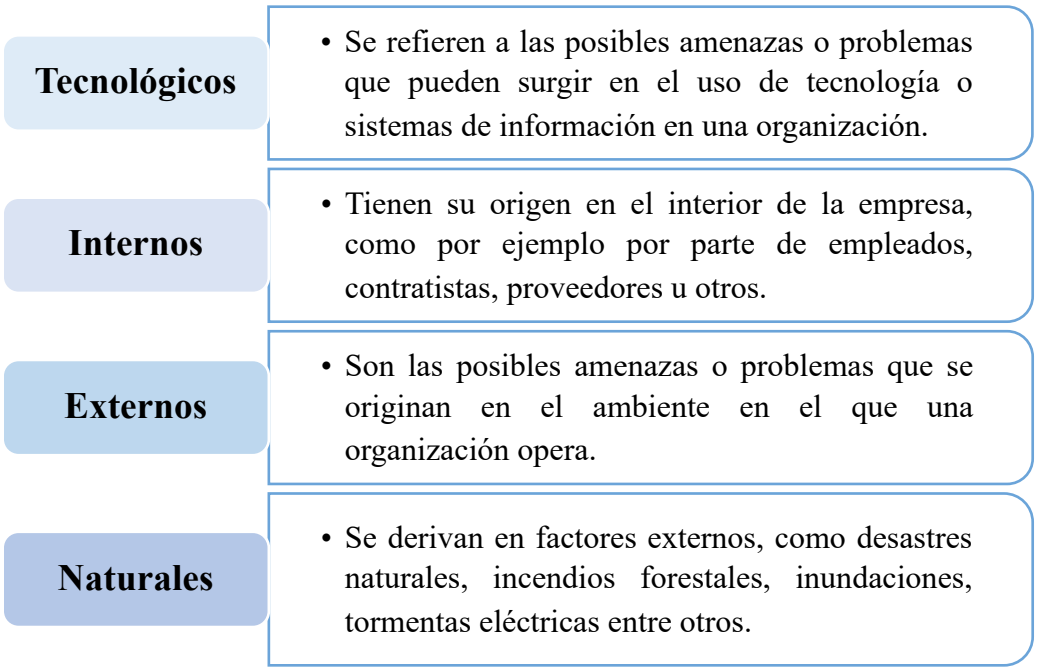
1.2.8. Administración de riesgos

Es el procedimiento de reconocer, valorar y controlar los peligros asociados a los sistemas informáticos de una organización que se somete a auditoría. El objetivo es garantizar la integridad, resguardo de los informes y sistemas informáticos (Vieites, 2011).

1.2.8.1.Tipos de riesgos

Según Vieites (2011) dentro de las organizaciones se identifican cuatro tipos de riesgos que se detallan a continuación:

Ilustración 12.- Clasificación de riesgos



Elaborado por: Sánchez (2023)
Fuente: Vieites (2011)

1.2.8.2.Tipos de vulnerabilidades

De acuerdo con Baca (2016) los tipos de vulnerabilidades que se deben de tomar en cuenta son ocho:

Tabla 3.-Tipos de vulnerabilidades

VULNERABILIDADES	DESCRIPCIÓN
Física	Se refiere a la exposición y la habilidad de la estructura para resistir daños y mantener su integridad en caso de tales eventos.
Natural	Se refiere a la exposición de un sistema natural (zona geográfica) a amenazas o peligros que surgen de la propia naturaleza, como terremotos, ciclones, inundaciones, sequías, entre otros.
Hardware	Debilidad en la seguridad de un sistema informático que surge a partir de algún componente físico del propio sistema.
Software	Se refiere a la presencia de fallas, debilidades o errores en el código de un programa informático o aplicación.
Medios de almacenaje	Debilidades o fallos que pueden surgir en los medios físicos o magnéticos que se emplean para guardar datos, como los discos duros, memorias USB, o discos ópticos.
Comunicación	Se refiere a las debilidades o fallas en los procesos de comunicación (divulgación) entre individuos o sistemas, que pueden ser explotadas por atacantes para llevar a cabo acciones malintencionadas.
Humana	Se refiere a la condición natural de fragilidad y exposición de los seres humanos ante distintos factores que pueden afectar su bienestar, tanto físico como psicológico y social.

Elaborado por: Sánchez (2023)
Fuente: Baca (2016)

1.2.9. Definiciones básicas

Tabla 4.-Definiciones básica

Activo de información
Recursos que utiliza una organización para llevar a cabo sus operaciones. La información es un activo de la empresa y de hecho es el que más protección requiere. Ejemplos: personal, infraestructura física, hardware y software, datos, logo, equipos, instalación física, servicios y aplicaciones.
Vulnerabilidad
Son las inseguridades a las que enfrenta el activo, pueden ser atribuidas tanto a problemas tecnológicos como a problemas de procedimientos.
Amenaza
Circunstancias o eventos maliciosos, como virus informáticos, software malicioso, ataques de phishing, entre otros.
Impacto
Es el impacto negativo que ocurre cuando una amenaza se materializa en un activo. Se mide con el porcentaje de degradación que afecta al activo, si este porcentaje es superior al 100%, se trata de la pérdida total del activo.
Probabilidad de Ocurrencia
La posibilidad de que ocurra un incidente se puede estimar utilizando datos objetivos, como información sobre incidentes pasados dentro de la empresa, o utilizando datos subjetivos, como información de otras empresas o expertos.
Riesgo Informáticos
Es el resultado del impacto y la probabilidad de que ocurra un evento. Se estima cuantitativamente. Impacto x Probabilidad = Riesgo

Elaborado por: Sánchez (2023)
Fuente: Ramos (2020)

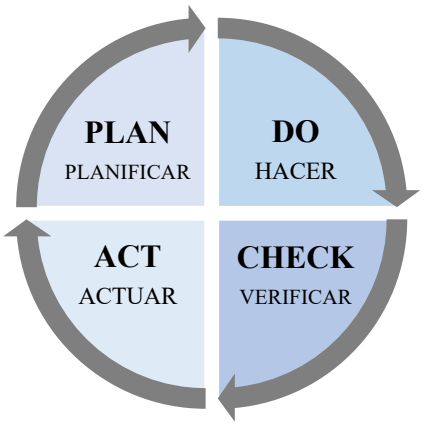
1.2.10. Marco legal

1.2.10.1. Norma ISO 27000

Alrededor del mundo, existen diversos factores que afectan el sistema de la información, lo cual ha generado la necesidad de implementar normas que brinden protección al sistema. Es por eso por lo que, se han creado las normas ISO 27000, que son estándares de seguridad para las empresas. Según Baena et al. (2019) estas normas

permiten la ejecución de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo la metodología del ciclo Deming o PDCA.

Ilustración 13.- Ciclo deming o PDCA



Elaborado por: Sánchez (2023)
Fuente: Baena et al. (2019)

Plan (Planificar): Corresponde a la primera fase en la elaboración del SGSI, donde se realiza el reconocer los peligros que impactan en la protección de la información. Esto implica realizar una evaluación cuantitativo y cualitativo de los peligros detectados, además de planificar la respuesta y los controles necesarios para mitigarlos.

Do (Hacer): En la segunda fase se efectúa y se práctica el SGSI tal como se definió en la fase anterior.

Check (Verificar): En la tercera fase se lleva a cabo una revisión y evaluación para comprobar su eficacia. Si se identifican deficiencias se proponen posibles mejoras.

Act (Actuar): En la última fase, se realizan ajustes en los procesos para así lograr los objetivos determinados inicialmente.

1.2.10.2. Norma ISO 27001

La norma ISO 27001 es un modelo registrado a nivel global que establece los requerimientos esenciales para efectuar, conservar y perfeccionar permanentemente un Sistema de Gestión de Seguridad de la Información (SGSI). La norma define como objetivo asegurar que la información de una organización se mantenga protegida, completa y accesible, incluyendo el manejo de los riesgos asociados a la misma. La

norma ISO 27001 instaura procedimientos para la gestión de activos de información, la seguridad física y de los recursos humanos, el registro de acceso, la seguridad de la red y las comunicaciones, la adquisición y tratamiento de sistemas, la gestión de incidentes y el sostenimiento ininterrumpido de las operaciones comerciales (Chicano, 2015).

1.2.10.3. Norma ISO 27002

Esta norma tiene como objetivo proporcionar una guía instaurar, ejecutar, conservar y perfeccionar la seguridad de los informes en las empresas, y contiene un grupo de medidas de seguridad que se pueden aplicar a los sistemas de información mediante un total de 114 controles organizados en 14 áreas temáticas y 35 metas de control (Cuniglio, 2016).

Tabla 5.- Beneficios ISO 27002

Beneficios para la empresa	Principales Ítems
- Mejor concienciación sobre protección de datos. - Mayor vigilancia en activos. - Oportunidad de identificar y corregir debilidades. - Mejor organización con los procesos. - Implementación de políticas de control.	- Políticas de seguridad de la información. - Gestión de activos. - Seguridad física y del medio ambiente. - Control de acceso. - Mantenimiento de sistemas.

Elaborado por: Sánchez (2023)
Fuente: ABNT (2005)

1.2.10.4. Norma ISO 31000:2009

Esta norma proporciona una guía con el fin de reconocer, examinar y valorar los riesgos y para diseñar e implementar medidas que permitan gestionarlos de manera efectiva. Al implementar las pautas y los principios rectores de la norma ISO 31000 internamente de su compañía, pueden aumentar la eficacia operativa, el gobierno y la confianza de las partes interesadas al tiempo que minimizan las pérdidas potenciales (ISO, 2009).

CAPÍTULO II

METODOLOGÍA

2.1.Descripción del entorno

2.1.1. Unidad de análisis

En el proyecto integrador, se cumplió con el diseño de controles de seguridad informática para el sistema de información en el departamento de Administración, específicamente en el área de Contabilidad. Se eligió a la empresa Telpronet de la ciudad de Ambato como unidad de análisis. Se evaluaron las vulnerabilidades, amenazas y riesgos a los que se encuentran exhibidos los activos de información, los cuales son elementos clave para la marcha de la empresa. Entre los activos más trascendentales se encontraron los documentos internos, sistemas de información, software contable, marcas, entre otros.

Los sistemas de información fueron evaluados debido a los constantes ataques informáticos en los últimos años, así como también las vulnerabilidades en el registro de datos y reportes contables. En otras palabras, los activos de información son esenciales para mantener el correcto desempeño de la compañía y alcanzar los objetivos señalados por la alta dirección. Por lo tanto, es necesario analizarlos para determinar su nivel de importancia y a través de los controles preventivos, detectivos y correctivos que la empresa ha utilizado ante las vulnerabilidades aplicar las políticas necesarias para protegerlos de manera adecuada. La intención de este proyecto fue diseñar controles para el Sistema de Gestión de Seguridad de la información (SGSI) fundamentados en la norma ISO 27001, estas directrices proporcionaron instrucciones sobre cómo aplicar medidas técnicas y políticas internas para proteger la integridad, confidencialidad y disponibilidad de los datos de la empresa.

2.1.2. Fuentes y técnicas de recolección de información

2.1.2.1.Fuentes de información primaria

Para el proyecto integrador se recopilaron datos de fuentes primarias, lo que significa que se obtuvo directamente la información con el personal de la empresa. Con base en esto, se aplicó la técnica de la encuesta para recopilar datos primarios de la empresa

con la gerente de Telpronet, el encargado del área de Sistemas Informático, el asistente contable y el asistente administrativo. Esto permitió obtener antecedentes sobre cómo se ha gestionado los controles de los activos de información, así como también conocer cómo las amenazas y riesgos han afectado negativamente el desarrollo de la compañía. Para finalizar se utilizó la técnica de la observación realizada a los activos de información permitiéndonos conocer a profundidad los tres principios fundamentales.

Tabla 6.-Personas entrevistadas y encuestadas

Nombres	Cargo	Departamento
Tannia Castillo	Gerente de la empresa	Gerencia
Rommel Guano	Técnico de Soporte Informático	Sistemas Informáticos
Karen Ponluisa	Asistente Administrativa	Comercial y Atención al Cliente
Fernanda Villacrés	Asistente Contable	Administrativo

Elaborado por: Sánchez (2023)

Encuesta. - La técnica de la encuesta se realizó el 7 de noviembre de 2023 a las 11h00 en las oficinas de Telpronet. Fue llevada a cabo de manera presencial a las personas involucradas en las áreas de estudio con el objetivo de conocer el nivel de protección de la información de la compañía.

