



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
CARRERA CONTABILIDAD Y AUDITORÍA

**AUDITORÍA INFORMÁTICA A LA EMPRESA SERVISILVA CÍA.
LTDA. DEL CANTÓN FRANCISCO DE ORELLANA, PROVINCIA
DE ORELLANA, PERÍODO 2020.**

Trabajo de Integración Curricular

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

LICENCIADA EN CONTABILIDAD Y AUDITORÍA CPA

AUTORA:

PAULA ANDREA JARAMILLO MOREIRA

Riobamba – Ecuador

2023



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
CARRERA CONTABILIDAD Y AUDITORÍA

**AUDITORÍA INFORMÁTICA A LA EMPRESA SERVISILVA CÍA.
LTDA. DEL CANTÓN FRANCISCO DE ORELLANA, PROVINCIA
DE ORELLANA, PERÍODO 2020.**

Trabajo de Integración Curricular

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

LICENCIADA EN CONTABILIDAD Y AUDITORÍA CPA

AUTORA: PAULA ANDREA JARAMILLO MOREIRA

DIRECTOR: ING. HÍTALO VELOZ SEGOVIA

Riobamba – Ecuador

2023

© 2023, Paula Andrea Jaramillo Moreira

Se autoriza la reproducción total o parcial con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.

Yo, Paula Andrea Jaramillo Moreira, declaro que el presente Trabajo de Integración Curricular es de mi autoría y que los resultados del mismo son auténticos. Los textos en el documento que proviene de otras fuentes están debidamente citados y referenciados.

Como autora asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Integración Curricular, el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 18 de enero de 2023

A handwritten signature in blue ink, reading "Paula Jaramillo", is placed on a light-colored rectangular background.

Paula Andrea Jaramillo Moreira
C.C: 070681886-1

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
CARRERA CONTABILIDAD Y AUDITORÍA

El Tribunal del Trabajo de Integración Curricular certifica que: El Trabajo de Integración Curricular, Tipo: Proyecto de Investigación, **AUDITORÍA INFORMÁTICA A LA EMPRESA SERVISILVA CÍA. LTDA. DEL CANTÓN FRANCISCO DE ORELLANA, PROVINCIA DE ORELLANA, PERÍODO 2020**, realizado por la señorita: **PAULA ANDREA JARAMILLO MOREIRA**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

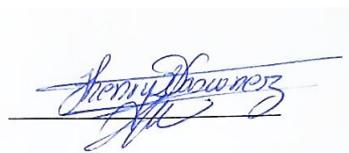
FIRMA

FECHA

Ing. Henry David Vásconez Vásconez

2023/01/18

PRESIDENTE DEL TRIBUNAL



Ing. Hítalo Bolívar Veloz Segovia

**DIRECTOR DEL TRABAJO DE
INTEGRACIÓN CURRICULAR**



2023/01/18

Ing. Willian Geovanny Yanza Chávez

**ASESOR DEL TRABAJO DE
INTEGRACIÓN CURRICULAR**



2023/01/18

DEDICATORIA

Dedico el presente trabajo de investigación en primer lugar a Dios y a la Virgen María, por ampararme bajo su bendición, por haberme brindado esa sabiduría y fortaleza necesaria para culminar con mis estudios.

A mis padres Ángel Jaramillo y Marisol Moreira quienes han sido un pilar fundamental a lo largo de mi vida personal y profesional, siendo las personas más importantes para mí, contando siempre con su apoyo incondicional.

A mis hermanos Ileana y Mauricio, por ser mi fuente de inspiración para poder superarme día a día, y haberme brindado su apoyo en todo momento. Y a mi sobrina Dariana.

A mi familia y a mis amigos que de alguna u otra manera contribuyeron para de esa manera poder realizarme profesionalmente.

Paula

AGRADECIMIENTO

A Dios y a la Virgen María por caminar junto a mí lo largo de esta maravillosa trayectoria lo que permitió cumplir con dicha meta tan anhelada.

A la Escuela Superior Politécnica de Chimborazo la cual me otorgó la oportunidad de cursar mis estudios en tan prestigiosa institución y convertirme en profesional obteniendo los conocimientos necesarios para el ejercicio de la carrera.

A todos aquellos docentes de la Escuela de Contabilidad de Auditoría, de manera especial al Ing. Hítalo Veloz e Ing. Willian Yanza, por todo su apoyo, quienes me han sabido guiar con sus conocimientos en el desarrollo del presente trabajo de integración curricular.

A la Empresa Servisilva Cía. Ltda. por haberme abierto sus puertas y poder realizar mi trabajo de investigación en dicha institución.

Paula

TABLA DE CONTENIDO

ÍNDICE DE TABLAS.....	x
ÍNDICE DE GRÁFICOS.....	xii
ÍNDICE DE FIGURAS.....	xiv
ÍNDICE DE ANEXOS.....	xv
RESUMEN.....	xvi
ABSTRACT.....	xvii
INTRODUCCIÓN.....	1

CAPÍTULO I

1. MARCO TEÓRICO REFERENCIAL.....	2
1.1. Planteamiento del problema.....	2
1.1.1. <i>Título.....</i>	2
1.1.2. <i>Planteamiento del problema.....</i>	2
1.1.3. <i>Formulación del problema.....</i>	3
1.1.4. <i>Sistematización del problema.....</i>	3
1.1.5. <i>Objetivos.....</i>	3
1.1.6. <i>Justificación.....</i>	4
1.2. Antecedentes de Investigación.....	5
1.3. Marco Teórico.....	6
1.3.1. <i>Reseña histórica de la auditoría.....</i>	6
1.3.2. <i>Definición de Auditoría.....</i>	7
1.3.3. <i>Definición de Auditoría Informática.....</i>	7
1.3.4. <i>Objetivos de la Auditoría Informática.....</i>	8
1.3.5. <i>Tipos de Auditoría Informática.....</i>	9
1.3.6. <i>Ámbito de la Auditoría Informática.....</i>	10
1.3.7. <i>Control Interno Informático.....</i>	10
1.3.7.1. <i>Definición Control Interno Informático.....</i>	10
1.3.7.2. <i>Tipos de Controles Internos Informáticos.....</i>	10
1.3.8. <i>Normas, Técnicas y Estándares de Auditoría Informática.....</i>	11
1.3.8.1. <i>Control Objectives for Information and Related Technology, COBIT.....</i>	11
1.3.8.2. <i>Information Technology Infrastructure Library, ITIL.....</i>	12
1.3.8.3. <i>Normas ISO.....</i>	13
1.3.8.4. <i>Committee Of Sponsoring Organizations Of The Treadway Commission, COSO.....</i>	13

1.3.9.	<i>Proceso de la Auditoría Informática</i>	16
1.3.9.1.	<i>Planificación de la auditoría informática</i>	16
1.3.9.2.	<i>Ejecución de la auditoría informática</i>	16
1.3.9.3.	<i>Comunicación de resultados de la auditoría informática</i>	17
1.3.10.	<i>Riesgos de Auditoría</i>	17
1.3.11.	<i>Pruebas de Auditoría</i>	17
1.3.12.	<i>Evidencia</i>	18
1.3.12.1.	<i>Tipos de evidencia</i>	18
1.3.13.	<i>Hallazgos de Auditoría</i>	18
1.3.13.1.	<i>Atributos del hallazgo</i>	19
1.3.14.	<i>Papeles de Trabajo</i>	19
1.3.14.1.	<i>Objetivos de los Papeles de Trabajo</i>	19
1.3.14.2.	<i>Tipos de Papeles de Trabajo</i>	20
1.3.15.	<i>Marcas de Auditoría</i>	20
1.3.16.	<i>Informe de Auditoría</i>	21
1.3.16.1.	<i>Objetivos del informe de auditoría:</i>	21
1.3.17.	<i>Riesgo Informático</i>	21
1.3.18.	<i>Seguridad Informática</i>	22

CAPÍTULO II

2.	MARCO METODOLÓGICO	24
2.1.	Enfoque de investigación	24
2.2.	Nivel de investigación	24
2.2.1.	<i>Exploratoria</i>	24
2.2.2.	<i>Descriptiva</i>	24
2.2.3.	<i>Explicativa</i>	25
2.3.	Diseño de investigación	25
2.4.	Tipo de estudio	25
2.4.1.	<i>Investigación Documental</i>	25
2.4.2.	<i>Investigación de campo</i>	25
2.5.	Población y planificación, selección y cálculo del tamaño de la muestra	25
2.5.1.	<i>Población</i>	25
2.5.2.	<i>Muestra</i>	26
2.6.	Métodos, técnicas e instrumentos de investigación	26
2.6.1.	<i>Métodos</i>	26
2.6.1.1.	<i>Inductivo</i>	26

2.6.1.2.	<i>Deductivo</i>	26
2.6.1.3.	<i>Analítico</i>	27
2.6.2.	<i>Técnicas</i>	27
2.6.2.1.	<i>Observación</i>	27
2.6.2.2.	<i>Encuesta</i>	27
2.6.3.	<i>Instrumentos</i>	27
2.6.3.1.	<i>Guía de encuestas</i>	27
2.6.3.2.	<i>Guía de observación</i>	27

CAPÍTULO III

3.	MARCO DE RESULTADOS Y DISCUSIÓN DE RESULTADOS	28
3.1.	Resultados	28
3.1.1.	<i>Encuesta</i>	28
3.2.	Desarrollo de la propuesta	69
3.2.1.	<i>Archivo Permanente</i>	70
3.2.2.	<i>Archivo Corriente</i>	90
3.2.2.1.	<i>Fase I: Planificación</i>	92
3.2.2.2.	<i>Fase II: Ejecución</i>	99
3.2.2.3.	<i>Fase III: Comunicación de Resultados</i>	130

CONCLUSIONES	141
---------------------------	-----

RECOMENDACIONES	142
------------------------------	-----

GLOSARIO

BIBLIOGRAFÍA

ANEXOS

ÍNDICE DE TABLAS

Tabla 1-2:	Población.....	26
Tabla 1-3:	Protección de los equipos tecnológicos.....	28
Tabla 2-3:	Plan de Contingencia.....	29
Tabla 3-3:	Sistema de Videovigilancia.....	30
Tabla 4-3:	Instalaciones eléctricas.....	31
Tabla 5-3:	Mantenimientos preventivos.....	32
Tabla 6-3:	Frecuencia de mantenimientos preventivos.....	33
Tabla 7-3:	Tiempo para implementar mantenimientos correctivos.....	34
Tabla 8-3:	Registro de los mantenimientos.....	35
Tabla 9-3:	Programas en contra de softwares maliciosos.....	36
Tabla 10-3:	Contraseñas en el sistema informático.....	37
Tabla 11-3:	Respaldos de información.....	38
Tabla 12-3:	Frecuencia en el cambio de claves.....	39
Tabla 13-3:	Inventario de los equipos.....	40
Tabla 14-3:	Equipos tecnológicos adicionales.....	41
Tabla 15-3:	Políticas de seguridad y manejo.....	42
Tabla 16-3:	Conocimiento de las políticas de seguridad.....	43
Tabla 17-3:	Calidad del internet.....	44
Tabla 18-3:	Interruptores de energía y cables de red.....	45
Tabla 19-3:	Página web.....	46
Tabla 20-3:	Necesario realizar auditoría informática.....	47
Tabla 21-3:	Desempeño de equipos tecnológicos.....	48
Tabla 22-3:	Conocimiento de las políticas de seguridad.....	49
Tabla 23-3:	Estado de los equipos tecnológicos.....	50
Tabla 24-3:	Instalaciones eléctricas.....	51
Tabla 25-3:	Sistema informático.....	52
Tabla 26-3:	Programas de protección.....	53
Tabla 27-3:	Respaldos de información.....	54
Tabla 28-3:	Mantenimientos preventivos.....	55
Tabla 29-3:	Frecuencia de mantenimientos preventivos.....	56
Tabla 30-3:	Mantenimientos correctivos.....	57
Tabla 31-3:	Tiempo para implementar mantenimiento correctivo.....	58
Tabla 32-3:	Calificación de mantenimientos brindados.....	59
Tabla 33-3:	Contraseñas.....	60