Cuestionario: En la presente investigación se utilizaron preguntas de opción ternaria, es decir, el encuestado tuvo que seleccionar una de las tres opciones disponibles, tal como se evidencia en la tabla 7:

Tabla 7.- Preguntas del cuestionario y escalas

Preguntas	Escala
1.- ¿Disponen de un inventario de activos de información actualizado?	**1.-** Si; **2.-** No; **3.-** Parcial
2.- ¿La empresa cuenta con políticas de Seguridad de la Información?	**1.-** Si; **2.-** No; **3.-** Parcial
3.- ¿Está de acuerdo en aplicar las Normas de Seguridad de Información en la empresa?	**1.-** Si; **2.-** No; **3.-** Parcial
4.- ¿En el último año se ha impartido una capacitación en cuanto a la seguridad de la información?	**1.-** Si; **2.-** No; **3.-** Parcial

5.- ¿Se realiza mantenimiento preventivo a los equipos de la institución?	**1.-** Si; **2.-** No; **3.-** Parcial
6.- ¿Se realizan copias de seguridad del software contable?	**1.-** Si; **2.-** No; **3.-** Parcial
7.- ¿En los últimos 6 meses ha sido víctima de un ataque o virus?	**1.-** Si; **2.-** No; **3.-** Parcial
8.- ¿Las computadoras de la empresa tienen instalado un antivirus actualizado y con licencia?	**1.-** Si; **2.-** No; **3.-** Parcial
9.- ¿El software contable está programado para un cierre automático al inhabilitarse la sesión de un usuario?	**1.-** Si; **2.-** No; **3.-** Parcial
10.- ¿Existe una política interna para la creación y asignación de contraseñas a usuarios para el sistema contable?	**1.-** Si; **2.-** No; **3.-** Parcial
11.- ¿La empresa cuenta con un plan de contingencia ante posibles desastres?	**1.-** Si; **2.-** No; **3.-** Parcial
12.- ¿Para el acceso a las instalaciones la empresa mantiene algún tipo de seguridad?	**1.-** Si; **2.-** No; **3.-** Parcial

Elaborado por: Sánchez (2023)
Fuente: Cepreven (2023)

Entrevista. - La técnica de la entrevista se llevó a cabo el 7 de noviembre de 2023 a las 12h00 en las oficinas de Telpronet de manera presencial. El objetivo de la entrevista fue conseguir información sobre la seguridad de los activos.

Guía de entrevista. - Se realizaron un total de 18 preguntas, con una duración aproximada de media hora, abarcando diferentes categorías vinculadas con la seguridad de la información. Esto permitió obtener información clara y precisa. Posteriormente, en la tabla 8 se detallan las preguntas que se hicieron durante la entrevista:

Tabla 8.- Preguntas de la entrevista y sus categorías

Preguntas	Dimensión o categoría
1.- ¿Qué conocimientos tiene sobre la seguridad de la información?	Conocimiento acerca de la seguridad de la información
2.- ¿Cuál es su nivel de comprensión sobre la norma ISO 27001?	Conocimiento acerca de la seguridad de la información
3.- ¿Se lleva a cabo la evaluación y prevención de riesgos en relación con la seguridad de la información?	Conocimiento acerca de la seguridad de la información

4.- ¿Qué software contable utiliza y cómo calificaría la utilización del mismo?	Conocimiento acerca de la seguridad de la información
5.- ¿Se aplica políticas de seguridad para la información de las áreas administrativa, contable e informática?	Conocimiento acerca de la seguridad de la información
6.- ¿Existe la designación de una persona a cargo para crear los usuarios en los sistemas aplicativos que utiliza la empresa?	Políticas de seguridad de la información
7.- ¿Las cuentas de usuarios que están en período de vacaciones o que ya no trabajan en la empresa son bloqueadas de forma oportuna?	Políticas de seguridad de la información
8.- ¿Las claves de usuarios son creadas con fechas de caducidad?	Políticas de seguridad de la información
9.- ¿Se ha configurado con un mínimo de caracteres la creación de nuevas contraseñas?	Protección de datos
10.- ¿Los usuarios pueden ingresar al sistema contable desde cualquier dispositivo?	Protección de datos
11.- ¿Con qué periodicidad son cambiadas las contraseñas de usuarios?	Acceso a información confidencial
12.- ¿Se permite el acceso a la navegación de páginas no vinculadas con las de la empresa?	Acceso a información confidencial
13.- ¿Se puede utilizar el celular durante la jornada laboral?	Acceso a información confidencial
14.- ¿El administrador del gestor puede hacer modificaciones en la base de datos?	Administración de Sistemas
15.- ¿Se han ejecutado simulacros ante una caída del sistema contable?	Administración de Sistemas
16.- ¿Los equipos cuentan con la capacidad de memoria RAM y almacenamiento suficiente para evitar ralentización en las activades diarias del trabajo?	Activo de información
17.- ¿La empresa tiene registro de bitácoras por los mantenimientos a los equipos informáticos de la empresa?	Activo de información
18.- ¿Ha existido algún tipo de robo de información o un problema similar en la empresa?	Activo de información

Elaborado por: Sánchez (2023)
Fuente: Sánchez (2018)

2.1.3. Fases de desarrollo

Tabla 9.- Fases de desarrollo del diseño de controles de seguridad informática

Objetivos Específicos	Fase o etapa	Descripción
Realizar el inventario de activos de información de la empresa, identificando amenazas, vulnerabilidades y riesgos que se encuentren expuestos, para su respectivo nivel de tasación.	Análisis Preliminar	En la Fase I se realizó la documentación preliminar mediante entrevistas al personal para obtener una visión general de la empresa. Además, se realizó el levantamiento del inventario de activos de información con el objetivo de analizar y determinar su nivel de tasación a través de los tres principios básicos de la seguridad informática que son: confidencialidad, integridad, disponibilidad. De esta manera, se pudo conocer el grado de criticidad de cada activo.
Evaluar las amenazas y riesgos para la identificación de los posibles impactos que provoque la deficiencia en los controles de SGSI.	Ejecución	En la fase II se realizó una matriz en donde se evaluaron las amenazas y riesgos de cada activo de información con el objetivo de valorar los niveles de controles. Se utilizó la matriz de los activos de información y se aplicó la norma ISO/IEC 27000. Esto permitió ponderar a los controles existentes y determinar posibles acciones preventivos, detectivos o correctivos dependiendo de los casos analizados.
Establecer las políticas del SGSI conforme lo que establecido en la norma ISO/IEC 27000 para la seguridad informática y los controles aplicarse.	Comunicación	En la fase III se elaboró las políticas del SGSI siguiendo lo establecido en la norma ISO/IEC 27000, teniendo en cuenta las vulnerabilidades identificadas en la empresa. El documento fue dirigido a la gerente de Telpronet, quien es la responsable de analizar y decidir la aplicación de dichas políticas de seguridad con el fin de resguardar sus activos de información.

Elaborado por: Sánchez (2023)

Criterios de cada una de las fases

Fase I Análisis Preliminar

En este punto, se procedió a analizar tanto la entrevista como la encuesta realizada al personal de empresa, para ello se tomó en cuenta diversas áreas en donde se puede llegar a tener un contexto completo de la organización, entre las áreas que se tomó en cuenta fue el inventario de activos de información, políticas de la empresa, vulnerabilidad, ataques, robos de información entre otros. Todos estos parámetros enfocados a la norma ISO 2700.

Fase II Ejecución

En la fase II de igual manera se aplicaron las normas ISO para el análisis de los activos de información para ello se tomaron en cuenta diversos criterios especificados en la siguiente tabla 10:

Tabla 10.- Criterios para los 3 principios de la información

Valor del Activo	Confidencialidad	Integridad	Disponibilidad
5 (Muy Alto)	Únicamente el personal de alto rango tiene acceso a este tipo de información.	No se tolera pérdida o alteración en los componentes del activo.	El activo siempre deberá estar disponible.
4 (Alto)	Solo miembros de un proyecto particular pueden acceder a este tipo de información.	La vulneración del activo afectaría gravemente a la empresa.	El activo puede estar fuera de servicio durante un período máximo de una hora.
3 (Medio)	Solo el personal de ciertas áreas internas puede acceder a esta información confidencial.	La vulneración del activo afectaría considerablemente a la empresa.	El activo puede estar fuera de servicio durante un período máximo de un día.
2 (Bajo)	Solo el personal ABC tiene autorización para acceder a esta información de uso interno.	La vulneración del activo afectaría parcialmente a la empresa.	El activo puede estar fuera de servicio durante un período máximo de una semana.
1 (Muy Bajo)	La información está disponible para cualquier tipo de persona.	El activo puede soportar una pérdida o alteración total de sus componentes.	Se acepta que el activo este indisponible por un periodo de tiempo indefinido.

Elaborado por: Sánchez (2023)
Fuente: Araujo (2019)

Conjuntamente se estableció una escala de evaluación del nivel de tasación de los activos de información, tal como se muestra en la tabla 11.

Tabla 11.- Escala del nivel de tasación

Valor del Activo	Nivel de Tasación
4,001 - 5,000	Muy Alto
3,001 - 4,000	Alto
2,001 - 3,000	Medio
1,001 - 2,000	Bajo
1,000 - 1,000	Muy Bajo

Elaborado por: Sánchez (2023)
Fuente: Araujo (2019)

En el apartado de la valoración de los controles actuales de la compañía se utilizó la siguiente escala en donde podemos describir de mejor manera el control, es decir si cumple o no con las normas, tal como se detalla en la tabla 12:

Tabla 12.- Calificación de los controles

Calificación	Significado
3	Aceptable
2	Mejorable
1	Deficiente
0	Muy deficiente

Elaborado por: Sánchez (2023)
Fuente: Bestratén (2013)

De igual forma para la evaluación del nivel de riesgo se utilizaron diversos parámetros para poder calificar el nivel de probabilidad, impacto que pudiera tener cada activo de información. Los criterios para tomarse en cuenta se especifican en la siguiente tabla 13:

Tabla 13.- Niveles probabilidad e impacto

	Probabilidad	**Impacto**
5	Altamente Probable	Muy alto
4	Muy probable	Alto
3	Probable	Medio
2	Poco Probable	Moderado
1	Improbable	Bajo

Elaborado por: Sánchez (2023)
Fuente: Culture (2023)

La tabla 14 detalla la escala utilizada para establecer el nivel de riesgo de los activos de información en la compañía.

Tabla 14.- Calificación de los controles

Nivel de riesgo= Probabilidad * impacto	
Muy Alto	Mayor o igual que 20
Alto	Mayor o igual que 10 y menor que 20
Medio	Mayor o igual que 5 y menor que 10
Moderado	Mayor o igual que 3 y menor que 5
Bajo	Menor que 3

Elaborado por: Sánchez (2023)
Fuente: Culture (2023)

CAPÍTULO III

DESARROLLO

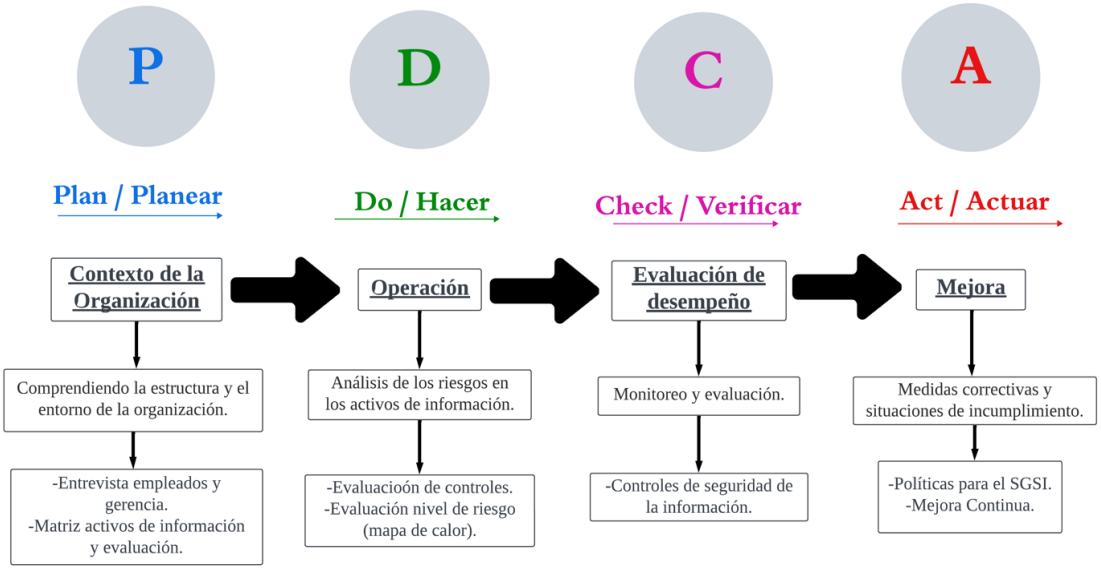
3.1.Desarrollo de los controles de seguridad de la información

En los apartados anteriores del proyecto integrador se explicaron las razones por las cuales se diseñaron los controles de seguridad informática en la empresa Telpronet. El objetivo fue identificar las vulnerabilidades, amenazas y riesgos de la empresa para evaluar y determinar cuál de los activos de información es el más crítico. Como resultado, se elaboró un manual de políticas basado en la serie de la norma ISO 27000 para gestionar adecuadamente los activos de información y aumentar su seguridad en la empresa.

En la primera fase, denominada "Análisis Preliminar", se realizó una entrevista al personal de la empresa y se creó una matriz de los activos de información para determinar su nivel de criticidad. Esto brindó una visión general de la empresa y permitió identificar sus fortalezas y debilidades. En la segunda fase, denominada "Ejecución", se analizaron todos los activos, evaluando sus vulnerabilidades, amenazas, riesgos y los controles implementados en cada uno. Esto permitió determinar la posibilidad de ocurrencia y el impacto potencial en caso de robo de información. Con estos resultados, se obtuvo el nivel de riesgo de cada activo, lo que facilitó la creación de un mapa de calor para distinguir los riesgos bajos, medios, altos y muy altos a los que se enfrentaba la empresa. Finalmente, en la tercera fase, denominada "Comunicación", se elaboró y socializó el manual de políticas del Sistema de Gestión de Seguridad de la Información (SGSI) apoyado en la norma ISO 27000. Este manual resaltó la importancia de los activos de información en la empresa y la necesidad de adoptar procesos formales y definir responsabilidades.

Cabe mencionar que la norma ISO 27001 es ajustable a cualquier prototipo de negocio, lo que le permite obtener beneficios y cumplir con sus objetivos de seguridad de la información. Al implementar la norma ISO 27001, las compañías pueden proteger la confidencialidad, integridad y disponibilidad de la información, y demostrar su compromiso de gestionar y proteger proactivamente sus activos de información.

Ilustración 14.- Relación entre el modelo PDCA y la ISO 27001



Elaborado por: Sánchez (2023)
Fuente: Moreno (2020)

3.1.1. Análisis preliminar

La recolección de información fue de vital importancia, ya que permitió obtener una visión general de la empresa. Esto se logró a través de la realización de entrevistas al personal de la empresa que incluyó, al ingeniero en Sistemas, la gerencia y los empleados de los departamentos operativos. Durante estas entrevistas, se determinó los distintos controles y procedimientos que se aplican a los activos de información. También se evaluó las normas de seguridad que emplean actualmente en la empresa y los medios utilizados para llevar a cabo las actividades diarias, como software o dispositivos tecnológicos. Esta recopilación de información resultó fundamental para el proyecto integrador.

Para elaborar las preguntas de la entrevista, se fundó en los estándares de la seguridad informática. El objetivo principal fue comprender a fondo la gestión de los activos de información en la empresa, considerando que son útiles para la operatividad de esta esto es: hardware, software contable, redes de comunicación interna, documentación de archivo, entre otros. Tomando en cuenta que las actividades diarias de la empresa se desarrollan a través del manejo de la tecnología, recae importante considerar la información que se emite producto de esta utilización. Durante el proceso, se percibió los niveles de conocimiento de los entrevistados en cuanto a la norma y lo que representa para el SGSI (Sistema de Gestión para la seguridad de la información).

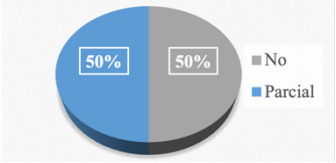
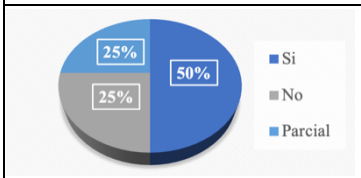
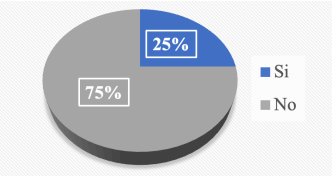
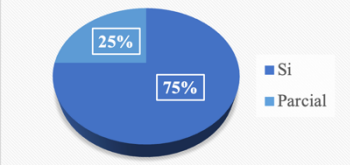
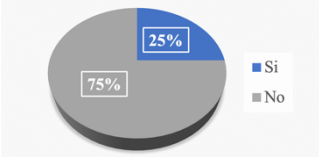
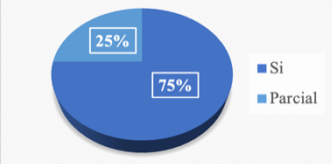
Tabla 15.- Análisis de la entrevista

Tannia Castillo	Rommel Guano	Fernanda Villacrés	Karen Ponluisa
Conocimiento acerca de la seguridad de la información			
Muy básico, solo he escuchado la ISO 27001.	Si tengo conocimientos considerables.	Bueno, debemos guardar la información (respaldo).	Lo más básico, trata sobre proteger la información.
Interpretación: Según las personas entrevistadas manifiestan que el conocimiento que tienen sobre el tema es básico, siendo esto un factor que podría dar paso a correr el riesgo de ser víctimas de robo de información u otros delitos cibernéticos.			
Políticas de la seguridad de la información			
No se aplica políticas sino como normas.	Si a través del Ing. en Sistemas.	La información se sube a la nube.	Solo aplicamos a lo que es a la nube.
Interpretación: Según las respuestas de los entrevistados se puede decir que, existe diferentes niveles de conocimiento debido a que por una parte mencionan que, si aplican políticas, pero por otra parte solo mencionan que aplican normas, y en el mejor de los casos respaldan su información en la nube.			
Protección de Datos			
Contraseñas poseen un número mínimo de caracteres.	No se ha configurado un mínimo de caracteres en contraseñas.	No tengo conocimiento.	En contraseñas se puede escribir lo que se desea.
Interpretación: Existe una falta de consenso o falta de políticas claras en cuanto a la seguridad de contraseñas ya que por una parte mencionan que si está configurado con un mínimo de caracteres mientras que otros mencionan que no tienen parámetros.			
Acceso a información confidencial			
Si, ya que el celular forma parte de las herramientas de trabajo.	Si se tiene acceso a todo tipo de páginas.	Si tenemos acceso a todo tipo de páginas.	Si, no hay problema.
Interpretación: Los empleados tienen total libertad para navegar por páginas no vinculadas a la empresa, lo que sería beneficioso siempre y cuando cuenten con una política y restricción establecidas por la empresa para su uso correcto.			
Administración de Sistemas			
El administrador es el único que realiza cambios.	Mas o menos.	Si.	Si, realiza cambios sin problema.
Interpretación: Se garantiza el principio de integridad de datos y se previene los cambios no autorizados, lo que indica que si se cumple la norma ISO 27000.			
Activo de Información			
Si, una suplantación de identidad por parte de un trabajador. Ofreció el logo en otra empresa.	No ha existido problemas.	No ha existido problemas.	Por el momento no.
Interpretación: Se puede interpretar que la Gerente ha decidido mantener la información del robo de manera confidencial para evitar la preocupación en los empleados o también para que esta información no sea divulgada y afecte negativamente a la imagen de la empresa, por lo que la administración considera importante la reputación empresarial ante sus clientes.			

Elaborado por: Sánchez (2023)

De igual manera, en lo que respecta a la encuesta se llevó a cabo a los empleados de la compañía con el fin de reafirmar las respuestas obtenidas en la entrevista. Esto permitió obtener respuestas verídicas que ayudaron a tener un diagnóstico más preciso de la empresa en la que se realizó el proyecto integrador. A través de la encuesta, se pudo explorar diferentes aspectos, como el conocimiento de la entidad, los controles preventivos, las normas, las amenazas y vulnerabilidades a los que se encuentra expuesto los activos de información dentro de la compañía en los departamento administrativo, técnico y proyectos y comercial.

Tabla 16.- Análisis de la encuesta

Gráfico	Análisis
Inventario de Activos de Información / Mantenimiento a los equipos de la institución	
	Existe una división equitativa entre los encuestados debido a la falta de comunicación, por lo que indican que los activos de información se encuentran actualizados, pero de manera parcial, de igual forma existen deficiencias en el mantenimiento preventivo.
Políticas de Seguridad de la Información / Copias de Seguridad Software Contable	
	Existe limitación en la uniformidad con respecto a la ejecución de políticas de seguridad y copias de seguridad en el software contable, por lo que los encuestados no coinciden, siendo la principal causa su poca difusión o la importancia que le dan los empleados a la información.
Normas de Seguridad de la Información / Capacitación relacionada a la Seguridad de la Información	
	La opinión de todos los encuestados coincide en la importancia y la necesidad de implementar las normas de seguridad en la empresa, sin embargo, la mayoría de encuestados no ha recibido instrucción en tema de seguridad de la información debido a, la falta de un cronograma planificado de capacitaciones ya que el tiempo de sus horarios de trabajo son ajustados al requerimiento de sus clientes.
Ataques informáticos, virus o códigos maliciosos/ Instalación de antivirus actualizado y con licencia/	
	Según los datos se puede decir que, en los últimos 6 meses la empresa ha tomado medidas de seguridad efectivas, por lo que no se ha evidenciado ataques informáticos, pudiéndose deber a la importancia de mantener un antivirus actualizado debido al control preventivo que este complementa la seguridad del hardware.
Sistema contable con función de Log Out/ Política para la creación de usuario y contraseña	
	La falta de programación para el cierre automático en el software contable se debe a una falta de políticas en cuanto al riesgo que puede ocasionar el robo de este tipo de información.
Seguridad física en el acceso a instalaciones / Plan de contingencias	
	La mayor parte de los encuestados consideran necesario e importante la seguridad física para el paso a la infraestructura, aunque hay quienes indican que se debe mejorar la seguridad física a través de un plan de contingencias.

Elaborado por: Sánchez (2023)

3.1.2. Ejecución

3.1.2.1.Activos de información

Considerando la criticidad de seguridad en cada activo de información, según las respuestas obtenidas tanto en la entrevista como en la encuesta, se constató que la empresa no tenía un inventario actualizado de activos de información. Por lo tanto, se procedió a cumplir con el objetivo 1 del proyecto integrador, que consistía en efectuar el inventario a través de una lista de activos de información, a los cuales se les asignó una calificación con base a los tres principios según lo que establece la norma ISO 27000. Se procedió a asignar una calificación al activo en cuanto a la confidencialidad para lo cual, se consideró a los usuarios que tienen acceso al activo. Para el principio de Integridad se ponderó de acuerdo con la tolerancia del activo, es decir, cómo la vulneración del activo afecta a la empresa, o si solo causa un impacto mínimo. Finalmente, para el principio de disponibilidad se consideró el tiempo en que el activo puede estar indisponible o si fuese el caso estar siempre a disposición de las personas responsables. Después de ponderar los tres principios se procedió a calcular el valor promedio, aquellos valores por encima de 4 se consideran "muy alto", los que están por encima de 3 se consideran "alto", los que son mayores de 2 se consideran "medio", los que sobrepasan a 1 se consideran "bajo" y los iguales a 1 se consideran "muy bajo". Esto permitió determinar el nivel de tasación de cada activo y conocer cuáles son los más críticos en la empresa, delimitando así su nivel de importancia.

Tabla 17.- Tasación de los activos de información

Activo	Descripción del Activo	Tipo de activo	Confidencialidad	Integridad	Disponibilidad	Valor	Nivel de tasación (criticidad)
Software Contable	SEFAC	Software	3	4	5	**4,00**	**Alto**
Redes sociales	Facebook, Instagram, X	Software	1	3	3	**2,33**	**Medio**
Página web	www.telpronet.com	Software	1	3	4	**2,67**	**Medio**
Correo Electrónico	telpronet@hotmail.com	Software	2	3	3	**2,67**	**Medio**
Sistema de Red	Wifi y cable	Software	2	4	5	**3,67**	**Alto**
Computadoras de escritorio, Laptop	Sistema Windows 10 de 64 bits	Físico	2	5	5	**4,00**	**Alto**
Impresora	Epson TM-T20II / Epson 3L95 / RICOH MP C3003	Físico	2	4	4	**3,33**	**Alto**
TV	Marca Hyundai 32"	Físico	2	3	3	**2,67**	**Medio**
Router	TOTOLINK 720R	Físico	3	4	5	**4,00**	**Alto**
Terminal de línea Óptica	ONU HW	Físico	3	4	5	**4,00**	**Alto**
Regulador de voltaje	PowestRefriline	Físico	2	4	5	**3,67**	**Alto**
Equipo Biométrico	ZK 9500	Físico	4	5	5	**4,67**	**Muy Alto**
UPS (Sistema de Alimentación Ininterrumpida)	15KVA	Físico	2	4	5	**3,67**	**Alto**
Cámaras de Seguridad	Hikvision Hd	Físico	3	5	5	**4,33**	**Muy Alto**
Carpetas físicas	(Contratos, clientes, facturas, SRI)	Físico	2	4	4	**3,33**	**Alto**
Pendrives	Flash memory	Físico	2	3	3	**2,67**	**Medio**
Personal	Gerente, Ing. Contabilidad, Ing. Administrativo, Ing. En Sistemas	Personas	5	4	3	**4,00**	**Alto**

Elaborado por: Sánchez (2023)
Fuente: Vidaline (2009)

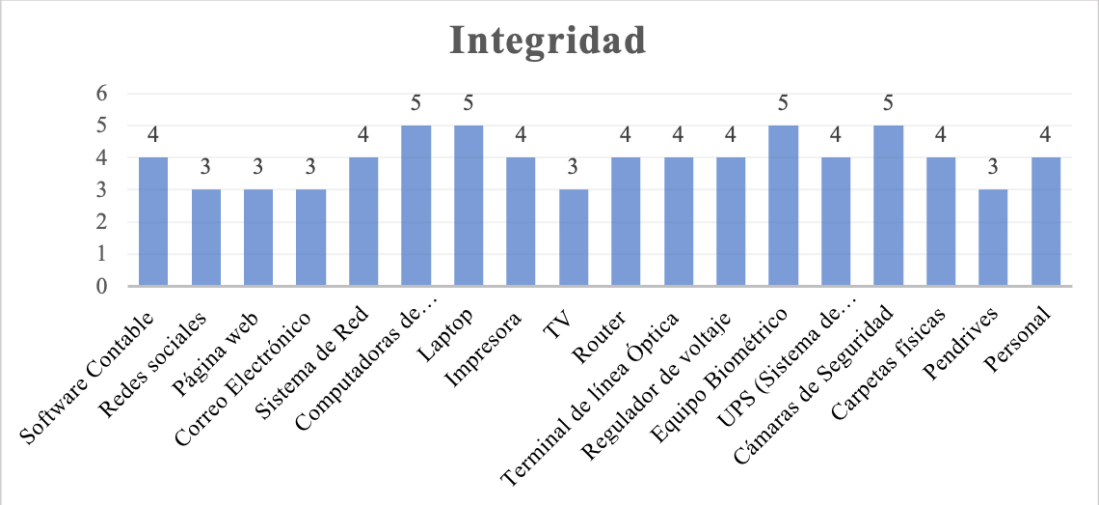
En relación con el principio de la Confidencialidad, se pudo observar que el personal es un activo de información muy importante, ya que conoce a fondo la operatividad interna como, por ejemplo: datos financieros, estrategias de comerciales, secretos comerciales, entre otros. Esto es especialmente relevante en un entorno empresarial donde la filtración de información puede ocasionar efectos negativos para la empresa. Es por esa razón que el acuerdo de confidencialidad a los empelados es de suma importancia, por lo que garantiza que los datos de la compañía se conserven protegidas, evitando así su divulgación no autorizada.