Tabla 34-3: Página web o aplicación móvil.....	61
Tabla 35-3: Servicio de internet.....	62
Tabla 36-3: Necesario realizar una auditoría informática.....	63
Tabla 37-3: Conocimiento de las políticas de seguridad	64
Tabla 38-3: Página web o aplicación móvil.....	65
Tabla 39-3: Instalaciones eléctricas	66
Tabla 40-3: Servicio de internet.....	67
Tabla 41-3: Ejecución de auditoría informática.....	68

ÍNDICE DE GRÁFICOS

Gráfico 1-3:	Protección de los equipos tecnológicos.....	28
Gráfico 2-3:	Plan de Contingencia.....	29
Gráfico 3-3:	Sistema de videovigilancia.....	30
Gráfico 4-3:	Instalaciones eléctricas.....	31
Gráfico 5-3:	Mantenimientos preventivos.....	32
Gráfico 6-3:	Frecuencia mantenimientos preventivos.....	33
Gráfico 7-3:	Tiempo para implementar mantenimientos correctivos.....	34
Gráfico 8-3:	Registro de los mantenimientos.....	35
Gráfico 10-3:	Contraseñas en el sistema informático.....	37
Gráfico 11-3:	Respaldos de información.....	38
Gráfico 12-3:	Frecuencia en el cambio de claves.....	39
Gráfico 14-3:	Equipos tecnológicos adicionales.....	41
Gráfico 15-3:	Políticas de seguridad y manejo.....	42
Gráfico 16-3:	Conocimiento de las políticas de seguridad.....	43
Gráfico 17-3:	Calidad del internet.....	44
Gráfico 18-3:	Interruptores de energía y cables de red.....	45
Gráfico 19-2:	Página web.....	46
Gráfico 20-3:	Necesario realizar auditoría informática.....	47
Gráfico 21-3:	Desempeño de equipos tecnológicos.....	48
Gráfico 22-3:	Conocimiento de las políticas de seguridad.....	49
Gráfico 23-3:	Estado de los equipos tecnológicos.....	50
Gráfico 24-3:	Instalaciones eléctricas.....	51
Gráfico 25-3:	Sistema informático.....	52
Gráfico 26-3:	Programas de protección.....	53
Gráfico 27-3:	Respaldos de información.....	54
Gráfico 28-3:	Mantenimientos preventivos.....	55
Gráfico 29-3:	Frecuencia de mantenimientos preventivos.....	56
Gráfico 30-3:	Mantenimientos correctivos.....	57
Gráfico 31-3:	Tiempo para implementar mantenimiento correctivo.....	58
Gráfico 32-3:	Calificación de mantenimientos brindados.....	59
Gráfico 33-3:	Contraseñas.....	60
Gráfico 34-3:	Página web o aplicación móvil.....	61
Gráfico 35-3:	Servicio de internet.....	62
Gráfico 36-3:	Necesario realizar una auditoría informática.....	63

Gráfico 37-3: Conocimiento de las políticas de seguridad	64
Gráfico 38-3: Página web o aplicación móvil.....	65
Gráfico 39-3: Instalaciones eléctricas	66
Gráfico 40-3: Servicio de internet.....	67
Gráfico 41-3: Ejecución de auditoría informática.....	68

ÍNDICE DE FIGURAS

Figura 1-1: Tipos de Auditoría Informática.....	9
Figura 2-1: Ámbito de la Auditoría Informática.....	10
Figura 3-1: Tipos de Controles Internos Informáticos.....	10
Figura 4-1: Principios de COBIT 5.....	11
Figura 5-1: Componentes del COSO II	15
Figura 6-1: Tipos de Papeles de Trabajo	20
Figura 1-3: Metodología de Auditoría Informática	69
Figura 2-3: Ubicación Empresa Servisilva Cía. Ltda.	83
Figura 3-3: Logo Empresa Servisilva Cía. Ltda.	85
Figura 4-3: Vista Exterior Servisilva Cía. Ltda.....	94

ÍNDICE DE ANEXOS

ANEXO A: DOCUMENTACIÓN

ANEXO B: RUC SERVISILVA CÍA. LTDA

ANEXO C: FICHA MANTENIMIENTO CORRECTIVO A COBERTURA DE RED

ANEXO D: CÁMARAS DE SEGURIDAD

ANEXO E: FICHA DE INVENTARIO

ANEXO F: POLÍTICAS DE SEGURIDAD INFORMÁTICAS

ANEXO G: ETIQUETAS DE RESPALDOS DE BASE DE DATOS POR ÁREA

RESUMEN

El presente trabajo de integración curricular tuvo como finalidad la ejecución de una auditoría informática a la Empresa Servisilva Cía. Ltda., de la provincia de Orellana, la cual se encuentra ubicada Km 7 ½ Vía Lago Agrio, del período 1 de enero al 31 de diciembre del 2020, con el objetivo de conocer el manejo y uso de los equipos tecnológicos de la empresa. Para el desarrollo de la auditoría se aplicó encuestas al personal administrativo, operativo y encargado al área de sistemas, visitas, observación directa, lo cual permitió conocer la situación actual de la empresa, como así también, se aplicó cuestionarios de control interno mediante el método del COSO II, posibilitando la identificación de hallazgos, entre los que se puede encontrar los siguientes: carencia de un plan informático estratégico, falta de seguridad en el área de sistemas en donde se encuentra ubicado el servidor, inexistencia de un plan de contingencia que permita salvaguardar los equipos tecnológicos y no se llevan a cabo evaluaciones de control interno en Servisilva Cía. Ltda.. Mediante emisión de informe de auditoría se recomienda a las autoridades y personal encargado del área de sistemas desarrollar métodos, planes, que proporcionen seguridad a los equipos tecnológicos y salvaguardar la confiabilidad e integridad de la información de la organización, a fin de que se tomen medidas preventivas y correctivas en beneficio del desarrollo de la empresa Servisilva Cía. Ltda.

Palabras claves: <CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS>, <AUDITORÍA INFORMÁTICA>, <CONTROL INTERNO>, <EQUIPOS TECNOLÓGICOS>, <COSO II>.



27-02-2023

0394-DBRA-UPT-2023

ABSTRACT

The fundamental purpose of this research was to conduct a computer audit of the Company Servisilva Limited Company from the province of Orellana, located at Km 7 ½ Vía Lago Agrio, from January 1 to December 31, 2020. The computer audit developed in this research aimed to get involved with the management procedures and use of the company's technological equipment. In addition, surveys addressed to the administrative, operational and personnel in charge of the systems area were necessary, as well as visits and direct observation. This process led to knowing the current situation of the company. Other essential aspects involved using internal control questionnaires by the COSO II method, which made it possible to identify findings, such as a lack of a strategic IT plan, lack of security in the systems area where the server is located, lack of a contingency plan to safeguard the technological equipment and internal control, and finally, the evaluations in Servisilva Limited Company need to be performed. For this reason, by issuing an audit report, it is recommended that the authorities and personnel in charge of the systems area develop methods and plans that provide security to the technological equipment and safeguard the reliability and integrity of the organization's information so that preventive and corrective measures are taken for the benefit of the development of the company Servisilva Cía. Ltd.

Keywords: <ECONOMIC AND ADMINISTRATIVE SCIENCES>, <COMPUTER AUDIT>, <INTERNAL CONTROL>, <TECHNOLOGICAL EQUIPMENT>, <COSO II>.

A handwritten signature in blue ink, appearing to read 'Mónica Logroño Becerra', written over a horizontal line.

Lic. Mónica Logroño Becerra
C.I: 060274953-3

INTRODUCCIÓN

El presente el trabajo de integración curricular está enfocado en la ejecución de una Auditoría Informática a la empresa Servisilva Cía. Ltda., de la ciudad de Francisco de Orellana, durante el periodo comprendido entre el 1 de enero al 31 de diciembre 2020, en el cual el uso de recursos tecnológicos es parte de sus actividades diarias, donde se presentan falencias en los equipos y sistemas informáticos, es por ello que, se debe contar con sistemas de control interno y medidas de seguridad precautelando la integridad, confiabilidad y disponibilidad de la información, contrarrestando posibles riesgos informáticos.

CAPÍTULO I: Se encuentra conformado por el planteamiento del problema de la investigación, delimitación de problema, justificación desde la perspectiva teórica, metodológica y práctica, objetivos generales y específicos que permiten alcanzar el desarrollo del presente trabajo de integración curricular, además se encuentra el sustento del marco teórico de la Auditoría Informática en base a las variables de estudio, se recurrió en la investigación de teoría en varios autores para sustentar la propuesta y desarrollo de la investigación, consta de los antecedentes históricos y fundamentación teórica.

CAPÍTULO II: Está determinado por la metodología a emplearse, nivel de población y métodos, técnicas e instrumentos de recolección de la información para el desarrollo del presente trabajo investigativo.

CAPÍTULO III: Se encuentra estructurado por el marco propositivo, justificación y propuesta en la cual contiene el desarrollo de auditoría: planificación, ejecución y comunicación de resultados, obteniendo hallazgos y finalmente el informe de auditoría informática.

CAPÍTULO I

1. MARCO TEÓRICO REFERENCIAL

1.1. Planteamiento del problema

1.1.1. Título

Auditoría Informática a la Empresa Servisilva Cía. Ltda. del cantón Francisco de Orellana, Provincia de Orellana, período 2020.

1.1.2. Planteamiento del problema

En la Provincia de Orellana, Cantón Puerto Francisco de Orellana, se encuentra ubicada la empresa Servisilva Cía. Ltda. Institución fundada el 28 de junio de 1995, misma que ofrece servicios de revestimiento, roscado y maquinados en general, tratamiento térmico y trabajos relacionados al sector petrolero brindando soluciones a lo largo de la industria.

Por lo cual, existen áreas que requieren de recursos tecnológicos, tanto hardware como software para facilitar el desarrollo de las actividades, dichas áreas necesitan de determinados recursos a fin de contribuir al buen manejo de la información ya sea de un proceso a elaborar, trámites administrativos, operaciones generales o cualquier tipo de información fundamental para la gestión empresarial.

Hoy en día Servisilva Cía. Ltda. labora en base a una red compartida denominada SocServer que permite compartir información entre cada uno de los departamentos con unidades tecnológicas de manera simultánea.

Al realizar un breve diagnóstico, se pudo evidenciar una serie de irregularidades tales como:

- ✓ El software instalado no se encuentra sujeto a evaluaciones de control interno poniendo en riesgo la seguridad de la información.
- ✓ Falta de políticas y procedimientos que aseguren la eficacia en la administración de los recursos informáticos.
- ✓ No ha sido objeto de una auditoría informática anteriormente.
- ✓ No cuentan con indicadores que comprueben el nivel de eficiencia en cuanto al uso de los equipos incidiendo en el desenvolvimiento de estos.

- ✓ No existe seguridad informática en el software donde reposa la información de todas las actividades, gestiones, operaciones y procesos de la empresa.
- ✓ En determinadas áreas no se posee una correcta instalación eléctrica de los equipos de cómputo, por lo que representa un problema en el desarrollo de sus actividades diarias.
- ✓ No se encuentran instaladas cámaras de seguridad en el lugar donde se localiza el servidor de la empresa.