Ilustración 15.- Principio #1 "confidencialidad"

Elaborado por: Sánchez (2023)

Con respecto al principio de la Integridad, se pudo observar que las computadoras, laptops, equipo biométrico y cámaras de seguridad no pueden tolerar una alteración o modificación de estos, ya que afectaría de manera considerable a la empresa. La Integridad asegura que los datos sean exactos y coherentes. Cuando los activos de información mantienen un excelente nivel de integridad, se evita modificaciones no autorizadas como en este caso se pudiera dar en los equipos biométricos, de igual forma se evita la modificación de datos. Esto es esencial para asegurar que la información sea confiable y valiosa para la elección adecuada y las operaciones comerciales.

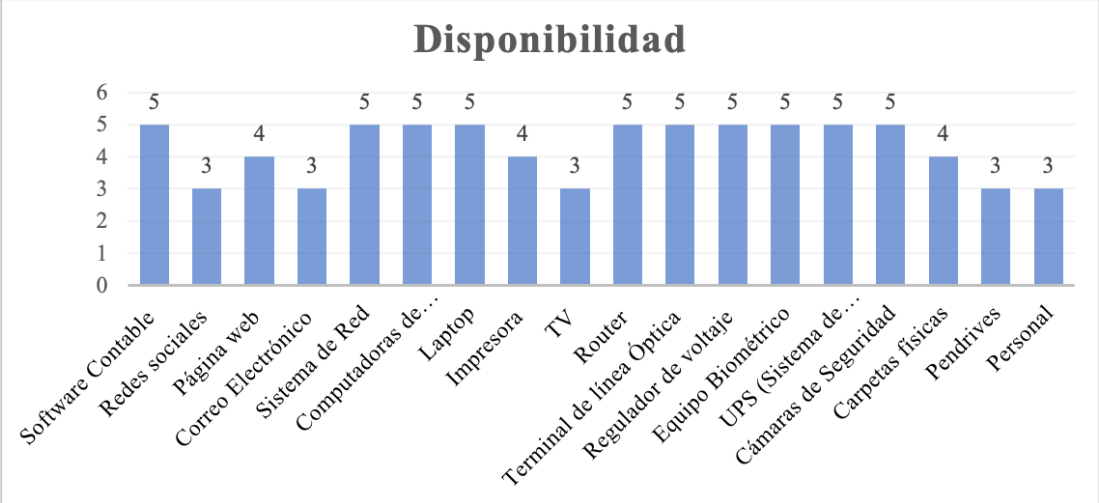
Ilustración 16.- Principio #2 “integridad”



Elaborado por: Sánchez (2023)

Conforme al principio de la Disponibilidad, se observó que la mayor parte de los activos de la empresa siempre deben estar con total disponibilidad, ya que, si uno de estos falla comprometería la actividad diaria de la empresa. La falta de disponibilidad de los activos de información puede causar retrasos en el trabajo, interrupciones en los procesos comerciales, pérdida de productividad, lo que puede afectar la habilidad de la compañía para atender las demandas de manera oportuna y eficiente. Además, la disponibilidad es esencial para brindar un buen servicio empresarial.

Ilustración 17.- Principio #3 “disponibilidad”



Elaborado por: Sánchez (2023)

3.1.2.2.Controles actuales de la empresa

En la tabla 18 se observó las posibles amenazas a las que la empresa podría enfrentarse por el manejo de la información a través de la tecnología. Es debido a esta razón que surge la necesidad de evaluar cada uno de los controles de los activos. Al elaborar una matriz da la posibilidad de gestionar de mejor manera los riesgos, el resguardo de datos y la obediencia a la norma y estándares aplicables. En este caso las vulnerabilidades que tiene los activos son las posibles causas que dan paso a que una amenaza se materialice. La amenaza por otro lado está relacionada con la probabilidad de que ocurra un evento y que cause daño a los activos como la pérdida de información, filtración de datos, acceso no autorizado entre otros. El riesgo se deriva de la combinación entre la vulnerabilidad y la amenaza, es decir, son los daños o pérdidas potenciales que se presentan en cada activo. Los controles actuales de la empresa son muy básicos por lo que la calificación del mismo en su mayor parte no sobrepasa de 2. En este caso la calificación más alta sería 3, y la mínima 0 que muestra que no existe ningún tipo de control asociado al activo.

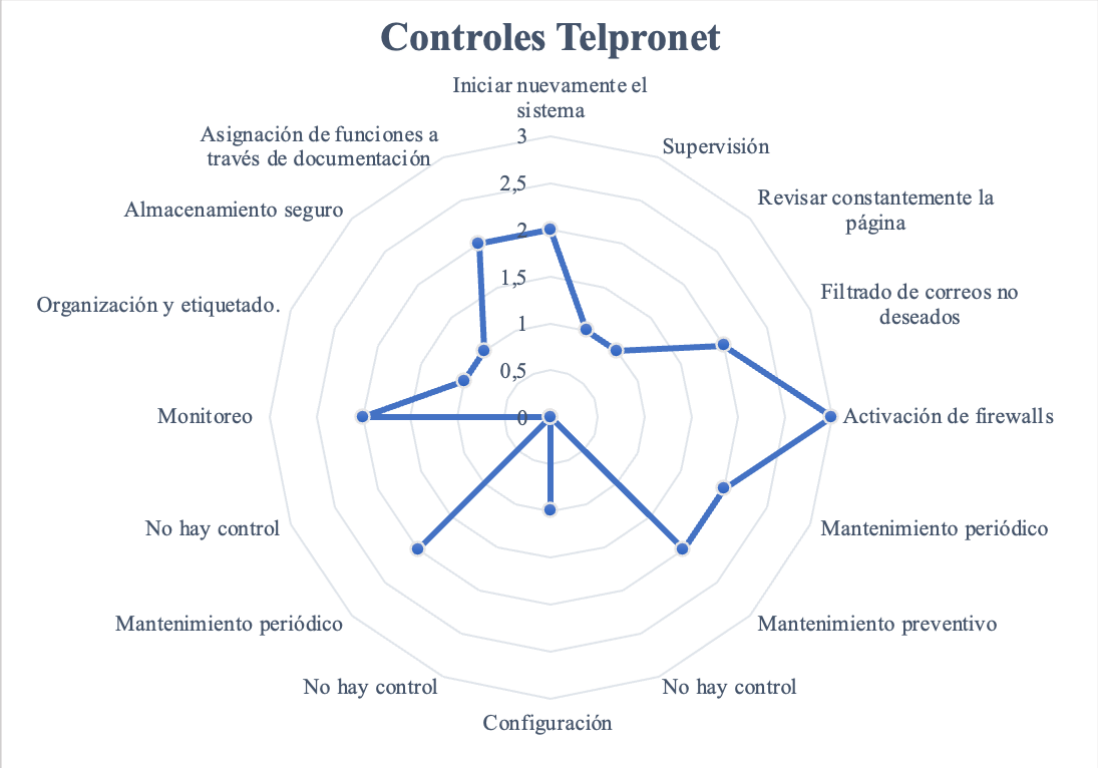
Tabla 18.- Controles actuales de la empresa

Activo	Vulnerabilidades	Amenazas	Riesgos	Controles Actuales	Calificación
Software Contable	Contraseñas con poca seguridad y sin ser cambiadas.	Personal no autorizado acceda al sistema.	Pérdida de información.	Iniciar nuevamente el sistema	2
Redes sociales	Contraseñas poco seguras.	Personas ajenas puedan hackear las redes.	Pérdida de redes, seguidores y publicidad.	Supervisión	1
Página web	Problemas en el acceso de la página web.	Ataques a la página web mediante códigos maliciosos.	Daño en la reputación de la empresa.	Revisar constantemente la página	1
Correo Electrónico	Contraseñas del correo sin alta seguridad.	Filtración de datos.	Pérdida o sustracción de datos corporativos	Filtrado de correos no deseados	2
Sistema de Red	No se cuenta con un paquete de software antivirus.	Infiltración de malware.	Afectación a PC y redes mediante pérdida de información.	Activación de firewalls	3
Computadoras de escritorio, Laptop	Configuración del equipo, contraseñas de inicio de sesión.	Programas o aplicaciones no se ejecuten adecuadamente.	Pérdida de información en aplicaciones o en la nube.	Mantenimiento periódico	2
Impresora	Falta de actualizaciones de firmware.	Acceso no autorizado a la impresora.	Daño o robo de impresora.	Mantenimiento preventivo	2
TV	Configuración de la TV.	Acceso no autorizado a la TV.	Robo de la TV.	No hay control	0
Router, Terminal de línea Óptica	Inestabilidad de conexión.	Fallas de conexión en los dispositivos.	Exposición de IP.	Configuración	1
Regulador de voltaje	Capacidad de regulación de voltaje.	Fallas en el circuito de regulación.	Daño de dispositivos conectados al regulador.	No hay control	0
Equipo Biométrico	Configuración del dispositivo.	Manipulación indebida del dispositivo.	Registros inexactos y exposición de datos biométricos.	Mantenimiento periódico	2
UPS	Fluctuaciones de voltaje.	Fallas en componentes eléctricos.	Daño a los dispositivos conectados.	No hay control	0
Cámaras de Seguridad	Capacidad de memoria baja.	Personas manipulen las cámaras de seguridad.	Pérdida de videos importantes.	Monitoreo	2
Carpetas físicas	Falta de registros de todas las carpetas.	Empleados deshonestos, factores externos.	Robo de datos e información de la empresa.	Organización y etiquetado.	1
Pendrives	Lugar no seguro para guardar.	Infección por malware o virus.	Pérdida de acceso a la información.	Almacenamiento seguro	1
Personal	Falta de cartas de confidencialidad en empelados.	Incumplimiento de leyes y reglamentos.	Suplantación de identidad.	Asignación de funciones.	2

Elaborado por: Sánchez (2023)

Los controles actuales en cuanto a la seguridad de la información se refieren con los que cuenta la compañía son muy básicos, por lo que puede dar paso a que ciertas vulnerabilidades sean explotadas por las amenazas por lo que el riesgo puede tener mayor impacto en los activos de la empresa. Al tener controles de seguridad básicos, se corre el riesgo de sufrir ataques cibernéticos, como el robo de datos, malware o intrusiones en la red. Además, la falta de medidas de seguridad adecuadas puede ocasionar la entrada no autorizada a aplicaciones y sistemas, lo cual podría comprometer la integridad de la información y amenazar la imagen corporativa de la compañía. Es fundamental que la empresa defina controles de seguridad robustos, implementando políticas y procedimientos adecuados, así como la utilización de herramientas y tecnologías de seguridad eficaces. Esto incluye el uso de firewalls, sistemas de detección de intrusiones, antivirus actualizados y la educación continua de los empleados en cuanto a buenas prácticas de seguridad, cifrado de datos y concientización de la importancia y relevancia de lo que este tema representa.

Ilustración 18.- Controles Telpronet



Elaborado por: Sánchez (2023)

3.1.2.3.Evaluación nivel de riesgo

En la tabla 19 se creó una matriz para exponer el nivel de riesgo por la materialización de las amenazas identificadas. La evaluación de riesgos de los activos de información consiste en determinar, analizar y evaluar los probables riesgos y amenazas que pueden inquietar la seguridad y disponibilidad de la información de la empresa. Esta evaluación se la realizó con un propósito en común que es, aplicar medidas preventivas, detectivas y correctivas para proteger los activos y de la misma forma minimizar los riesgos asociados.

La evaluación del riesgo implica varios pasos, como la identificación de las amenazas y riesgos de cada activo, a continuación, se procedió a asignar una calificación que va entre 1 y 5 dependiendo a la probabilidad de que algo suceda y el impacto que puede tener. Finalmente, la evaluación se obtuvo como resultado de la multiplicación entre la probabilidad de ocurrencia y el impacto, lo cual permitió determinar sus niveles de riesgo.

Tabla 19.- Probabilidad e impacto de los activos de información

No.	Activo	Amenazas	Riesgos	Probabilidad	Impacto	Evaluación Nivel de Riesgo	Ocurrencia del Riesgo
R1	Software Contable	Personal no autorizado acceda al sistema.	Pérdida de información.	3	5	15	Alto
R2	Redes sociales	Personas ajenas puedan hackear las redes.	Pérdida de redes, seguidores y publicidad.	4	4	16	Alto
R3	Página web	Ataques a la página web mediante códigos maliciosos.	Daño en la reputación de la empresa y reducción de la confianza del usuario.	4	3	12	Alto
R4	Correo Electrónico	Filtración de datos.	Pérdida o sustracción de datos corporativos.	3	4	12	Alto
R5	Sistema de Red	Infiltración de malware.	Afectación a PC y redes mediante pérdida de información.	2	3	6	Medio
R6	Computadoras de escritorio, Laptop	Programas o aplicaciones no se ejecuten adecuadamente.	Pérdida de información en aplicaciones o en la nube	3	5	15	Alto
R7	Impresora	Acceso no autorizado a la impresora.	Daño o robo de impresora.	3	3	9	Medio
R8	TV	Acceso no autorizado a la TV.	Robo de la TV.	3	3	9	Medio
R9	Router, Terminal de línea Óptica	Fallas de conexión en los dispositivos.	Exposición de IP.	3	3	9	Medio
R10	Regulador de voltaje	Fallas en el circuito de regulación.	Daño de dispositivos conectados al regulador de voltaje.	1	1	1	Bajo
R11	Equipo Biométrico	Manipulación indebida del dispositivo.	Registros inexactos y exposición de datos biométricos de empleados.	4	4	16	Alto
R12	UPS	Fallas en componentes eléctricos.	Daño a los dispositivos conectados.	1	1	1	Bajo
R13	Cámaras de Seguridad	Personas manipulen las cámaras de seguridad.	Pérdida de videos importantes.	4	4	16	Alto
R14	Carpetas físicas	Empleados deshonestos, factores externos.	Robo de datos o pérdida de información de la empresa.	4	5	20	Muy Alto
R15	Pendrives	Infección por malware o virus.	Pérdida de acceso a la información.	3	3	9	Medio
R16	Personal	Incumplimiento de leyes y reglamentos.	Suplantación de identidad.	3	4	12	Alto

Elaborado por: Sánchez (2023)

En la ilustración 19 se pudo identificar de mejor manera cuáles son los riesgos asociados al activo en cuanto al mayor y menor impacto que puede producirse en el caso de la materialización de la amenaza siendo los altos y más altos R1, R2, R4, R6, R11, R13, R14 y R16. Es decir, el mapa de calor permite apreciar de mejor forma las áreas en donde se debe poner mayor interés en cuanto a la aplicación de acciones preventivas, detectivas y correctivas con el fin de lograr una mejora constante en los procesos y cumplir de manera eficiente con la seguridad de la información.

Ilustración 19.- Mapa de calor

MAPA DE CALOR		Impacto				
		Bajo	**Moderado**	**Medio**	**Alto**	**Muy alto**
Probabilidad	**Valor**	1	2	3	4	5
Altamente probable	5					
Muy probable	4			R3	R2/R11/R13	R14
Probable	3			R7/R8/R9/R15	R4/R16	R1/R6
Poco probable	2			R5		
Improbable	1	R10/R12				

Elaborado por: Sánchez (2023)

A continuación, en la ilustración 20, se presenta gráficamente la evaluación del grado de riesgo asociado a los activos de información mediante un gráfico radial. En este gráfico, los puntos que se encuentran más alejados al centro representan un mayor riesgo de vulnerabilidad, mientras que los puntos más cercanos al centro indican una menor probabilidad de enfrentar riesgos.

Se observa que las carperas físicas son las más propensas a ser vulnerables de perder la información, por diversas razones como el deterioro por el tiempo, incendios, inundaciones u otros desastres naturales es por eso por lo que se debería tener los respectivos respaldos digitales que ayudarían a disminuir el riesgo de ocurrencia, existiendo también algunos activos que están considerados con una calificación alta

como: software contable, redes sociales, correo electrónico, computadoras y laptops, equipo biométrico, cámaras de seguridad y el personal de la empresa, por lo que se debería de igual manera prestar atención y priorizar los controles para su salvaguarda. Por otro lado, tanto el regulador de voltaje como el UPS son aquellos activos los cuales la probabilidad de ocurrencia es casi nula debido a que son dispositivos diseñados para proteger los equipos electrónicos y garantizar un suministro de energía estable.

Ilustración 20.- Nivel de riesgo de los activos

Elaborado por: Sánchez (2023)

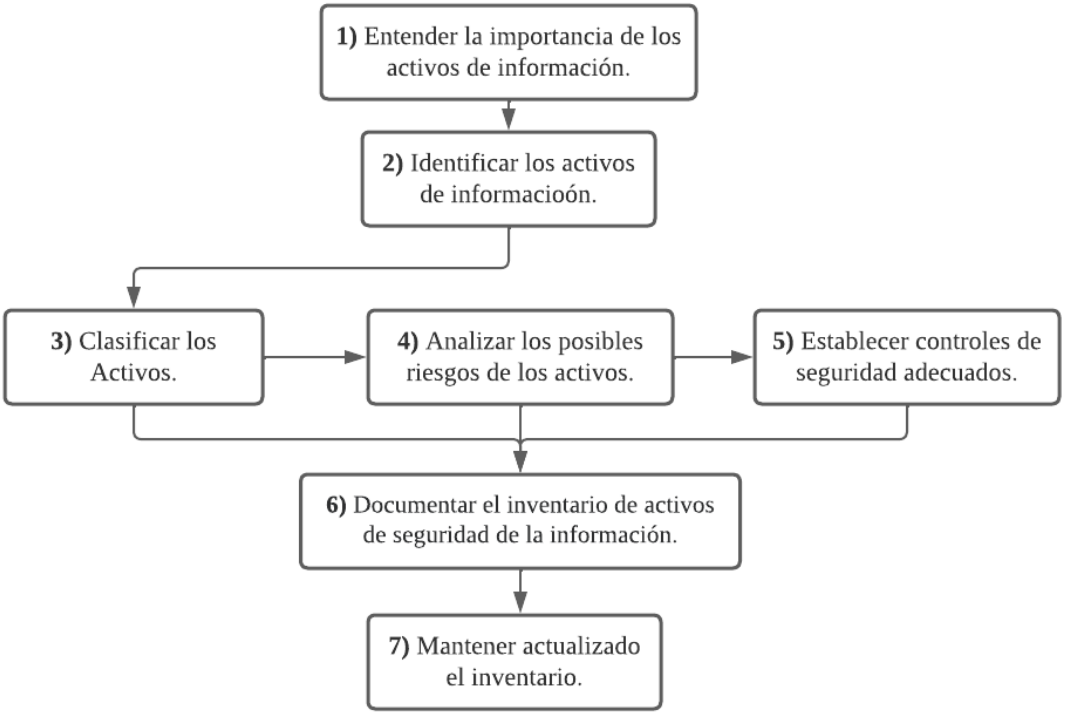
3.1.3. Comunicación

3.1.3.1.Inventario de activos de información con base a las normas ISO

Para el desarrollo de las políticas para los activos es necesario mencionar que el inventario de activos de información de acuerdo con la ISO 27001 señala que es la más importante para cada empresa u organización, es por esa razón que se tomó en cuenta el procedimiento para alcanzar una protección apropiada, cumplir con los estándares y objetivos de seguridad tanto físico, lógico, y de acceso (ISO Tools, 2023).

Según ISO Tools (2023) los pasos a seguir para realizar un inventario de activos de información actualizado según la norma ISO son los siguientes:

Ilustración 21.- Pasos para la elaboración de un inventario de activos



Elaborado por: Sánchez (2023)
Fuente: ISO Tools (2023)

1) **Entender la importancia de los activos de información**

Es el paso inicial y fundamental para realizar un inventario de activos de información de excelente calidad. Es crucial comprender y tener claridad sobre lo que se considera un activo, ya que esto proporciona el contexto necesario para comprender la estructura de una empresa. Esto permite identificar y distinguir los diferentes tipos de activos, como software, hardware, datos, instalaciones, entre otros, que son componentes vitales que aseguran el adecuado desempeño de la compañía.

2) **Identificar los activos de información**

Una vez que se haya comprendido de manera clara el concepto de activos de información, es fundamental proceder a identificarlos. Esto implica llevar a cabo una evaluación exhaustiva de los activos relevantes de la empresa, aquellos que aportan valor, como bases de datos, sistemas de control, servidores, entre otros.

3) **Clasificar los activos**

Esta característica reviste una importancia fundamental, puesto que permite comprender la importancia y el nivel de criticidad de cada activo. La clasificación de los activos ayuda a focalizarnos en aquellos que tienen mayor relevancia, lo que permite establecer controles y políticas para garantizar su seguridad. Además, reconoce si los activos son de bajo, medio, alto o muy alto nivel de criticidad en relación con su importancia.

4) **Analizar los posibles riesgos de los activos**

Una vez que se haya completado el paso anterior, es fundamental clasificar los activos según los tres pilares de la información: mantenerla en secreto, asegurar la integridad y garantizar el acceso. Esto permite identificar el activo más importante en la empresa. Posteriormente, la evaluación de riesgos será más factible, ya que se pude identificar posibles vulnerabilidades, amenazas y riesgos, lo que permite estar preparados ante posibles riesgos en el futuro.

5) **Establecer controles de seguridad adecuados**

En este paso es fundamental establecer los controles de seguridad más adecuados para proteger cada activo. Estos controles pueden adoptar diferentes formas, como controles físicos, técnicos, organizativos, de vigilancia, entre otros, con el objetivo de proteger los activos. Es importante tener en cuenta la norma ISO 27001, la cual proporciona pautas para la elaboración de dichos controles.

6) **Documentar el inventario de activos de seguridad de la información**

El paso que sigue es igualmente importante, ya que toda acción debe tener su respectivo respaldo. Por lo tanto, en este punto se hace referencia a plasmar en un documento todas las acciones realizadas con el inventario de activos de información: activos, riesgos, controles. Esta documentación permite tener una referencia para futuras actualizaciones, auditorías y revisiones.

7) **Mantener actualizado el inventario**

Realizar el inventario de activos de información no es un documento que se realiza solo una vez, sino que debe estar en constante actualización. Esto se debe a que la empresa adquiere nuevos activos, realiza modificaciones o los da de baja. Por esta razón, es importante establecer políticas para que el encargado realice un monitoreo y revisión periódica, con el fin de garantizar que el inventario refleje con exactitud la realidad de la organización.

3.1.3.2.Normas generales de la empresa

Es crucial que los colaboradores conozcan y cumplan con las normas establecidas por la organización, ya que estas pautas constituyen un grupo de reglas formales o informales que establecen cómo funciona la empresa en su interior. Estas medidas abarcan aspectos como la seguridad, la convivencia, la vestimenta, el trabajo, la contratación, entre otros, y tienen como objetivo garantizar la seguridad, promover la confianza y aumentar la productividad a los empleados sin interrumpir sus tareas o distraerlos innecesariamente de él. Además, es crucial que las normas cumplan con la legislación laboral vigente, garantizando que se respeten los derechos de los colaboradores y promoviendo un ambiente de trabajo seguro y saludable. En este sentido, es esencial mencionar que las normas generales de la empresa y las normas relacionadas con los activos de información tienen una estrecha relación. Una depende de la otra, ya que, al conocer las normas, podemos asegurar la protección de los recursos de información y protegerlos de posibles amenazas y riesgos.

Tabla 20.- Normas generales de Telpronet

Norma Actual	Acción de Mejora	Tipo de Control
Respaldar información en la nube.	Todos los empleados de la organización que manejen datos en sistemas de cómputo deberán realizar copias de seguridad de forma semanal en la nube y unidades externas.	Preventivo
Uso del uniforme de la entidad.	Los colaboradores de la empresa serán conscientes de mantener en buen estado el uniforme de la empresa y deberán utilizarlo en todo momento durante la jornada laboral, a menos que se especifique lo contrario por autorización de la gerencia.	Preventivo
Uso del EPP para empleados de campo.	Los empleados que realicen actividades de campo deberán utilizar de forma obligatoria el EPP (Equipos de Protección Personal para Trabajos Eléctricos) durante la realización de trabajos eléctricos.	Preventivo
Para la contratación de nuevos empleados.	La contratación de nuevos empelados tendrá que cumplir con requisitos específicos, entre uno de los más importantes es la experiencia, el conocimiento y las habilidades.	Preventivo
Puntualidad, honestidad y responsabilidad en cada área de trabajo.	Todos los empleados de la empresa deberán llegar a tiempo a su trabajo, ser honestos en todas sus actividades laboral y cumplir con las tareas asignadas por los supervisores o jefes, caso contrario su incumplimiento puede resultar en medidas disciplinarias notificando tanto de forma verbal como escrita.	Preventivo
Mantener la oficina ordenada y limpia	Todos los empleados de la organización deberán mantener su propio espacio de trabajo limpio y ordenado.	Preventivo
Cumplir con las disposiciones que se den por los supervisores.	Todos los empleados de la organización deben acatar órdenes y directrices dadas por los supervisores o jefes.	Preventivo
Atención al cliente de forma amable.	Los empleados en especial, lo encargados de la atención al cliente deben de saludar de manera cordial y mostrar interés genuino en sus necesidades y consultas que las realicen en todo momento.	Preventivo
Cumplir con el horario establecido para el almuerzo.	Los empleados deberán de utilizar el horario de almuerzo exclusivamente para la ingesta de alimentos y el descanso necesario.	Preventivo
Hacer cierres de caja al finalizar cada jornada.	Al finalizar cada jornada de trabajo, los empleados responsables de las transacciones deberán realizar el cierre de caja en donde los valores deben de coincidir con el sistema contable.	Preventivo
Seguir las reglas y protocolos de seguridad internos que ha establecido la empresa.	Todos los empleados de la organización deberán conocer y comprender las normas y procedimientos de seguridad integral e internos establecidos por la empresa para su correcto cumplimiento de este.	Preventivo

Elaborado por: Sánchez (2023)

3.1.3.3.Políticas por cada grupo de activos de información

Después de identificar los pasos necesarios para salvaguardar un inventario de activos de información y haber determinado las normas generales de la empresa, se procedió a establecer políticas para cada grupo de activos de la compañía. Esto es primordial, ya que ayuda a establecer un marco general para la gestión de los activos, lo que a su vez proporciona la base para la implementación de medidas y controles específicos.