Con estos antecedentes identificados es necesaria la ejecución de una auditoría informática, que comprenderá la evaluación de los recursos informáticos apoyada en la composición del control interno con la finalidad de contribuir al crecimiento empresarial de Servisilva Cía. Ltda. y hacer de ella una de las mejores en la provincia de Orellana puesto que no ha sido objeto a este tipo de auditoría.

1.1.3. Formulación del problema

¿De qué manera la Auditoría Informática contribuirá en la evaluación de los equipos tecnológicos de la Empresa Servisilva Cía. Ltda., en el cantón Francisco de Orellana, Provincia de Orellana, período 2020?

1.1.4. Sistematización del problema

- ✓ ¿Cómo realizar una evaluación que sirva de base para conocer la situación actual de los equipos tecnológicos de la empresa?
- ✓ ¿Qué herramientas, técnicas e instrumentos aplicar en la ejecución de la auditoría informática en la empresa Servisilva Cía. Ltda.?
- ✓ ¿Cómo ejecutar la auditoría informática a Servisilva Cía. Ltda.?

1.1.5. Objetivos

1.1.5.1. Objetivo General

Ejecutar una Auditoría Informática a la Empresa Servisilva Cía. Ltda., mediante la aplicación de técnicas de auditoría, para obtener un informe que permita conocer los resultados en el manejo de los equipos tecnológicos, durante el período 2020.

1.1.5.2. Objetivos Específicos

- ✓ Fundamentar el marco teórico a través de la revisión de fuentes secundarias de información para sustentar el proyecto de investigación de Auditoría Informática.
- ✓ Aplicar técnicas de investigación mediante la utilización de instrumentos, que se emplearan en áreas con equipos tecnológicos para determinar la situación de estos.
- ✓ Ejecutar una Auditoría Informática en la Empresa Servisilva Cía. Ltda. durante el período 2020, para emitir recomendaciones y conclusiones a través de la emisión del informe.

1.1.6. Justificación

1.1.6.1. Justificación teórica

La auditoría informática consiste en la evaluación y control de los sistemas informáticos de una empresa mediante la aplicación de técnicas y herramientas de auditoría, a fin de conocer el manejo de la gestión y seguridad informática.

La presente investigación es necesaria ya que en la Empresa Servisilva Cía. Ltda., se ha evidenciado una ausencia en el control de equipos tecnológicos, pues no ha sido objeto de este tipo de auditoría. Para el desarrollo del trabajo se realizará un análisis teórico concerniente a Auditoría Informática donde se considerará toda información secundaria mediante la utilización de libros, ensayos, artículos científicos, páginas web académicas, entre otros.

La viabilidad de este proyecto de investigación se basa por el aporte que representa identificar las condiciones actuales de los equipos informáticos, proporcionando resultados indispensables para la organización que contribuye a la eficiencia y eficacia de sus operaciones.

1.1.6.2 Justificación metodológica

En el presente trabajo de investigación se empleará métodos, técnicas e instrumentos de investigación primordiales para la recopilación de información principal, confiable y oportuna del trabajo investigativo como lo es la Auditoría Informática, debido a que los resultados obtenidos son la base primordial para la emisión de conclusiones y recomendaciones objetivas a fin de tomar las mejores decisiones a beneficio de la empresa.

A realizar con un enfoque exploratorio, ya que se requiere de información fundamental de la empresa para previo inicio del proyecto de investigación, y un enfoque descriptivo con el fin de detallar el comportamiento de los equipos tecnológicos percibiendo así su gestión y control.

1.1.6.3. Justificación práctica

Este trabajo investigativo tiene como propósito demostrar los conocimientos adquiridos dentro de la vida estudiantil en la escuela de Contabilidad y Auditoría, mismos que serán puestos en práctica en el momento de la aplicación de la Auditoría Informática a la Empresa Servisilva Cía. Ltda.

La investigación contribuye a la evaluación de cada uno de los recursos informáticos de la empresa, la cual inicie con una adecuada recolección de información estableciendo puntos importantes que permitan el correcto desarrollo de la auditoría informática. Siendo los beneficiarios directos la Empresa Servisilva Cía. Ltda., los accionistas y los empleados; y los beneficiarios indirectos los clientes.

1.2. Antecedentes de Investigación

Antes de construir la fundamentación teórica del presente trabajo investigativo, se tomó como base a otros proyectos investigativos referentes al tema de Auditoría Informática a fin de que sus principales conclusiones contribuyan de soporte en la investigación a realizarse.

En el repositorio digital ESPOCH (ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO):

Según (Neira, 2019, pág. 140) en su tema de investigación “Auditoría Informática a la Unidad Educativa Fiscomisional San Vicente de Paúl del cantón Riobamba, Provincia de Chimborazo, períodos 2016-2017”, concluye que:

La Unidad Educativa Fiscomisional San Vicente de Paúl no dispone con políticas, normas y procedimientos informáticos que aseguren la administración de los equipos tecnológicos, mismo que pone en riesgo a estos recursos con la pérdida de datos y amenaza de virus; por otra parte, no existe un sistema de control interno informático, debido al desconocimiento de las normas 410 (Tecnologías de Información) de la Contraloría General del Estado, lo que impide un adecuado desempeño en las actividades diarias institucionales.

Por su parte (Villena, 2019, pág. 228) en su trabajo de titulación denominado “Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del Cantón San Pedro de Pelileo, Provincia de Tungurahua, período 2016” concluye que: Las instalaciones físicas de la institución no son adecuadas para el funcionamiento de los equipos informáticos siendo estos vulnerables ante diversas situaciones como lo son los riesgos ambientales: cambios de temperatura, goteras, incendios exponiendo a peligros al personal que labora en la unidad de gestión tecnológica. Además, no se aplican indicadores de eficiencia en cuanto al uso de los equipos, incidiendo en la optimización de estos.

Para (Calapucha, 2020, pág. 204) con el tema de investigación “Auditoría Informática a la Unidad de Tecnologías de la Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del Cantón Loreto, Provincia de Orellana, período 2018”, cuyas conclusiones expresan lo siguiente: El GAD Municipal del Cantón Loreto no ha sido objeto de una Auditoría Informática, por lo que se presenta irregularidades en el software y hardware de los equipos informáticos generando perjuicios en las actividades cotidianas de la entidad, de tal manera no garantiza seguridad y confidencialidad de datos en la Unidades de las Tecnologías de la Información.

Una vez analizadas las referencias antes expuestas se pudo determinar que la ejecución de una Auditoría Informática dentro de cualquier institución es esencial, sin embargo en la actualidad no la aplican de manera correspondiente. Esta auditoría representa una gran importancia debido a que proporciona un control adecuado de los recursos informáticos midiendo su eficiencia y eficacia en la gestión empresarial. El presente trabajo será de gran utilidad a la problemática de la empresa debido a que no se ha realizado una auditoría informática en la Empresa Servisilva Cía. Ltda.

1.3. Marco Teórico

1.3.1. Reseña histórica de la auditoría

El surgimiento de la auditoría se remonta a los comienzos de la humanidad en la época prehistórica, cuando el ser humano se ve forzado a desarrollar el comercio, presentándose la necesidad de desarrollar y aplicar auditoría. “Desde el momento en que existió el comercio, se ejecutaron auditorías de algún tipo”.

El propósito principal de las primeras auditorías era hallar desfalcos y comprobar si las personas en posiciones de confianza se encontraban actuando e informando de una manera responsable. En la Revolución Industrial con el avance del comercio y de la producción, el auditor se vio en la necesidad de desarrollar nuevas habilidades y métodos para así asegurar la veracidad e integridad de la información procesada.

A inicios del siglo XX se sistematizan principios y técnicas de auditoría, integrándose funciones automatizadas con la creación de bases de datos que almacenan información necesaria mediante software especializados. En la actualidad la tecnología y la auditoría son una asociación necesaria, y que se mantendrá en constante crecimiento en los próximos años (Blanco, 2008, pág. 29).

1.3.2. Definición de Auditoría

“La auditoría en general, es un examen metódico y sistemático de una empresa que se desarrolla mediante la comprobación de operaciones registradas y la investigación de todos aquellos hechos que puedan tener relación con estas, a fin de establecer su corrección” (Salgado, Osuna, Sevilla, & Morales, 2017, pág. 3).

Para (Sandoval, 2012, pág. 28) la auditoría es el examen de las demostraciones y registros administrativos, en donde el auditor observa la integridad, exactitud y autenticidades de tales demostraciones, registros y documentos. De manera que la auditoría resulta un instrumento de gran importancia al momento de realizar las respectivas actividades de control dentro de las empresas, tomando en cuenta todo tipo de información, para de esta manera comprobar si eran exactos confrontando el registro con las operaciones y los documentos.

1.3.3. Definición de Auditoría Informática

Según (Echenique, 2013, pág. 17) establece que la auditoría informática es una actividad que ha sido desarrollada para proteger los activos asegurando los sistemas de los equipos informáticos, mantener la integridad de los datos y lograr alcanzar los objetivos de la organización en forma eficiente y eficaz.

Por otra parte, (Sánchez, 2021, pág. 77) menciona que la auditoría informática es la evaluación de riesgos y controles existentes en los sistemas de información, tiene como propósito comprobar si los equipos (hardware) y los aplicativos (software) se encuentran correctamente protegidos o si han sufrido alguna manipulación o alteración indebida. Finalmente, (Piattini Velthuis, Navarro, & Ruiz, 2015), mencionan que la auditoría informática es el proceso de recopilar, concentrar y evaluar

evidencias para determinar si un sistema informatizado protege los activos, mantiene la confidencialidad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

De acuerdo con las definiciones revisadas, se puede concluir que la Auditoría Informática consiste en un conjunto de procedimientos y técnicas que permiten evaluar el control de los sistemas informáticos de una empresa verificando si sus actividades se desarrollan eficientemente, de manera que permitan detectar con anterioridad las deficiencias y así poder disminuir posibles riesgos.

1.3.4. Objetivos de la Auditoría Informática

A continuación (Tamayo, 2001, pág. 11) expone los objetivos que persigue la auditoría informática:

- ✓ Evaluar las políticas generales de orden técnico en relación con el software, hardware, desarrollo, implementación, operación y mantenimiento de sistemas de información.
- ✓ Evaluar los recursos informáticos de la empresa con prioridad en su nivel tecnológico, producción de software y programas más recurrentes.
- ✓ Conocer las políticas generales y actitudes de los directivos frente a la auditoría y seguridad de los sistemas informáticos y proceder a hacer las recomendaciones pertinentes.
- ✓ Ejecutar un análisis de la concepción, implementación y funcionalidad de la seguridad aplicada a los sistemas de información.