Los grupos de activos para tener en cuenta son el Software Contable, Hardware, Redes, Instalaciones y Personal, ya que se relacionan entre sí creando vínculos y conexiones con el fin de lograr los objetivos de la compañía. Es elemental destacar que en este trabajo integrador se enfocó principalmente en la parte del Software Contable, el cual es considerado uno de los activos más valiosos de la compañía. Por esta razón, se estableció políticas y controles claros para evitar errores por parte de los empleados y salvaguardar este activo de información contra posibles amenazas y riesgos en el futuro.

TELPRONET

MANUAL DE POLÍTICAS Y CONTROLES DE SEGURIDAD

AMBATO - ECUADOR

ÍNDICE MANUAL DE POLÍTICAS Y CONTROLES

CONTENIDO **PÁGINA**

3.1.3.4. Políticas y controles software contable 60
3.1.3.5. Políticas y controles hardware..... 64
3.1.3.6. Políticas y controles redes..... 66
3.1.3.7. Políticas y controles instalaciones..... 68
3.1.3.8. Políticas y controles personal..... 70

Introducción

Las políticas de seguridad de la información son imprescindibles para salvaguardar la integridad de los sistemas y establecer las conductas y medidas necesarias para implementar las destrezas en Telpronet. Estas políticas ayudan a evitar y hacer frente a posibles riesgos, basándose en los principios de mantener la integridad, disponibilidad y confidencialidad de la información y activos críticos, al mismo tiempo que establecen las responsabilidades, derechos y deberes de los colaboradores. Además, las políticas de seguridad son esenciales para cumplir con regulaciones y estándares internacionales, como la norma ISO/IEC 27001, que provee directrices y prácticas para asegurar la gestión de la seguridad de la información.

Principios según la norma ISO 27000

Confidencialidad

Garantiza que la información sea asequible únicamente para personas acreditadas como gerente y jefes de los departamentos, además, constituye uno de los principios esenciales en la seguridad de la información y busca preservarla mediante la implementación de controles y protocolos establecidos.

Integridad

La información que se presenta a la gerente de la empresa es precisa, completa y protegida contra modificaciones no autorizadas. Los controles incluyen el desarrollo de políticas y procedimientos para prevenir la alteración de datos. Al proteger la integridad de la información, la empresa puede evitar el fraude, la manipulación maliciosa y otros riesgos que podrían afectar su reputación y operaciones.

Disponibilidad

Los recursos como estados financieros están disponibles y accesibles cuando sean necesarios. Esto implica asegurar que los sistemas, servicios y datos estén disponibles para su uso y funcionamiento continuo, evitando interrupciones o tiempos de inactividad no planificados. Estos controles incluyen el desarrollo de sistemas de respaldo y recuperación de información, la protección contra amenazas físicas y lógicas, para asegurar la continuidad de las operaciones comerciales.

Software Contable

Detalles de la empresa

Los detalles de la empresa fueron recolectados de la página oficial de la empresa (Setca Group, 2023):

Empresa: SETCA GROUP

Descripción de la empresa: Empresa enfocada a ofrecer soluciones tecnológicas para ayudar a las empresas a crear y optimizar los procesos diarios. Cuenta con una amplia gama de servicios, que están diseñados de manera personalizada para satisfacer las necesidades exclusivas de cada usuario.

Nombre del Software: SEFAC

Logo

Ilustración 22.- Logo del sistema contable

Fuente: Setca Group (2023)

Módulos Habilitados

- Facturación Electrónica
- Cuentas por Cobrar y Pagar
- Clientes ISP
- Suspensión de Clientes Automática y manual
- Control de Compartición (Simple Queue, PPPoE, PCQ)
- Control RB Mikrotik
- Envío Automático de Avisos de pagos pendientes vía WhatsApp
- Inventario
- Módulo de Contabilidad

- Módulo RRHH
- Reportería

Características del Sistema

- Búsqueda por RUC
- Actualización
- Soporte
- Respaldos de datos
- 100% Online
- Autorización Automática SRI

Según lo comentado por la Asistente Contable de la empresa Telpronet Fernanda Villacrés (2023) la empresa cuenta con las siguientes ventajas y desventajas con relación al software.

Ilustración 23.- Ventajas y desventajas

Ventajas	Desventajas
•Sistema diseñado para el giro del negocio que en este ocasión es la provisión de servicio de Internet a los clientes. •El sistema puede realizar cortes automáticos del servicio de Internet cuando el cliente no realice el pago a tiempo y podrá configurar los días tolerancia. •El sistema puede enviar de manera automatica avisos y pagos que deben hacer los clientes vía WhatsApp.	•El seguimiento y actualización de inventarios en la empresa no es eficiente ni efectivo. •Los registros que se realiza el sistema de forma automática en los libros contables de compras y ventas presentan discrepancias y errores. •El módulo de reportes presenta deficiencias, ya que no proporciona una respuesta inmediata, sino que requiere un tiempo prolongado de espera.

Elaborado por: Sánchez (2023)
Fuente: Villacrés (2023)

Utilización del software contable

Según lo expuesto por la Asistente Administrativa de la empresa Telpronet Karen Ponluisa (2023) los pasos a seguir para realizar las distintas transacciones en el software contable son las siguientes:

Pasos para realizar una compra

1. Se identifica si la factura es física o electrónica.
2. Se ingresa al software contable con el usuario y contraseña.
3. Módulo de Contabilidad.
4. Sección Compras.
5. Ingresa la factura en XML si es electrónica o se ingresan los datos requeridos si es física (fecha, nombre proveedor, datos de la factura, numero de autorización y valor).
6. Registro automático.
7. Guardar

Control para realizar una compra

1. Asistente Contable realiza la proforma.
2. Enviar proforma a la gerente de la empresa.
3. Gerente aprueba o desaprueba la proforma.
4. Asistente contable realiza el pago si se aprobó la proforma.

Pasos para realizar una venta

1. Se ingresa al software contable con el usuario y contraseña.
2. Sección Clientes.
3. Se identifica si el usuario se encuentra creado o si no se procede a introducir uno nuevo.

3.1. Si no se encuentra creado el cliente, se dirige a crear nuevo clientes y se introducen los campos requeridos como: Nombre, RUC, dirección, número de celular. El sistema asigna de forma automática un código alfanumérico al cliente.

4. Seleccionar el cliente.
5. Elegir el plan de Internet que quiere el cliente.
6. Se asigna la fecha de instalación e inicio del servicio.
7. Se registra la forma de pago.
8. Se firma y se envía automáticamente la factura electrónica al cliente.

Pasos para realizar un pago

1. Se ingresa al software contable con el usuario y contraseña.
2. Módulo cuentas por pagar.
3. Busco al proveedor que quiero cancelar.
4. Selecciono el método de pago si es efectivo o depósito.
5. Se disminuye la cuenta por pagar automáticamente.

Pasos para realizar un cobro

1. Se ingresa al software contable con el usuario y contraseña.
2. Módulo cuentas por cobrar.
3. Se selecciona el cliente.
4. Se revisa las cuotas que está adeudando.
5. Se realiza la factura.
6. Se realiza el cruce respectivo automáticamente tanto en efectivo como depósito.

Según lo expuesto por la Asistente Administrativa de la empresa Telpronet Karen Ponluisa (2023) el manejo de las cuentas se la realiza de la siguiente manera:

Manejo de la cuenta caja y bancos

Cada empleado tiene la obligación de realizar un arqueo de caja, después de culminar su jornada laboral, asegurándose de que los valores coincidan con la información almacenada en el sistema sobre los pagos efectuados por los clientes.

Manejo del libro diario

Los empleados evitan utilizar ese módulo debido a una mala experiencia. Después de llevar a cabo varias actividades como compras y ventas, los registros que se mostraban en el módulo eran completamente incorrectos, lo que generaba confusión entre los empleados de la empresa. Desde entonces, han decidido no utilizar el módulo Contabilidad específicamente la sección del Libro diario.

Manejo de los inventarios

El módulo de inventarios del software contable es deficiente, ya que no está completamente integrado para mantener un registro preciso y actualizado de los inventarios. Como resultado, los empleados han optado por no utilizar el módulo y en su lugar han tenido que recurrir a tarjetas Kardex para gestionar el inventario de la empresa.

Manejo de los reportes

Los empleados han decidido no utilizar el módulo de inventarios, ya que los reportes que genera no son adecuados ni cumplen con las características requeridas. En su lugar, gestionan los reportes en una hoja de Excel para poder emitir un reporte que cumpla con las condiciones necesarias cuando la gerente lo solicite. Esta decisión se debe a la deficiencia del módulo de inventarios en el software contable

3.1.3.4.Políticas y controles software contable

El manual de políticas para la utilización del sistema contable es necesario para establecer pautas claras y consistentes que regulen el uso del sistema. Proporciona a los empleados una guía sobre cómo deben interactuar con el sistema, lo que contribuye a asegurar que los datos contables sean precisos, coherentes y seguros. Además, el manual puede incluir procedimientos para la resolución de problemas técnicos, lo que ayuda a reducir el tiempo en que el sistema no está en funcionamiento y a mantener la continuidad de las operaciones.

Objetivo

Proporcionar una guía clara y coherente para el registro preciso y el uso apropiado de las cuentas, así como para la aplicación consistente de las políticas contables en la organización.

Alcance

Enfocado a los usuarios (empleados) actuales de la empresa que son los encargados del manejo y administración del software contable, estos deberán cumplir con todas las normativas y los requisitos legales y de información.

Políticas para el acceso al software

- Solo los empleados designados y autorizados tendrán acceso al software contable.
- Cada empleado recibirá sus respectivas credenciales (password) para el ingreso al software, en ella constará su usuario y contraseña.
- Cada empleado deberá guardar de forma segura sus credenciales y no compartirlas con personas externas de la empresa.
- Cada empleado será responsable de cambiar su contraseña de forma periódica e informar al supervisor quien es el administrador y encargado de la gestión de contraseñas.
- El supervisor de la gestión de contraseñas deberá realizar un bloqueo a la contraseña de aquellos empleados que salgan de vacaciones o hayan terminado la relación laboral con la empresa.

Políticas para la utilización del software contable

- Solo los empleados designados por la gerencia podrán hacer uso del software contable según sus funciones establecidas dentro de la empresa.
- El Ingeniero en Sistemas será el encargado (Supervisor) de llevar una bitácora de accesos al Sistema Contable.
- El sistema contable debe ser utilizado exclusivamente para actividades relacionadas con el trabajo.
- Los empleados deben mantener de forma confiable la información de la empresa.
- No se debe compartir ningún tipo de información con personas no autorizadas, ni divulgarla de forma digital.
- Todas las transacciones dentro del sistema contable deben de registrarse de manera oportuna, completa y precisa.
- Si se necesita realizar modificaciones a la base de datos del sistema, se debe solicitar la asistencia técnica del ingeniero en sistemas ya que, es el responsable autorizado de manejar el gestor de base.
- Realizar copias de seguridad en la nube y en dispositivos externos de forma periódica cada semana, para así prevenir posibles amenazas o riesgos que se puedan presentar.
- La empresa brindará capacitaciones continuas a los empleados para la correcta utilización del software contable.

Políticas para la creación de contraseñas

- Las contraseñas deben ser lo suficientemente complejas, lo que implica una mezcla entre mayúsculas, minúsculas, números y caracteres especiales para fortalecer la protección.
- El número de caracteres para crear una contraseña debe ser mínimo 8 dígitos y máximo 10.
- La contraseña no debe contener información personal, ni fechas de nacimiento, tampoco número celulares.
- Evitar seguir un patrón de letras, números, ya que puede ser de fácil conocimiento.

- El cambio de contraseñas de cada usuario debe ser de forma trimestral, para evitar uso excesivo de contraseñas.
- Las contraseñas no deben ser compartidas con nadie, ni tampoco guardarlas en los dispositivos tecnológicos.

Políticas para la emisión de información contable

- La información que la empresa emita debe estar en conformidad con los tres principios de la información, los cuales son confidencialidad, integridad y disponibilidad.
- Evitar la modificación de valores en los reportes ya que, podría ocasionar elecciones no adecuadas por parte de la administración.
- La información que se emita debe ser revisada y aprobada por las personas responsables de dicha información con firmas de responsabilidad.
- La emisión de información debe ajustarse a todas las normativas contables y tributarias pertinentes, incluyendo aquellas que se refieren al resguardo de datos y la publicidad.
- La información emitida desde el software deberá ser tanto en físico como en archivo digital en formato PDF.