1.3.5. Tipos de Auditoría Informática

Auditoría con la computadora
<ul style="list-style-type: none">• Se lleva a cabo con el apoyo de equipos de cómputo y sus programas, para evaluar cualquier tipo de actividades y operaciones.
Auditoría sin la computadora
<ul style="list-style-type: none">• Emplea de técnicas y procedimientos tradicionales, sin el uso de sistemas computacionales.• Evalúa el comportamiento y validez de las actividades que requieren el uso de sistemas informáticos en una área de cómputo.
Auditoría a la gestión informática
<ul style="list-style-type: none">• Se enfoca exclusivamente en la revisión de las funciones y actividades de tipo administrativo.• Tiene el propósito de dictaminar sobre la adecuada gestión administrativa de los sistemas computacionales de una empresa y del propio centro informático.
Auditoría al sistema de cómputo
<ul style="list-style-type: none">• Auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correcto del equipo de cómputo, hardware y software
Auditoría alrededor de la computadora
<ul style="list-style-type: none">• Revisión específica a toda actividad de los sistemas computacionales, de ser posible, dejar a un lado todos los aspectos particulares, especializados y técnicos de los sistemas.
Auditoría de la seguridad de los sistemas computacionales
<ul style="list-style-type: none">• Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado a la seguridad de un sistema de cómputo a fin de salvaguardar base de datos, redes e instalaciones de los equipos asegurando el buen funcionamiento del área de sistematización.
Auditoría a los sistemas de redes
<ul style="list-style-type: none">• Evaluación a las redes de una empresa considerando el tipo de red, topología, conexiones, accesos y otros aspectos relacionados.• Revisión del software institucional, información de las operaciones y hardware de un sistema
Auditoría integral a los centros de cómputo
<ul style="list-style-type: none">• Concentra todas las evaluaciones bajo una misma auditoría con un enfoque global del área de sistemas, a fin de evaluar en forma integral el manejo y control de los sistemas de cómputo.
Auditoría ISO-9000 a los sistemas computacionales
<ul style="list-style-type: none">• Tipo de auditoría muy especializada y específica que brinda una certificación de calidad a los sistemas, realizada únicamente por auditores especializados.• Su propósito fundamental es evaluar, dictaminar y certificar que la calidad de los sistemas computacionales se encuentren apegados a los requerimientos del ISO-9000.
Auditoría outsourcing
<ul style="list-style-type: none">• Se realiza esta auditoría para evaluar la calidad en el servicio de asesoría o procesamiento externo de información que proporciona una empresa a otra.
Auditoría ergonómica de sistemas computacionales
<ul style="list-style-type: none">• Evalúa la calidad, eficiencia y utilidad del entorno hombre-máquina-medio ambiente que rodea el uso de sistemas computacionales en una empresa, con la finalidad de proporcionar bienestar, confort y comodidad a los usuarios de los sistemas de cómputo.

Figura 1-1: Tipos de Auditoría Informática

Fuente: (Muñoz Razo, 2002)

Realizado por: Jaramillo, P. 2023.

1.3.6. *Ámbito de la Auditoría Informática*

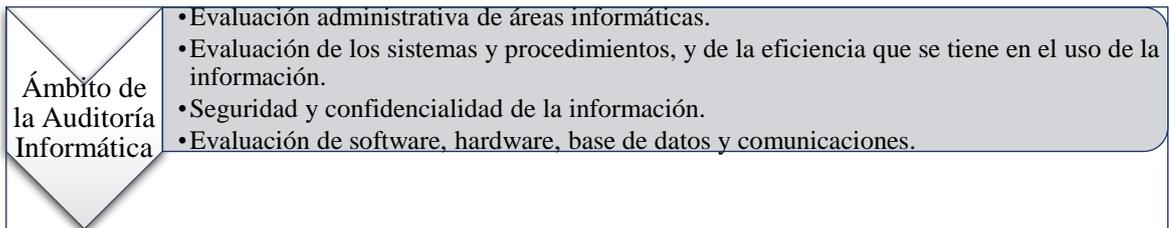


Figura 2-1: *Ámbito de la Auditoría Informática*

Fuente: (Echenique, 2001, pág. 20)

Realizado por: Jaramillo, P. 2023.

1.3.7. *Control Interno Informático*

1.3.7.1 *Definición Control Interno Informático*

Actividad o acción que se realiza para inspeccionar que todas las actividades de sistemas de información sean desarrolladas cumpliendo con los estándares, procedimientos y normas fijadas por la dirección de la institución o por el departamento de tecnologías de la información, a fin de prevenir y corregir errores o irregularidades que puedan afectar el cumplimiento de los objetivos empresariales (Piattini Velthuis, Navarro, & Ruiz, 2015, pág. 9).

1.3.7.2 *Tipos de Controles Internos Informáticos*

A lo largo de la historia, los controles informáticos se han clasificado en las siguientes categorías:

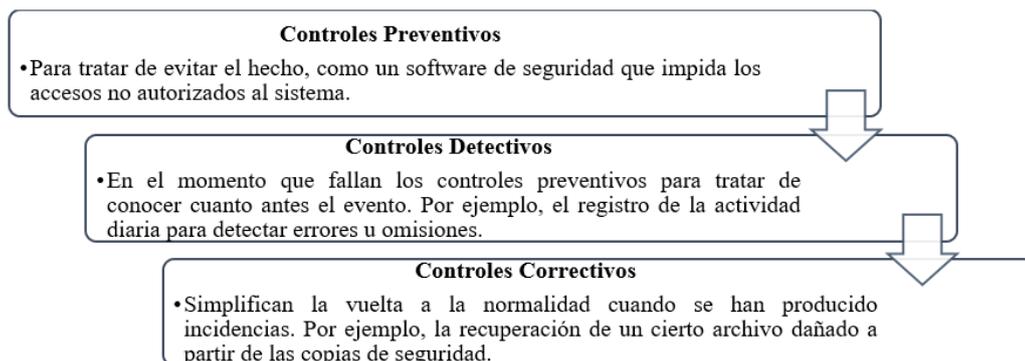


Figura 3-1: *Tipos de Controles Internos Informáticos*

Fuente: (Piattini Velthuis, Navarro, & Ruiz, 2015)

Realizado por: Jaramillo, P. 2023.

1.3.8 Normas, Técnicas y Estándares de Auditoría Informática

Actualmente el Ecuador cuenta con un marco regulatorio y normativo reducido en materia informática, por lo que se profundizaran en las normas y organizaciones internacionales más relevantes en este ámbito estableciendo políticas y lineamientos que garanticen el proceso de auditoría (Quintuña, 2012, pág. 18).

1.3.8.1 Control Objectives for Information and Related Technology, COBIT

Es un marco de referencia que se fundamenta en los objetivos de control existente de la InformationSystems Audit and Control Foundation (ISACF), es un modelo que posee una estructura con un marco de acción donde se ajustan los razonamientos de investigación como son la seguridad y eficacia, se verifican los recursos que perciben la tecnología de información, mediante recurso humano, instalaciones técnicas, entre otras y, al final una valoración sobre los métodos involucrados en la organización.

Misión: “Investigar, desarrollar, publicar y promover un conjunto de objetivos de control generalmente aceptados por las tecnologías de la información que sea autorizado y actualizado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocios, profesionales de TI y profesionales de aseguramiento” (COBIT 5, 2012).

Principios

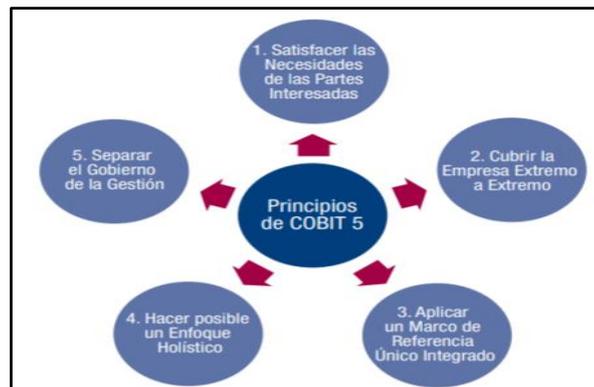


Figura 4-1: Principios de COBIT 5

Fuente: (COBIT 5, 2012)

Realizado por: Jaramillo, P. 2023.

1.3.8.2. *Information Technology Infrastructure Library, ITIL*

Es un conjunto de las mejores prácticas para la gestión de servicios de tecnologías de la información, incluye 4 dimensiones que proveen a las empresas flexibilidad y estabilidad para ofrecer servicios de TI, entre las que se halla:

- **Organización y Personas:** trata acerca de la cultura de la organización, roles, responsabilidades, sistemas de autoridad y comunicación.
- **Información y Tecnología:** relativo a la tecnología necesaria para la gestión de los servicios y sus relaciones.
- **Socios y Proveedores:** versa sobre las relaciones con otros que participan en una cadena de valor.
- **Flujos de Valor y Procesos:** integra el trabajo entre varias partes de la organización y su coordinación, así como la identificación y comprensión de los flujos de valor detectados por la organización.

La versión 4.0 de ITIL se define el Sistema de Valor del Servicio (SVS), el cual describe como todos los componentes y actividades de la organización trabajan juntos como un sistema para permitir la creación de valor. Estos componentes y actividades, junto con los recursos de la organización se combinan de una manera flexible a medida que cambian las circunstancias, por lo que se trata de hacer una revisión y corrección de los procesos, y de realizar una documentación apropiada para que de esta manera la información permita brindar un adecuado soporte a estos servicios.

ITIL define práctica como un conjunto de recursos organizacionales diseñados para realizar un trabajo o cumplir un objetivo, se presentan las prácticas más relevantes basadas en la cadena de valor de servicio y alineadas a las cuatro dimensiones.

- ✓ **Gestión de incidentes:** propone recuperar la operación de los servicios en el menor tiempo posible de manera que no se propicie una baja en los niveles de calidad y disponibilidad, minimizando así el impacto desfavorable a las operaciones de la institución. Los incidentes tanto de software como hardware son atendidos para el proceso de gestión de incidentes.
- ✓ **Gestión de problemas:** prevenir problemas e incidentes producidos por errores de la infraestructura de TI, encontrando sus causas y por ende darles tratamiento e implementar soluciones. Esta gestión de problemas pretende hallar una solución permanente cuyo objetivo principal es identificar la causa principal del incidente, darles solución y prevenirlo.
- ✓ **Control de cambios:** pretende brindar garantía en los métodos y procedimientos que se usan a la hora de realizar cambios, permite minimizar el impacto que producen los incidentes y problemas en la infraestructura. Para tener una buena gestión de cambios es fundamental

tomar en cuenta la evaluación del riesgo, la continuidad del negocio, los requerimientos de recursos y su aprobación.

- ✓ **Gestión de niveles de servicio:** su función es proteger el ambiente de producción y servicios, cuidando el software, hardware y los elementos relacionados, asegurando que estén en uso solamente las versiones correctas probadas autorizadas, garantizando que los componentes utilizados en determinados lugares son los adecuados y estén disponibles en el momento oportuno.

1.3.8.3. Normas ISO

Las normas ISO/IEC 27000 integran una familia de estándares, desarrolladas por la International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC), dichos normas se publicaron ante la necesidad de contar con una base para la gestión de la seguridad de la información, detallando los requisitos para establecer, implementar, controlar, mantener e innovar un Sistema de Gestión de Seguridad de la Información (SGSI).

La serie ISO 27000 está formada por varias normas. Son consideradas como normas base: ISO 27001 e ISO 27002, mientras que las normas complementarias son principalmente: ISO 27003, ISO 27004, e ISO 27005.

1.3.8.4. Committee Of Sponsoring Organizations Of The Treadway Commission, COSO

Fue desarrollado con el objetivo de especificar el marco conceptual de control interno de las organizaciones, capaz de integrar las diferentes políticas y lineamientos que permiten alta dirección de sistemas de control interno. Hace recomendaciones a los encargados de TI sobre como evaluar, informar e implementar sistemas de control, teniendo como objetivo la efectividad y eficiencia de las operaciones, valoración de riesgos, actividades de control, información y comunicación y la verificación.

COSO I: El COSO I, está conformado por cinco componentes que fueron establecidos para evaluar el sistema de control de las empresas, está orientado a los diferentes campos y las diferentes áreas administrativas y operativas que permite el logro de objetivos, eficiencia y eficacia de las operaciones de la organización.

Componentes del Modelo COSO I:

1. Ambiente Interno de Control.
2. Evaluación de riesgos.
3. Actividades de control.
4. Información y Comunicación.
5. Supervisión.

COSO II – ERM: El 29 de septiembre del 2004 se lanzó el Marco de Control denominado COSO II que según su propio texto no contradice al COSO I, su enfoque es el mismo que el de COSO I pero basado en el riesgo, permite a las organizaciones mejoren sus prácticas de control interno o decidir encaminarse hacia un proceso más completo de gestión de riesgo. El Control Interno se define entonces como un proceso integrado a los procesos, y no un conjunto de mecanismos añadidos en uno mismo, llevado a cabo por el consejo de la administración, dirección y el resto del personal de una entidad, planteado con el objeto de proporcionar una garantía viable para el logro de objetivos (Acosta & Almeida, 2013).

Componentes

Los ocho componentes del COSO II se encuentran relacionados entre sí. Dichos procesos deben ser efectuados por el director, la gerencia y los demás miembros trabajadores de una determinada organización.

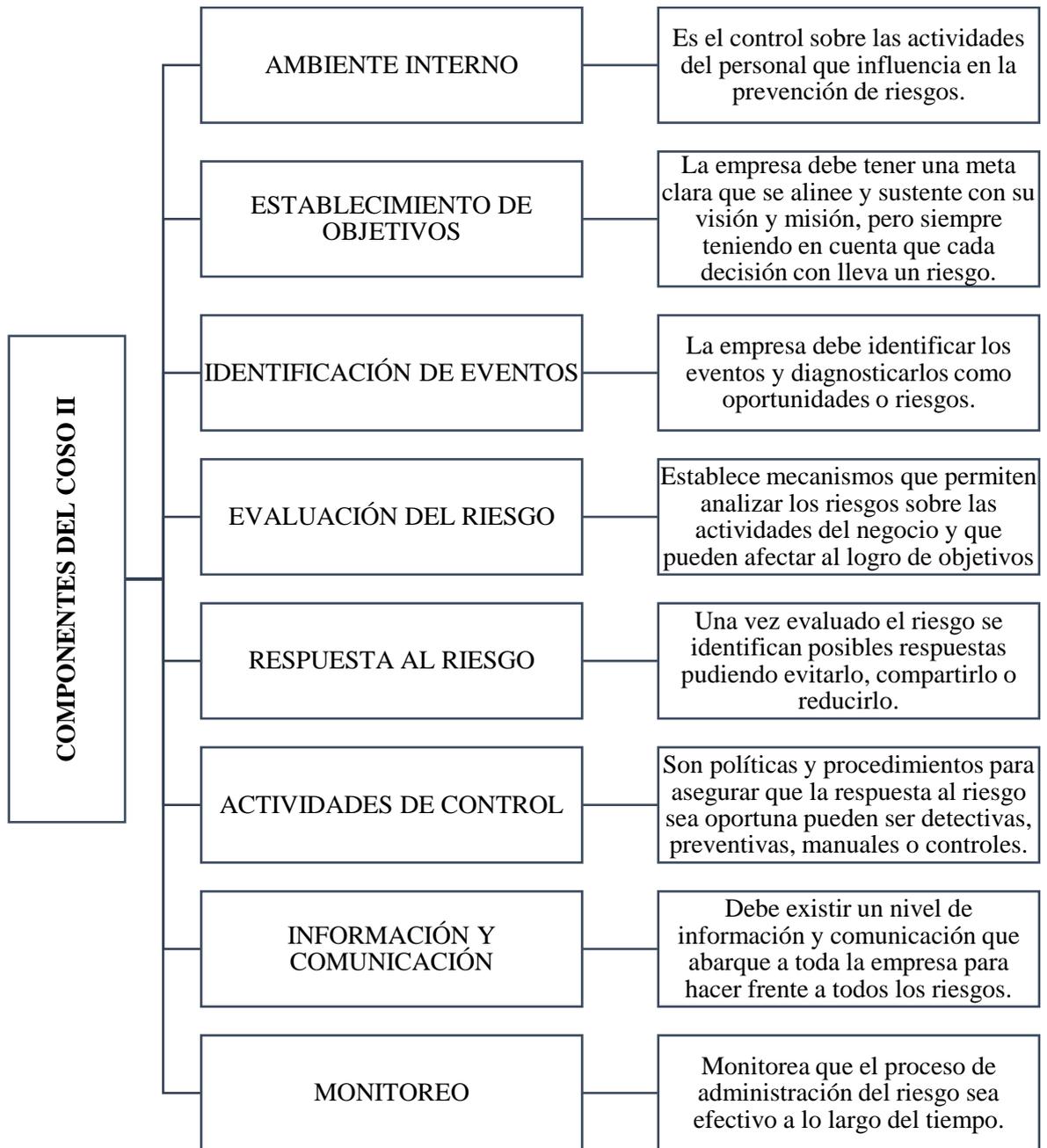


Figura 5-1: Componentes del COSO II

Realizado por: Jaramillo, P. 2023.

1.3.9. Proceso de la Auditoría Informática

El proceso de la auditoría informática se implementa con el propósito de salvaguardar los activos, asegurar la integridad de los datos y, la utilización racional de los recursos, con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias.

A continuación se detallan las etapas en un proceso de auditoría:

- Planificación de la auditoría Informática
- Ejecución de la auditoría informática
- Comunicación de resultados de la auditoría informática.

1.3.9.1. Planificación de la auditoría informática

En esta fase se establecen las relaciones entre auditores y colaboradores de la organización, para determinar el alcance y objetivos. Se realiza un análisis de la situación actual de la empresa, acerca su organización, controles internos, sistemas y demás elementos que le permitan al auditor elaborar el programa de auditoría que se llevará a efecto.

Elementos principales de esta Fase:

1. Conocimiento de la entidad
2. Objetivos y alcance de la auditoría
3. Análisis preliminar
4. Planeación específica de la auditoría
5. Elaboración de programas de auditoría

1.3.9.2. Ejecución de la auditoría informática

Constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones con respecto al manejo y administración de los equipos tecnológicos y área de sistemas. Para la recolección de información se pueden aplicar técnicas como cuestionarios, entrevistas entre otros, toda la información recopilada debe ser clasificada de manera que permita ubicarla fácilmente y además realizar un análisis respectivo, y justificar de manera correcta las recomendaciones. Obtenida una vez información real y confiable, se procede a evaluar los controles en la organización, para el mejoramiento continuo de la misma, por lo cual se obtendrá resultados reales.

1.3.9.3. Comunicación de resultados de la auditoría informática

Para finalizar un proceso de Auditoría Informática, se debe presentar un informe que contenga conclusiones y recomendaciones necesarias para que una empresa esté en mejoramiento continuo, esta documentación debe ser redactada por el equipo de auditoría.

1.3.10. Riesgos de Auditoría

El riesgo en auditoría, representa la posibilidad de que el auditor exprese una opinión errada en su informe, debido a que la información que se le proporciona al mismo se encuentre afectado por una distorsión material o normativa. En auditoría se conocen tres tipos de riesgo:

- ✓ **Riesgo inherente:** es la posibilidad de que existan errores significativos en la información auditada, al margen de la efectividad del control interno; son errores que no se pueden prever.
- ✓ **Riesgo de control:** está relacionado con la posibilidad de que los controles internos vigentes no prevean o detecten fallas que se estén dando en sus sistemas y que se pueden remediar con controles internos más efectivos.
- ✓ **Riesgo de detección:** está relacionado con el trabajo del auditor y, es que en la utilización de los procedimientos de auditoría, no detecte errores en la información que le suministran.

Este conjunto de riesgos es de aquellos que permiten que una organización o empresa mantenga claro cuáles son los riesgos que siempre deben estar pendiente de que no ocurra y pueda provocar algún tipo de desastre en dicha organización.

1.3.11. Pruebas de Auditoría

Las pruebas de auditoría se aplican solo los controles que en la evaluación de control interno presentaron un nivel de protección apropiado, dichas pruebas pueden ser realizadas con procedimientos manuales o asistidas por computadora.

Pruebas de cumplimiento: son el instrumento mediante el cual el auditor evalúa el sistema de control interno de la entidad auditada. Estas pruebas están encaminadas a comprobar:

- La existencia del control interno.
- La eficacia del mismo.
- Su continuidad durante el período.

Pruebas sustantivas: permiten obtener evidencia suficiente que proporciona al auditor emitir su juicio en las conclusiones acerca de cuándo puede ocurrir pérdidas materiales durante el procesamiento de la información.

1.3.12. Evidencia

Es cualquier información que utiliza el auditor para determinar si la información auditada se declara de acuerdo con el criterio establecido. La evidencia incluye información que es sumamente convincente, suficiente, competente y pertinente, que sustentan la opinión de la auditoría.

1.3.12.1. Tipos de evidencia

(Arens, Elder, & Beasley, 2007) mencionan los siguientes tipos de evidencias:

Física:

Se obtiene a través de una inspección o conteo que hace el auditor de un activo tangible. Es decir, la observación directa de actividades, bienes, muestras o sucesos.

Documental:

Examen que hace el auditor de los documentos y registro del cliente para apoyar la información que debe ser incluida en los estados financieros. Los documentos que examina el auditor son registros que utiliza el cliente para proporcionar información al realizar sus actividades de manera organizada.

Testimonial:

Se obtiene de otras personas en forma de declaraciones hechas en el curso de la auditoría o entrevistas, para verificar la autenticidad de los hechos.

Analítica:

Comprende un análisis de cálculos, y comparaciones de la información en sus componentes.

1.3.13. Hallazgos de Auditoría

Es importante resaltar que un hallazgo es cualquier situación irregular encontrada durante el trabajo de auditoría y contiene algunos atributos para describir cómo y en qué circunstancias de control la irregularidad y cuál sería su posible solución y recomendación, con el fin de que otras personas ajenas al auditor puedan entender el hallazgo encontrado.

1.3.13.1. Atributos del hallazgo

(Contraloría General del Estado, 2011) menciona los siguientes atributos:

- **Condición:** se refiere a la situación actual encontrada por el auditor al examinar una actividad, transacción u operación, entendida como “lo que es”.
- **Criterio:** comprende la concepción de “lo que debe ser”, con lo cual el auditor mide la condición del hecho o situación.
- **Efecto:** es el resultado adverso o potencial de la condición encontrada, generalmente representa una pérdida en términos monetarios originados por el cumplimiento para el logro de objetivos, metas y fines institucionales.
- **Causa:** es la razón básica por la que ocurrió la condición, o también el motivo del incumplimiento del criterio de la norma. Su identificación requiere de la habilidad y el buen juicio del auditor y, es fundamental para el desarrollo de una recomendación constructiva que prevenga la recurrencia de la condición.

1.3.14. Papeles de Trabajo

La documentación de la auditoría es el registro del trabajo de auditoría realizado, y la evidencia que sirve de soporte a las debilidades encontradas y las conclusiones a las que ha llegado el auditor. Los papeles de trabajo se deben diseñar y organizar según las circunstancias y las necesidades del auditor, esto han de ser completos, claros y concisos.

1.3.14.1. Objetivos de los Papeles de Trabajo

Entre los principales objetivos de los papeles de trabajo se destacan los siguientes:

- ✓ Proporcionar la información básica y fundamental necesaria para facilitar la ejecución durante todas las etapas del proceso de auditoría.
- ✓ Constituir el fundamento que dispone el auditor para elaborar el informe de auditoría.
- ✓ Servir de fuente para comprobar y explicar en detalle los comentarios, conclusiones y recomendaciones que se exponen en el informe de auditoría.
- ✓ Constituir la evidencia documental del trabajo realizado y de las decisiones tomadas, todo esto de conformidad con disposiciones, normas y reglamentos.