Controles

- Crear las claves de usuario con el perfil parcial restringiendo el acceso a modificaciones o eliminaciones de transacciones en el sistema contable dependiendo de las funciones que desempeñan en la empresa.
- Supervisar que aquellos usuarios con perfil total en el acceso al software realicen las actividades correspondientes a sus funciones dentro de la empresa.
- Verificar que la realización de copias de respaldo (backups) de la información se realice de forma semanal y en dispositivos externos y en la nube.
- Monitorear constantemente la actividad realizada en el software contable.
- Mantener la información contable al día, para evitar posibles retrasos y sanciones.
- Revisar frecuentemente las actualizaciones al software para evitar caducidad de su licencia y operatividad por cambios tributarios.

- Verificar que el software cumpla con un certificado de protección de datos digitales.
- Comprobar que el software contable permita bloqueo de fechas en la contabilidad para evitar descuadres o datos modificados que alteren el valor razonable de los estados financieros.
- Conciliar la información contable con los módulos operativos del sistema contable que guarde razonabilidad e integridad de los datos.

Responsables

- Técnico de Soporte Informático
- Asistente Contable
- Contador General
- Gerente general

3.1.3.5.Políticas y controles hardware

Es fundamental desarrollar un manual de políticas para la utilización del hardware con el fin de establecer directrices claras y procedimientos que regulen el uso apropiado de los ordenadores de mesa, laptops y otros dispositivos. Este manual abarca políticas para la instalación, mantenimiento y actualización del hardware, así como para el uso adecuado de los recursos informáticos asignados a cada usuario. Asimismo, puede abordar aspectos de seguridad informática, como la prohibición del uso de herramientas de hardware que vulnere los controles de seguridad, es por eso por lo que el propósito es resguardar la integridad y confidencialidad de la información de la compañía.

Objetivo

Asegurar la salvaguarda de los activos físicos de la organización, incluyendo equipos de cómputo, dispositivos de almacenamiento, entre otros. Además, establecer lineamientos y procedimientos para prevenir incidentes de seguridad, salvaguardar la integridad y confidencialidad de la información, y asegurar el funcionamiento adecuado.

Alcance

Enfocado a los empleados actuales de la empresa que son los encargados del manejo de equipos tecnológicos, independientemente de su cargo o función.

Políticas

- La contraseña para el acceso a los ordenadores tecnológicos deberá contener al menos 8 caracteres y una mezcla entre números y letras.
- Los dispositivos tecnológicos de la empresa como laptop, computadoras de escritorio, deberán tener un protector de pantalla (bloqueo automático) que se active después de 1 minuto de inactividad. Solicitando la contraseña para su ingreso.
- Mantener los dispositivos tecnológicos en áreas seguras y protegidas contra robos o daños causados por condiciones ambientales como humedad o calor.
- Conservar una temperatura adecuada para la protección de los ordenadores.

- Realizar mantenimientos periódicos a los equipos informáticos y dispositivos tecnológicos que presenten algún fallo.
- Mantener aseado el lugar donde se encuentra ubicados los ordenadores.

Controles

- Llevar un registro actualizado (bitácora) con fecha de mantenimiento y responsables de los dispositivos tecnológicos.
- Llevar un inventario de activos de seguridad de la información actualizado de todos los dispositivos tecnológicos en la empresa, comprobando la existencia del activo dentro de la empresa.
- Monitorear diariamente a través de las cámaras de seguridad el acceso físico no autorizado a los dispositivos tecnológicos.
- Mantener un registro actualizado de los dispositivos asignados a cada empleado, incluyendo el modelo, número de serie y fecha de entrega, los cuales deberán ser firmados en actas de entrega-recepción.
- Notificar de manera oportuna al área de soporte técnico si se produce algún fallo en los equipos.
- Revisar el estado del almacenamiento de las computadoras (memoria RAM) para el correcto funcionamiento y así evitar la ralentización en los mismos.
- Verificar constantemente el funcionamiento de los ventiladores en los ordenadores tanto servidores como terminales.
- En cuanto a la temperatura ambiente: Cuando el procesador está funcionando normalmente, la temperatura debe estar entre 30°C y 50°C. Sin embargo, cuando se utiliza intensivamente con programas de alto rendimiento, la temperatura puede alcanzar hasta 95°C. Es importante destacar que nunca se debe superar los 100°C, que es la temperatura máxima recomendada.

Responsables

- Técnico de Soporte Informático
- Gerente de la empresa
- Usuarios (empleados)

3.1.3.6.Políticas y controles redes

Las políticas de sistemas de red son un grupo de normas, directrices e instrucciones establecidas por una organización con el objetivo de resguardar la infraestructura de tecnología de la información contra posibles amenazas y riesgos de seguridad. Estas políticas definen las tareas óptimas e importantes para que la protección de la información sea segura, establecen los roles y responsabilidades de los usuarios, así también como los protocolos para el manejo de incidentes y detallan cómo responder ante eventuales amenazas de seguridad. El propósito de estas políticas es reducir al mínimo las vulnerabilidades y proteger los activos de información frente a posibles ataques. Es fundamental que las políticas de seguridad informática sean comunicadas de manera clara a todos los colaboradores y se establezcan mecanismos para garantizar y supervisar el cumplimiento de las mismas.

Objetivo

Crear un conjunto de directrices que cercioren la confidencialidad, exactitud y accesibilidad de la información, al mismo tiempo que se resguarde la infraestructura tecnológica contra posibles peligros y riesgos de seguridad.

Alcance

Engloban múltiples elementos que posibilitan la comunicación y el traspaso de información entre diversos dispositivos y usuarios.

Políticas

- Analizar de forma periódica las vulnerabilidades y amenazas en relación con la seguridad de red.
- Las contraseñas para el acceso a los sistemas de red deben de tener como mínimo 8 caracteres con una combinación entre letras y números.
- Cumplir con las normativas y regulaciones en temas de seguridad de la información y resguardo de datos.
- Todos los equipos tecnológicos deberán contar con una protección en cuanto a los sistemas de red.
- Activar firewalls para permitir solo el acceso al tráfico apropiado.

- Para el intercambio de información, la empresa establecerá acuerdos de confidencialidad con personas o entidades externas que participen en dicho proceso.
- El Ingeniero en Sistemas deberá ejecutar la conexión con VPN en los dispositivos de la empresa.

Controles

- Analizar periódicamente los sistemas de red con el fin de identificar a través de software malicioso, posibles amenazas.
- Supervisar y controlar la actividad de los sistemas de red como puertos y protocolos (IP's).
- Establecer la seguridad en el sistema de red con el fin de prevenir que los atacantes se aprovechen de configuraciones predeterminadas que sean vulnerables.
- Vigilar el funcionamiento de las redes inalámbricas de área local, los puntos de acceso y los dispositivos inalámbricos de los clientes.
- Verificar que la velocidad de gigas y transferencia de datos sea constante.

Responsable

- Técnico de Soporte Informático

3.1.3.7.Políticas y controles instalaciones

Las políticas con relación a las instalaciones de una empresa son un grupo de directrices y procedimientos que establecen los lineamientos para el funcionamiento y mantenimiento de los recursos e infraestructuras físicas de la organización. Estas políticas tienen como propósito garantizar la seguridad, eficiencia y cumplimiento de las normativas y regulaciones ajustables en materia de seguridad, higiene y bienestar en el lugar de trabajo.

Objetivo

Establecer un marco de trabajo seguro, eficiente y respetuoso con el medio ambiente, garantizando la protección de los activos de información ante cualquier vulnerabilidad o amenaza.

Alcance

Implica la protección de la infraestructura, la seguridad de las instalaciones, la gestión de riesgos y el mantenimiento de las mismas.

Políticas

- Realizar mantenimiento periódico a las instalaciones.
- La gerencia deberá realizar planes de capacitación y simulacros en cuanto a temas de seguridad y protección de instalaciones.

Controles

- Restringir el acceso a personas no autorizadas a la infraestructura de la empresa.
- Verificar que las instalaciones se encuentren cubiertas para garantizar la seguridad y eficiencia en el uso.
- Verificar que el cableado en las instalaciones se encuentre en áreas seguras, es decir, que no esté ubicado en lugares donde haya riesgo de incendio, inundaciones o sobrecargas eléctricas.
- Verificar que las personas que accedan a las instalaciones lleven un identificativo.

- Confirmar la actividad que las personas externas realizan dentro de las instalaciones.

Responsables

- Técnico de Soporte Informático
- Gerente de la empresa

3.1.3.8.Políticas y controles personal

Las políticas en relación con los trabajadores de una empresa son un grupo de directrices y procedimientos que establecen los lineamientos para el comportamiento, las responsabilidades y los derechos de los empleados dentro de la organización. Estas políticas incluyen elementos como las normas de comportamiento, presencia física, normas de vestimenta, la privacidad, la seguridad y otras áreas concernientes a las condiciones laborales.

Objetivo

Garantizar un ambiente laboral justo, seguro, respetuoso y productivo, promoviendo el bienestar de los empleados y el cumplimiento de las normativas legales y éticas.

Alcance

Aplica a todos los empleados dentro de la empresa, en donde deben cumplir con los requisitos establecidos en esta política.

Políticas

- Los candidatos que aspiren a ocupar un cargo en la compañía deberán pasar por un proceso de verificación de antecedentes, específicamente en relación con los procesos judiciales.
- Las personas que sean contratadas para ocupar un puesto en la empresa deberán firmar un contrato en el que se establezcan los acuerdos de seguridad, acatando las políticas de la empresa.
- Todos los empleados de la empresa deben firmar los acuerdos de confidencialidad, en donde se comprometen a mantener la privacidad de los datos de la empresa y de los usuarios.
- Los empleados deben hacer un uso responsable de los recursos de la compañía y limitarlo exclusivamente a actividades relacionadas con su trabajo.
- La empresa organizará charlas y capacitaciones periódicas con el fin de ofrecer chances de progreso, evolución y estímulo a su personal.
- La gerencia debe comunicar a los empleados, los normas, políticas y código de ética que deberán cumplir.

Controles

- Archivar de manera digital los registros de todos los postulantes a cargo en la empresa para futuras contrataciones conocer sus antecedentes.
- Verificar el registro de los empleados a través del sistema biométrico tanto para entrada como salida de la jornada laboral.
- Constatar a través de un registro de los empleados que asistan a las charlas o capacitaciones que brinda la empresa.
- Realizar test o evaluaciones trimestrales para verificar que el desempeño de los trabajadores sea aceptable.

Responsables

- Gerente de la empresa
- Asistente Administrativa

3.1.3.9.Matriz de seguimiento y monitoreo

La matriz de seguimiento de controles es una herramienta valiosa para salvaguardar los activos de información de una empresa. Al proporcionar una visión clara y estructurada de los controles implementados, esta matriz ayuda a identificar y llevar un seguimiento constante del cumplimiento de los controles para así salvaguardar los activos críticos de la empresa.

En el campo de porcentaje se calificará en un rango de 25%, 50%, 75% y 100%, lo que permitirá tener conocimiento claro del nivel de cumplimiento del control sugerido para la conservación de los activos de información. En el campo responsable deberá constar el nombre de la persona a cargo quien realizó el seguimiento en la matriz. Finalmente se registrará la fecha en la cual se realizó el monitoreo.

Esta matriz servirá como una bitácora para dar cumplimiento a los niveles de madurez según lo establece la norma ISO con la finalidad de que todos los controles alcancen un 100% lo que indicará que la empresa está cumpliendo con la seguridad de la información.

Tabla 21.- Matriz de seguimiento y monitoreo de activos

MATRIZ DE SEGUIMIENTO Y MONITOREO						
Activos de Información	**Control Sugerido**	**Medio de Verificación**	**Frecuencia**	**%**	**Responsable**	**Fecha monitoreo**
Software Contable	Verificar que la realización de copias de respaldo (backups) de la información se realice en unidades externas y en la nube.	Copias de seguridad	Semanal			
Redes sociales	Realizar revisiones en caso de preguntas por parte de los clientes	Opiniones de clientes	Semestral			
Página web	Verificar diariamente el correcto funcionamiento de la página web.	Informe mensual de seguimiento	Trimestral			
Correo Electrónico	Realizar copias de correos a gerente.	Copias en correos electrónicos	Diario			
Sistema de Red	Supervisar y controlar la actividad de los sistemas de red como puertos y protocolos (IP's).	Informe mensual de seguimiento	Mensual			
Computadoras de escritorio, Laptop	Mantener un registro actualizado de los dispositivos asignados a cada empleado, incluyendo el modelo, número de serie y fecha de entrega.	Actas de entrega-recepción	Semestral			
Impresora	Notificar de manera oportuna al área de soporte técnico en caso de producirse un fallo.	Correo electrónico enviado a Ing. en Sistemas	Mensual			

TV, Equipo Biométrico	Monitorear las cámaras de seguridad el acceso físico no autorizado.	Informe del registro de movimientos en cámara.	Diario			
Router, Terminal de línea Óptica	Notificar en caso de falla.	Correo electrónico enviado al Ing. en Sistemas.	Semestral			
Regulador de voltaje, UPS	Mantenimiento adecuado para el uso eficiente.	Bitácora de mantenimiento	Anual			
Cámaras de Seguridad	Verificar el almacenamiento de la grabación de video	Registro de acceso a la cámara.	Mensual			
Carpetas físicas	Verificar que los documentos físicos tengan respaldo en la nube y dispositivo externo	Informe sobre los documentos subidos a la nube.	Semanal			
Pendrives	Constatare que los pendrives se encuentren en lugares seguros	Reporte al final del día	Diario			
Personal	Realizar test o evaluaciones para verificar que el desempeño de los trabajadores sea aceptable.	Informe de los resultados de las evaluaciones.	Trimestral			

Elaborado por: Sánchez (2023)

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1.Conclusiones

Actualmente, las empresas enfrentan diversos riesgos asociados a la seguridad de la información. Es crucial que las entidades comprendan la importancia de resguardar sus datos y sistemas, implementando medidas de control adecuadas y necesarias para asegurar el amparo de los activos de información de la empresa. La inversión en seguridad de la información permite garantizar la confianza de los empleados, clientes y partes interesadas evitando la pérdida de datos primordiales. Dando paso a las conclusiones presentadas a continuación.