1.3.14.2. Tipos de Papeles de Trabajo

Los papeles de trabajo varían de acuerdo con las circunstancias y criterio del auditor, se presenta a continuación una clasificación que permite su fácil empleo y comprensión:

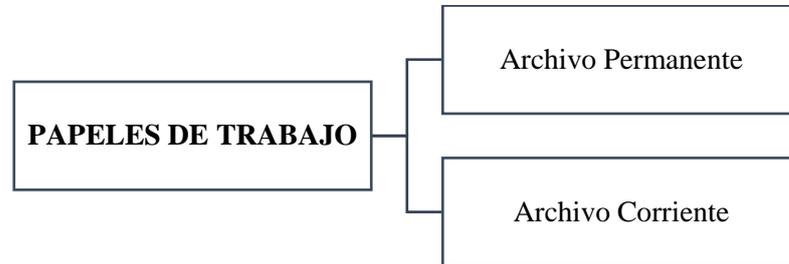


Figura 6-1: Tipos de Papeles de Trabajo

Realizado por: Jaramillo, P. 2023.

✓ **Archivo Permanente**

El archivo permanente contiene todos aquellos papeles que tienen un interés continuo, es la base para la aplicación y programación de la auditoría, permite optimizar el tiempo de los auditores, por ello, el auditor debe contar con un archivo permanente estructurado para facilitar la utilización de la extensa información acumulada.

✓ **Archivo Corriente**

Comprende todos los papeles de trabajo que corresponden a la ejecución de la auditoría, es decir, son aquellos que sustentan las conclusiones y recomendaciones emitidas en el informe de auditoría. Se debe mantener un archivo corriente por cada auditoría realizada y al igual que los anteriores archivos debe mantener sus papeles de trabajo debidamente identificados con índices, referencias y marcas (Hermoso, 2013).

1.3.15. Marcas de Auditoría

Las marcas de auditoría son símbolos que utilizan el auditor para señalar los papeles de trabajo, el tipo de revisión y pruebas efectuadas. Las marcas deben ser únicas y en color diferente al utilizado en la elaboración del papel de trabajo para facilitar su ubicación. El uso de las marcas en auditoría representa los siguientes beneficios:

- ✓ Facilita el trabajo y aprovecha el espacio al anotar en una sola ocasión el trabajo realizado.
- ✓ Facilita su supervisión al poderse comprender en forma inmediata el trabajo llevado a cabo.

1.3.16. Informe de Auditoría

El informe de auditoría debe contener las conclusiones y recomendaciones de los hallazgos más relevantes encontrados durante el desarrollo de la auditoría, especificando si el trabajo se realizó de acuerdo con las normas de auditoría, declarando independencia, integridad y objetividad en su opinión.

1.3.16.1. Objetivos del informe de auditoría:

- ✓ Comunicar los resultados del examen de auditoría a los entes auditados, para que se implementen los cambios que impliquen mayor trascendencia.
- ✓ Apoyar la toma de decisiones, sirviendo como documento de respaldo.
- ✓ Apoyar el análisis de las causas y efectos de los hallazgos de la auditoría.
- ✓ Servir de referencia para futuras auditorías.

En el desarrollo del informe es donde el auditor emite una opinión, la cual puede estar orientada a cuatro sentidos:

- ✓ **Opinión limpia:** significa que durante la auditoría no se encontró ninguna deficiencia relevante cerca de lo observado y se considera que la empresa se está manejando de manera correcta, para la emisión de esta opinión el auditor debe presentar evidencias para demostrarlo.
- ✓ **Opinión negativa:** implica una serie de observaciones relevantes acerca de algunas deficiencias que presentan los procesos que se llevan a cabo en el área auditada, al emitir esta opinión el auditor no observó debilidades materiales o físicas en este caso en las unidades tecnológicas.
- ✓ **Opinión adversa:** el auditor observó deficiencias materiales o físicas.
- ✓ **Sin opinión:** el auditor no tuvo la oportunidad de hacer todas las observaciones necesarias debido a que la información o evidencias no se encontraban disponibles, de manera que el auditor prefiere no emitir una opinión.

1.3.17. Riesgo Informático

Conjunto de procesos que buscan garantizar la confiabilidad de un cierto sistema informático en función de amenazas, vulnerabilidades y debilidades del sistema examinadas respecto a la probabilidad de ocurrencia e impacto de estas sobre los activos de las mismas (Carrillo, 2018, pág. 7).

Amenazas: resultado de la existencia de una vulnerabilidad y riesgos presentes en los procesos informáticos ya sean de índole personal, física, lógica, errores e inclusive desastres naturales que podrían causar daños en los activos (Carrillo, 2018).

Vulnerabilidades: son todas las condiciones que conllevan a que una amenaza se materialice por ejemplo hackers, suplantar identidad, fallos en la programación, software malicioso, errores humanos o factores latentes que podrían provocar incidentes (Carrillo, 2018).

Debilidades: falta de fortaleza de un determinado aspecto, se catalogan de acuerdo con la gravedad que presenta para el sistema informático (Carrillo, 2018).

1.3.18. Seguridad Informática

Método que con base en normas y políticas internas empresariales se encarga de salvaguardar la integridad y privacidad de la información que se encuentra guardada en un sistema informático, para así protegerla contra cualquier tipo de amenaza, reduciendo los riesgos tanto físicos como lógicos (Baca, 2016, pág. 13).

Controles físicos: son las medidas de seguridad aplicadas a los recursos físicos tanto personal como identificaciones (contraseñas, distintivos o restricciones temporales como a los equipos resguardo y vigilancia).

Controles lógicos: son medios de seguridad aplicados a los datos impidiendo su libre acceso a personal no autorizado o barreras que resguarden su uso.

En el caso de que una amenaza a la seguridad informática se haga efectiva, debe enfocarse a recuperar la información dañada o robada. Para lo cual la información debe poseer las siguientes características:

- ✓ **Efectividad:** se trata de conseguir que la información sea en realidad la necesaria para realizar cualquier de los trabajos que se llevan a cabo en la empresa u organización.
- ✓ **Eficiencia:** la información debe ser generada y procesada utilizando de manera óptima los recursos que tiene la empresa para este fin.
- ✓ **Confidencialidad:** todas las fases del procesamiento de la información se deben encontrar protegidas contra accesos no aprobados, los cuales conllevan a la alteración o robo de información confidencial.
- ✓ **Integridad:** que la información que se recibe sea precisa y completa para los fines que se persiguen con su procesamiento.
- ✓ **Disponibilidad:** significa que la información esté a la mano cuando se solicite realizar cualquiera de las etapas del proceso administrativo.

- ✓ **Apego a estándares:** en el proceso de información se deberán respetar normas, reglamentos y acuerdos internos a los cuales está sujeto la empresa.
- ✓ **Confiabledad:** hace referencia a que la información no debe ser alterada inapropiadamente.

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1. Enfoque de investigación

La investigación se sustentará en el enfoque cuantitativo y cualitativo. La primera fase de estudio en la investigación es enfoque cualitativo debido a que se deberá conocer las cualidades, valores, filosofía empresarial, entre otros aspectos trascendentales para la empresa. La segunda fase del estudio es la investigación cuantitativa, puesto que se pretende obtener datos cuantitativos que contribuirán a determinar los niveles de eficiencia en el manejo y control de las unidades tecnológicas a través de la aplicación de indicadores.

2.2. Nivel de investigación

El presente trabajo se desarrollará dentro de un contexto exploratorio – descriptivo – explicativo, debido a que se obtendrá información fundamental previo al inicio del trabajo, mediante investigación bibliográfica para la elaboración del marco teórico. Por otra parte, se ha considerado la investigación descriptiva que permitirá conocer de manera más puntual la realidad de la empresa. Cada uno de los siguientes niveles de investigación serán importantes para ejecutar la Auditoría Informática a la Empresa Servisilva Cía. Ltda., mismos que se detallan a continuación:

2.2.1. *Exploratoria*

Por medio de la aplicación de este nivel de investigación se recolectaron datos, información y elementos importantes que contribuyeron para dar inicio al proyecto investigativo.

2.2.2. *Descriptiva*

Mediante esta investigación se logrará conocer la situación real de la empresa Servisilva Cía. Ltda. mediante la descripción de sus actividades, procesos, operaciones, entre otros factores.

2.2.3. Explicativa

Se aplicará a partir de la identificación de los hallazgos encontrados en auditoría.

2.3. Diseño de investigación

El diseño de esta investigación es no experimental, dado que es un caso que no necesita ejecutarse en un laboratorio o necesite de alguna simulación para demostrar una hipótesis, asimismo no se manipulan variables de ninguna manera de modo que los resultados hallados son reales ni subjetivos.

2.4. Tipo de estudio

Para la realización de este trabajo los tipos de investigación utilizados fueron los siguientes:

2.4.1. Investigación Documental

Al mismo el trabajo se sustentará en la búsqueda de información por medio de documentos, ya sean estos artículos, revistas, libros, ensayos y todo documento procedente de fuentes confiables, puesto que dicha información contribuirá al desarrollo del presente trabajo de integración curricular.

2.4.2. Investigación de campo

Se desplegará dentro de la unidad objeto de estudio (la empresa), en vista de que es la única que proporcionará información trascendental de su situación actual mediante la aplicación de encuestas a las diferentes áreas.

2.5. Población y planificación, selección y cálculo del tamaño de la muestra

2.5.1. Población

La población es “el conjunto de personas u objetos de los que se desea conocer algo en una investigación” (López, 2004). Como población se tomó en consideración al personal que labora en las instalaciones de la Empresa Servisilva Cía. Ltda. del cantón Francisco de Orellana, provincia de Orellana.

Tabla 1-2: Población

Área	No.	%
Gerencia	4	4.82%
Contabilidad	5	6.02%
Bodega	3	3.61%
Ventas	3	3.61%
Recursos Humanos	1	1.20%
Calidad	8	9.64%
Operacional	59	71.08%
Total	83	100%

Fuente: (Servisilva Cía. Ltda. 2020)

Realizado por: Jaramillo, P. 2023.

2.5.2. Muestra

“Es un subconjunto o parte del universo o población en que se llevará a cabo la investigación. Hay procedimientos para conseguir la cantidad de los componentes de la muestra como lo son las fórmulas, lógica, entre otros” (López, 2004). En esta situación considerando que el total de la población es pequeña no se procederá aplicar la fórmula para el muestreo.

2.6. Métodos, técnicas e instrumentos de investigación

2.6.1. Métodos

2.6.1.1. Inductivo

Se empleará este método a fin de examinar aspectos particulares de Servisilva Cía. Ltda. para formular conclusiones generales acerca de la situación actual de manejo de equipos tecnológicos de la empresa de manera que se buscará dar una solución oportuna.

2.6.1.2. Deductivo

Parte de datos generales para obtener conclusiones particulares, recaudando información sobre la empresa de objeto de estudio conociendo las características de identidad para así poder llevar a cabo la Auditoría Informática.

2.6.1.3. Analítico

Este método permite reconocer los procesos y actividades que se realizan en la Unidad objeto de estudio como así también las causas de los problemas planteados para procesar datos y brindar información oportuna.

2.6.2. Técnicas

Las técnicas que se implementarán en el presente trabajo investigativo facilitando la recolección y procesamiento son las siguientes:

2.6.2.1. Observación

Técnica aplicada mediante visitas a las instalaciones de la empresa para obtener datos internos, procesos e información que contribuya al desarrollo de la investigación.

2.6.2.2. Encuesta

Técnica que se pondrá en práctica a los empleados de la Empresa Servisilva Cía. Ltda. mediante la elaboración de un cuestionario que contiene una serie de preguntas claras y concisas, de manera que se obtiene la información necesaria.

2.6.3. Instrumentos

2.6.3.1. Guía de encuestas

Instrumento realizado previo a la aplicación de la encuesta elaborando las preguntas de manera minuciosa a fin de que aporten para poder conocer el criterio de los empleados e identificar datos reales de la institución.

2.6.3.2. Guía de observación

Se la realiza como guía para estudiar la situación de la empresa, misma que se utilizó para el desarrollo del presente trabajo y empleado para plantear la problemática.

CAPÍTULO III

3. MARCO DE RESULTADOS Y DISCUSIÓN DE RESULTADOS

3.1. Resultados

3.1.1. Encuesta

En el presente trabajo de integración curricular se aplicó tres tipos de encuestas, las mismas que fueron dirigidas a todos los trabajadores de la Empresa Servisilva Cía. Ltda., la primera encuesta fue destinada al técnico informático, la segunda al personal administrativo el cual requiere de equipos tecnológicos para el desarrollo de sus actividad diarias, finalmente, la tercera encuesta estuvo dirigida al personal operativo, mismos que no requieren de equipos informáticos para llevar a cabo sus actividades.

1. ¿Los equipos tecnológicos se encuentran protegidos de desastres naturales, robos o cualquier situación que pueda poner en peligro a estos?

Tabla 1-3: Protección de los equipos tecnológicos

Respuestas	Nº de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 1-3: Protección de los equipos tecnológicos

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

De acuerdo con los datos obtenidos de la encuesta, el 1 técnico informático que representa el 100% manifestó que los equipos tecnológicos si se encuentran protegidos de desastres naturales, robos o cualquier situación que pueda poner en peligro a estos. Servisilva Cía. Ltda., ha contratado servicios de la Compañía Aseguradora AMB con una póliza que incluye las coberturas de incendio, terremoto, lluvia inundación, robo, remoción de escombros y daños maliciosos protegiendo así los equipos tecnológicos.

2. ¿Se cuenta con un plan de contingencia para los equipos tecnológicos en caso de posibles desastres?

Tabla 2-3: Plan de Contingencia

Respuestas	N° de Encuestas	Porcentaje
Si	0	0%
No	1	100%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 2-3: Plan de Contingencia

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación.

El 100% que representa el 1 técnico informático, certifica que no existe un plan de contingencia para los equipos en caso de posibles desastres que se puedan suscitar en la empresa, en consecuencia, el área de sistemas no cuenta con estrategias planteadas en caso de que se presenten fallas en los sistemas de información y equipos tecnológicos.

3. ¿Existen cámaras de videovigilancia en áreas donde se localizan equipos tecnológicos?

Tabla 3-3: Sistema de Videovigilancia

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

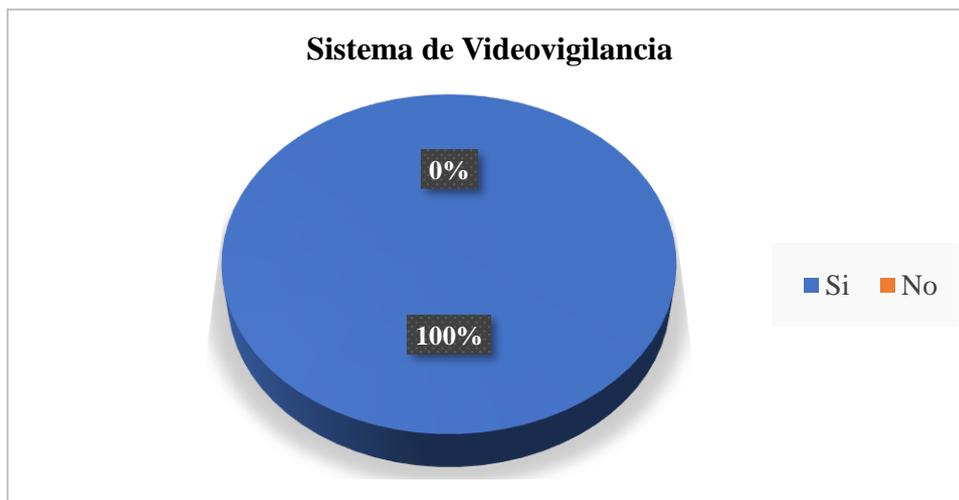


Gráfico 3-3: Sistema de videovigilancia

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 1 técnico informático que representa el 100% de encuestados, señala que existen cámaras de videovigilancia en todas áreas donde se localizan equipos tecnológicos permitiendo llevar un monitoreo continuo en el sector lo mismo que proporciona seguridad, sin embargo, se evidenció que en el área de sistemas donde se localizan los servidores y equipos de repuestos no cuenta con una cámara lo que expone a posibles robos de dichos recursos.

4. ¿Las instalaciones eléctricas para el funcionamiento de los equipos es?

Tabla 4-3: Instalaciones eléctricas

Respuestas	N° de Encuestas	Porcentaje
Excelente	1	100%
Bueno	0	0%
Regular	0	0%
Malo	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

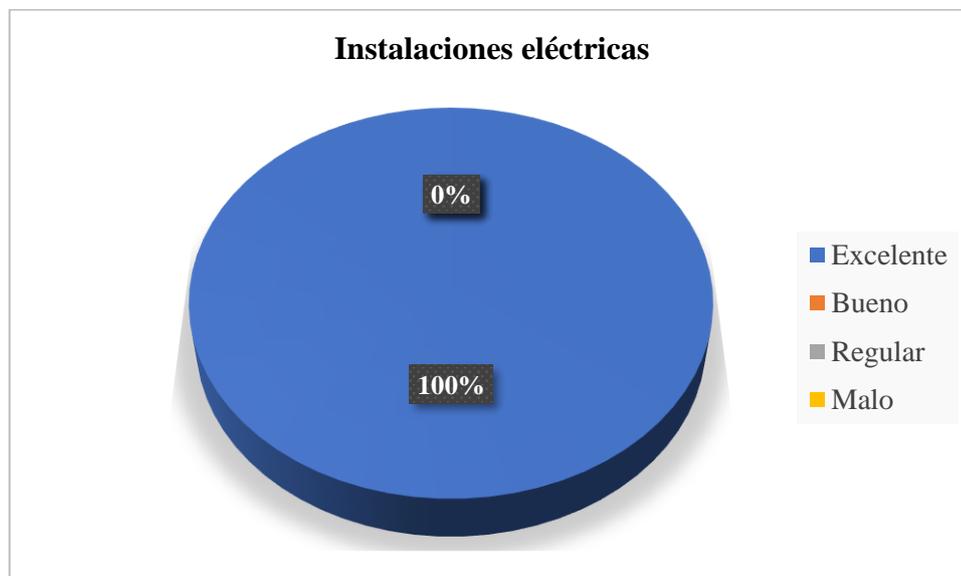


Gráfico 1-3: Instalaciones eléctricas

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 1 técnico informático que representa el 100% de encuestados, afirma que las instalaciones eléctricas se encuentran en el excelente estado. A pesar de ello, se realizó un recorrido por la empresa mediante en el cual se pudo visualizar que en determinadas áreas las instalaciones no se hallan en buen estado mismo que afecta al desarrollo de las actividades empresariales, por tanto, se causan daños en los equipos tecnológicos y fallos en los circuitos eléctricos de la institución.

5. ¿Se efectúan mantenimientos preventivos para verificar el buen estado de los equipos?

Tabla 5-3: Mantenimientos preventivos

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

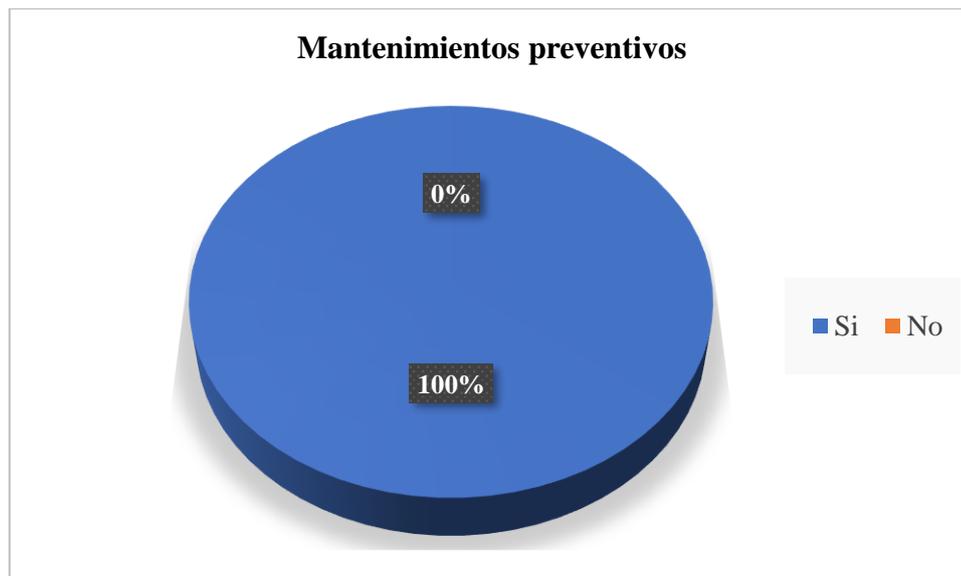


Gráfico 2-3: Mantenimientos preventivos

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 100% que representa el 1 técnico informático de la empresa, asegura que se realizan mantenimientos preventivos a los equipos informáticos de cada una de las áreas de la institución salvaguardando el buen estado de estos. No obstante, en la actualidad el técnico informático no cuenta con registro alguno que certifique que se ha efectuado dichos mantenimientos, pues se dejó de hacerlos sin una clara razón.

6. ¿Cada qué tiempo se realiza mantenimiento preventivo a los equipos tecnológicos?

Tabla 6-3: Frecuencia de mantenimientos preventivos

Respuestas	Nº de Encuestas	Porcentaje
Semanal	0	0%
Mensual	0	0%
Trimestral	1	100%
Semestral	0	0%
Anual	0	0%
Cuando requiera	0	0%
Nunca	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

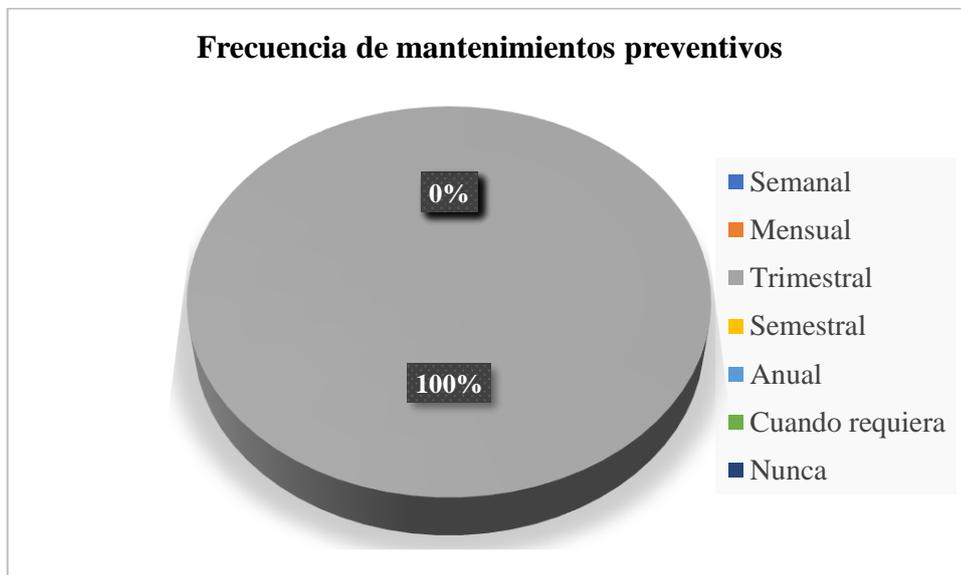


Gráfico 3-3: Frecuencia mantenimientos preventivos

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 1 técnico informático que representa el 100% de encuestados, señala que los mantenimientos preventivos se llevan a cabo de manera trimestral en los equipos tecnológicos, prolongando la vida útil de los equipos y reduciendo las necesidades de implementar mantenimientos correctivos.