- Los activos de información de la empresa no están actualizados debido a la falta de procedimientos adecuados que mencione las actividades de control y seguimiento que los empleados deben seguir en relación con los inventarios de los activos de la empresa. Además, se observa una falta de capacitación en cuanto a la importancia de la ISO 27000, los estándares internacionales y las directrices a seguir en temas de gestión empresarial.

- La información que maneja la empresa es de gran importancia según su nivel de valoración, lo que implica los tres principios fundamentales: confidencialidad, integridad y disponibilidad. A pesar de contar con controles básicos, existe una alta probabilidad de enfrentar amenazas y riesgos que podrían comprometer a la empresa y su información contable histórica si no existe una persona a cargo del control de estos, las posibilidades de riesgo incrementan.

- La empresa al encontrarse en crecimiento resulta trascendental reconocer los activos más críticos, por consiguiente, en los resultados se observa que la empresa tiene puntos débiles en cuanto a las políticas de seguridad. Esto implica una falta de revisión y gestión de los riesgos, lo que crea un punto débil

en el sistema de información, dificultando así la identificación de ataques o intrusiones en tiempo real.

- Las diversas amenazas a las que se enfrentan los activos de información de la empresa y su seguridad son muy evidentes debido a que, se identifican amenazas de tipo natural, así como, robo de información por terceras personas, se observa que las amenazas pueden explotar las vulnerabilidades detectadas en la empresa como: falta de procesamiento de datos, falta de capacitación en temas de seguridad de información al personal, entre otras. La inversión realizada en seguridad por parte de la administración está direccionada a salvaguardar los activos más importantes entre ellos se encuentra la información de sus clientes y partes interesadas.

- En el departamento de informática se reconoce la carencia de políticas y estrategias adecuadas para los controles en los sistemas informáticos. Los controles actuales de la empresa en su mayoría son preventivos. Sin embargo, la empresa sufrió un ataque como suceso imprevisto de robo de información, como respuesta a este evento solo optaron por limitados controles correctivos permitiendo recuperar parte de su información confidencial.

- Las políticas para el sistema de seguridad de la información si no son bien manejadas y aplicadas en la empresa provocan riesgos altos como es el caso del software contable y las carpetas físicas que son vulnerables a la pérdida de información según el mapa de calor donde claramente se los identifica.

4.2.Recomendaciones

- Se recomienda seguir los pasos necesarios para identificar los activos de acuerdo con los lineamientos establecidos en la norma ISO 27001, que implica realizar un inventario exhaustivo de los activos de información, documentarlos y mantenerlos actualizados de manera constante. Esto es fundamental para garantizar una adecuada protección de los activos de acuerdo con su nivel de significancia según la tasación asignada.

- Se sugiere aplicar una matriz de seguimiento de los controles aplicados para cada grupo de activos, con sus respectivos responsables debido a que, permite llevar un control, supervisión y evaluación de los mismos. Esto asegura que la información se mantenga confidencial, íntegra y disponible.

- Deberán utilizar plantillas en Excel automatizadas como herramienta auxiliar para el manejo adecuado del área de Contabilidad pues ayudará a evitar la pérdida de información y registros equívocos que puedan identificarse en el software contable.

- Se sugiere a la gerente de la empresa aprobar y poner en funcionamiento el manual de políticas y controles de seguridad para proteger la información que se indica en el presente proyecto integrador, puesto que permitirá tener un mejor control sobre los activos de información, especialmente el software contable. También, es fundamental difundir y capacitar a cada empleado sobre la importancia de salvaguardar la información, cumplir con las políticas de seguridad y los contratos firmados, con el fin de evitar eventos que comprometan la continuidad de la organización.

- Sería recomendable que la empresa opte por la adquisición de una herramienta contable que le permita cubrir las necesidades financieras, debido a que, el software que manejan actualmente es adecuado para el giro del negocio operativo, pero se encuentra con ciertas limitaciones para el área contable.

REFERENCIAS BIBLIOGRÁFICAS

Alias, A., & Cebrián, D. (2019). Tecnologías para la información de profesionales en educación. *Elibro*, *1*, 72–83. https://elibro.net/es/lc/uta/titulos/128512

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Dialnet*, *21*(2), 3–10. https://dialnet.unirioja.es/servlet/articulo?codigo=6989568

Araujo, A. (2019, August 24). *Creando un inventario de activos en 4 sencillos pasos*. Hackmetrix. https://blog.hackmetrix.com/inventario-de-activos-seguridad-de-la-informacion/

Baca, G. (2016). *Introducción a la Seguridad Informática*. *1*, 11–34. https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf

Baena, G., Mendoza, R., & Coronado, J. (2019). Importancia de la Norma ISO/IEC 27000 en la implementación de un Sistema de Gestión de la Seguridad de la Información. *Dialnet*, *22*, 2–12. https://dialnet.unirioja.es/descarga/articulo/8990740.pdf

Bestratén, M. (2013, September 25). Nivel de deficiencia. *Seguridad Minera*. https://www.revistaseguridadminera.com/gestion-seguridad/ntp-330-sistema-simplificado-de-evaluacion-de-riesgos/

Brien, J., & Marakas, G. (2006). Sistemas de Información Gerencial. *Mc Graw Hill*, *7*(1), 340–523. https://www.academia.edu/91551151/SISTEMAS_DE_INFORMACION_GERENCIAL_OBrein_y_Marakas_McGraw_Hill

Camargo, E., & Pinzón, M. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *Revista Ibérica de Sistemas e Tecnologías de Información*, *46*(6), 87–99. https://doi.org/10.17013/risti.46.87-99

Carvajal, A. (2020). Reflexiones sobre la seguridad de la información. *Revista Sistemas*, 8–17. https://doi.org/10.29236/sistemas.n155a2

Chicano, E. (2015). Auditoría de Seguridad Informática. *IC Editorial*, *MF0487_3*, 57–75. https://elibro.net/es/lc/uta/titulos/44136

Costas, J. (2010). Seguridad informática. *Digitalia*, 134–230. https://www.digitaliapublishing.com/a/109890

Cuniglio, L. (2016, December 30). *ISO 27002: Buenas prácticas para gestión de la seguridad de la información*. Seguridad Digital de Resultados. https://ostec.blog/es/aprendizaje-descubrimiento/iso-27002-buenas-practicas-gsi/?cn-reloaded=1

Dussan, C. (2020). Políticas de seguridad informática. *Entramado*, *2*(1), 86–92. https://www.redalyc.org/pdf/2654/265420388008.pdf

Estrada, R., Unás, J., & Flórez, E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista Logos, Ciencia & Tecnología*, *13*(3). https://doi.org/10.22335/rlct.v13i3.1446

Fletcher, L. (2019, May 12). *Gestión de la Seguridad de la Información ISO 27001*. Organismo de Certificación Global. https://normaiso27001.es/

Franco, D., Perea, J., & Tovar, L. (2013). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. *Información Tecnológica*, *24*(5), 13–22. https://doi.org/10.4067/S0718-07642013000500003

Gómez, Á. (2011). Gestión de incidentes de Seguridad informática. *Digitalia*, *MF0488_3*. https://www.digitaliapublishing.com/a/109924

Guaña, J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. *Recimundo*, *7*, 609–616. https://doi.org/10.26820/recimundo/7.(1).enero.2023.609-616

Guerra, E., Neira, H., Díaz, J., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información Tecnológica*, *32*(5), 145–156. https://doi.org/10.4067/s0718-07642021000500145

Hernández, M., Cantero, Z., Giseth, L., Vidal, R., & Marcela, D. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Redalyc*, *2*, 3–10. https://www.redalyc.org/articulo.oa?id=29063446029

ISO. (2009, November 15). *Norma Internacional ISO 31000 Gestión de Riesgos, Principios y Guías*. https://gestion-calidad.com/wp-content/uploads/2016/09/iso_31000_2009_gestion_de_riesgos.pdf

ISO Tools. (2023, July 25). *Pasos para hacer un inventario de activos de seguridad de la información con la nueva ISO 27001:2023.* ESG Innova. https://www.isotools.us/2023/07/18/pasos-para-hacer-un-inventario-de-activos-de-seguridad-de-la-informacion-con-la-nueva-iso-270012023/

Jordán, V., Galperin, H., & Peres, W. (2013). Banda ancha en América Latina: Más allá de la conectividad. *Dirsi*, 132–243. https://www.cepal.org/es/publicaciones/35399-banda-ancha-america-latina-mas-alla-la-conectividad

Kosevich, E. (2019). Estrategias de Seguridad Cibernética en los países de América Latina. *Iberoamérica*, 137–159. https://doi.org/10.37656/S20768400-2020-1-07

Madrigal, W. (2019). Conceptos Computacionales. *San Marcos*, 3–14. https://repositorio.usam.ac.cr/xmlui/handle/11506/956

Maino, V. (2022). Estrategia Nacional de Ciberseguridad del Ecuador. *Ministerio de Telecomunicaciones y de La Sociedad de La Información*, 30–45. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Martínez, D. (2023). *Software Contable: Setca Soft*. https://setca-group.com/setca-soft/

Meljem, S. (2018). Gobierno Corporativo: Su importancia en la objetividad e independencia de la función de auditoría interna. *IE Contadores Públicos*, *1*, 45–103. https://elibro.net/es/lc/uta/titulos/116950

Menéndez, S. (2022). Auditoría de la Seguridad Informática. *Rama Editorial*, 230–324. https://www.digitaliapublishing.com/a/116389

Michelena, J. (2023, June 25). *Ciberseguridad*. Cepreven. https://www.cepreven.com/cuestionario-ciberseguridad/

Moraga, C. (2023, January 8). *Guía para entender la matriz de riesgo*. Safety Culture. https://safetyculture.com/es/temas/evaluacion-de-riesgos/matriz-de-riesgo/

Moreno, C. (2020). Guía para la Implementación de la Seguridad de la Información. *Ministerio de Telecomunicaciones y de La Sociedad de La Información*, 12–34. https://www.gobiernoelectronico.gob.ec/wp-

content/uploads/2020/04/GU%C3%8DA-PARA-LA-IMPLEMENTACI%C3%93N-DEL-EGSI-ABRIL2020.pdf

Pelanzas, Á. (2022). Planificación de la Auditoría. *Paraninfo*, *UF0317*, 77–98. https://books.google.com.ec/books?id=2gBtDwAAQBAJ&printsec=copyright#v=onepage&q&f=false

Pérez, E. (2016). Consideraciones Técnicas para el Diseño de Transformadores de Medida de Corriente. *Revista Científica UISRAEL*, *3*(2), 54–73. http://www.editorialjuridicadelecuador.com/contacto

Ponce, J. (2017). Ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, *20*, 17–68. http://revistas.flacsoandes.edu.ec/index.php/URVIO

Ramos, J. (2020). Delitos contra la seguridad de los activos de los sistemas de información y comunicación en el Ecuador. *Corporación de Estudios y Publicaciones.*, 18–33. https://elibro.net/es/lc/uta/titulos/171995

Rivera, S. (2013). Modelo de gestión para las empresas familiares con perspectivas de crecimiento y sostenibilidad. *Redalyc*, *31*, 3–30. https://www.redalyc.org/pdf/4259/425941261003.pdf

Sánchez, F. (2018). Plan de Implementación de la ISO/IEC 27001:2013. *San Mateo*, 74–96. https://openaccess.uoc.edu/bitstream/10609/81145/6/feduardosanchezTFM0618memoria.pdf

Sánchez, P., García, J., Triana, A., & Pérez, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información Tecnológica*, *32*(5), 145–156. https://doi.org/10.4067/s0718-07642021000500145

Toapanta, S., De La Rosa, F., Fernandez, E., Trivino, F., & Gallegos, L. (2019). Prototype to Optimize the Management of Information Security Used by Internal Users in a Public Organization of Ecuador. *International Conference on Computer, Information and Telecommunication Systems*, 1–5. https://doi.org/10.1109/CITS.2019.8862103

Valencia, N., Yulán, C., & Chipe, B. (2023). Resiliencia en la informática. *Recimundo*, *7*(1), 79–86. https://doi.org/10.26820/recimundo/7.(1).enero.2023.79-86

Vidaline, F. (2009). Análisis y evaluación de riesgo de la información. *Dialnet*, *1*, 2–12. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004

Vieites, A. (2011). Seguridad Informática. *Digitalia*, 35–67. https://www.digitaliapublishing.com/a/70537

Zuñiga, A., Serrano, I., & Molina, L. (2020). Seguridad informática en las PyMES de la ciudad de Quevedo. *Journal of Business*, *4*(2). https://journalbusinesses.com/index.php/revista/article/view/97/221