7. ¿Cuál es el tiempo promedio para implementar una solución en un mantenimiento correctivo?

Tabla 7-3: Tiempo para implementar mantenimientos correctivos

Respuestas	N° de Encuestas	Porcentaje
Un día o varios días	1	100%
Una semana o varias semanas	0	0%
Un mes o varios meses	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 4-3: Tiempo para implementar mantenimientos correctivos

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

De acuerdo con los datos obtenidos de la encuesta, el 1 técnico informático que representa el 100% de encuestados mencionó que el tiempo promedio para implementar un mantenimiento correctivo a los equipos tecnológicos es de uno a varios días. Por otra parte, el encargado supo manifestar que la duración de los mantenimientos dependerá al tipo de avería que tenga el equipo.

8. ¿Existe un registro de los mantenimientos brindados a los equipos tecnológicos?

Tabla 8-3: Registro de los mantenimientos

Respuestas	N° de Encuestas	Porcentaje
Si	0	0%
No	1	100%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 5-3: Registro de los mantenimientos

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 1 técnico informático que representa el 100% de encuestados, señala que no existe un registro de los mantenimientos que se brindan a los equipos tecnológicos ya sea mediante bitácoras, programas o informes que faciliten la gestión de información en el área de sistemas. Sin embargo, indica que antes si se llevaba un registro de los mantenimientos, pero se los dejó de hacer sin algún motivo en específico.

9. ¿Se cuenta con un programa de protección de la información contra softwares maliciosos?

Tabla 9-3: Programas en contra de softwares maliciosos

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 9-3: Programas en contra de softwares maliciosos

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 1 técnico informático que representa el 100% de encuestados, declara que los equipos tecnológicos sí cuentan con un programa de protección de información en contra de softwares maliciosos, lo que permite garantizar la privacidad de los usuarios en el uso de sistemas informáticos creando una barrera de protección contra virus. El software contratado es Avast Premium – Empresarial, su licencia tiene la duración de 1 año y una vez finalizado se renueva dicha licencia.

10. ¿Para el uso del sistema informático de la institución, se cuenta con una contraseña personal de acuerdo con el perfil del trabajador?

Tabla 10-3: Contraseñas en el sistema informático

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 6-3: Contraseñas en el sistema informático

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 100% de los encuestados que representa el 1 técnico informático de la empresa, señala que si se cuenta con una contraseña personal para cada empleado de la empresa en el uso del sistema informático y plataforma web.

Para acceder a la red Socserver cual contiene información de la empresa, se proporciona a cada trabajador del área administrativa un usuario y una contraseña personal misma que es actualizada de manera trimestral. El técnico informático es la única persona que tiene acceso a mencionadas claves, en el momento que se realiza la actualización de las claves, el técnico se dirige a cada uno de los equipos de cómputo ingresando la nueva contraseña correspondiente este proceso se lleva a cabo cada tres meses, con la finalidad de la información se encuentre segura.

11. ¿Se realizan copias de información importante, en un lugar distinto al equipo de cómputo de trabajo?

Tabla 11-3: Respaldos de información

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 7-3: Respaldos de información

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 100% de los encuestados que representa el 1 técnico informático de la empresa expresa que, si se realizan respaldos de información en un lugar diferente al equipo de cómputo de trabajo, lo que permite tener una copia de seguridad de la información consiguiendo restaurarla en caso de posibles fallas en el sistema informático. Concretamente se efectúan dos tipos de respaldos, el primero que son respaldos diarios realizados en el mismo servidor de la empresa y, por otra parte, respaldos trimestrales que se ejecutan en discos especializados fuera del servidor, disquetes y en la nube.

12. ¿Con qué frecuencia se realizan cambios en las claves del sistema informático o equipo de cada empleado? (marque solo una)

Tabla 12-3: Frecuencia en el cambio de claves

Respuestas	N° de Encuestas	Porcentaje
Semanal	0	0%
Mensual	0	0%
Trimestral	1	100%
Semestral	0	0%
Anual	0	0%
Nunca	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

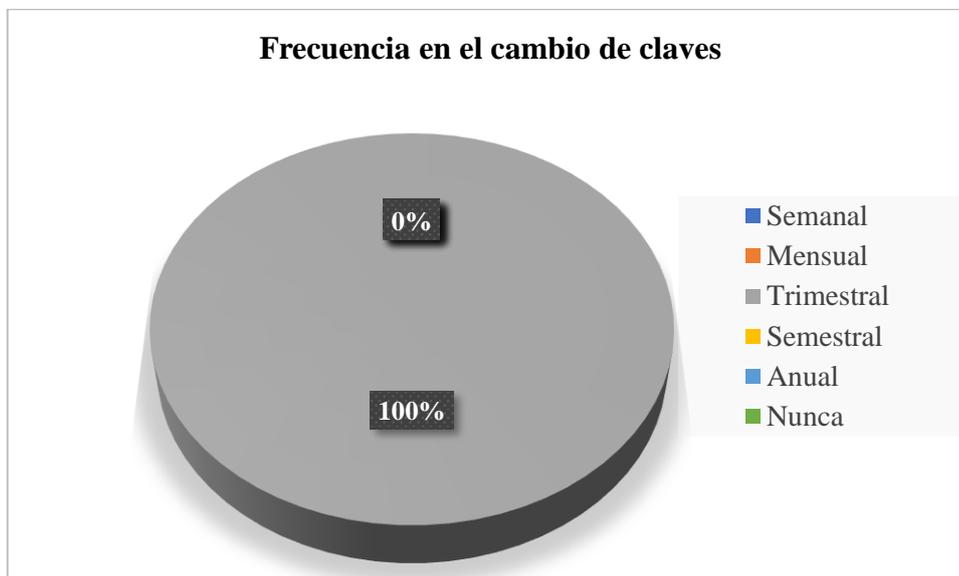


Gráfico 8-3: Frecuencia en el cambio de claves

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 100% de los encuestados que representa el 1 técnico informático de la empresa, manifiesta que se realizan cambios de claves en el sistema informático y equipos cómputo de manera trimestral, siendo este una medida de seguridad evitando fugas de información que reposan en programas específicos de la empresa.

13. ¿Se cuenta con un inventario actualizado de todos los equipos tecnológicos?

Tabla 13-3: Inventario de los equipos

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

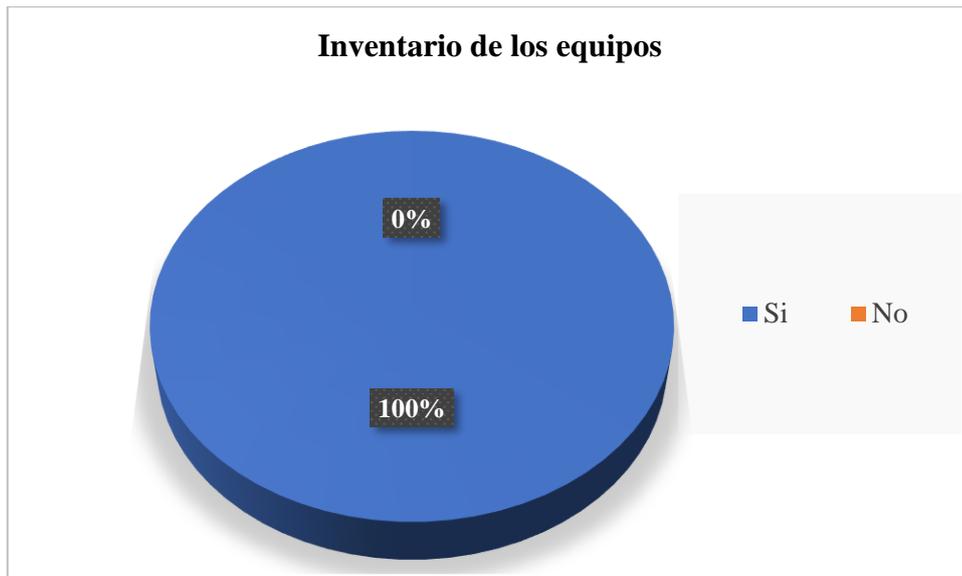


Gráfico 9-3: Frecuencia en el cambio de claves

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

El 1 técnico informático que representa el 100% de encuestados, afirma que sí se lleva un inventario actualizado de todos los equipos tecnológicos que posee la empresa, siendo una parte relevante ya que a través de este se inventario se maneja un control de entradas y salidas de los equipos tecnológicos. La plataforma donde se maneja el inventario se denomina TicketSoft.

14. ¿Se cuenta con equipos tecnológicos adicionales que reemplacen los dañados?

Tabla 14-3: Equipos tecnológicos adicionales

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

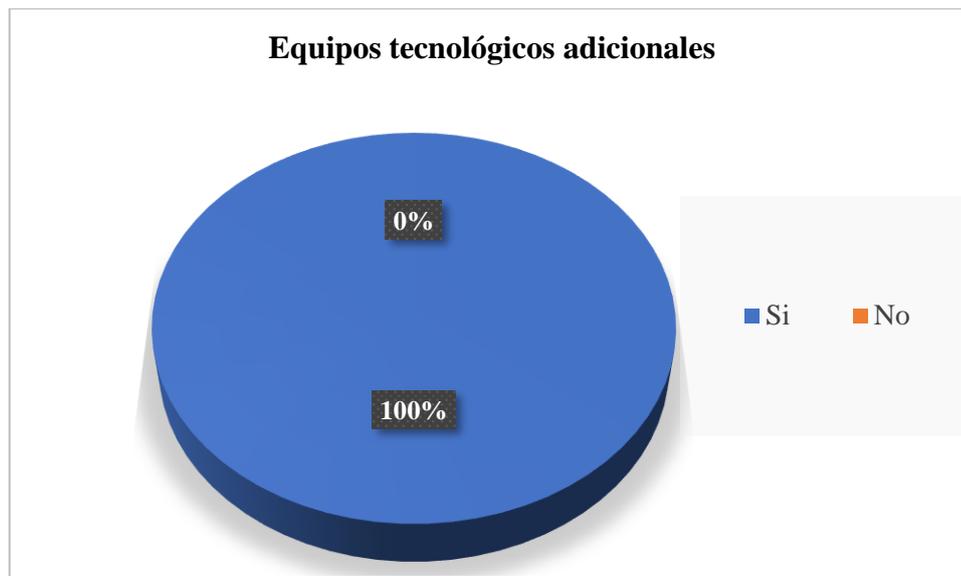


Gráfico 10-3: Equipos tecnológicos adicionales

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

El 1 técnico informático que representa el 100% de los encuestados, asegura que la empresa si tiene equipos tecnológicos adicionales que reemplacen a los equipos dañados, facilitando el trabajo a desarrollar por parte del técnico, puesto que dispone de las herramientas y piezas necesarias, también mejora la gestión de los procesos de mantenimiento.

15. ¿Existen políticas de seguridad y manejo de los equipos tecnológicos?

Tabla 15-3: Políticas de seguridad y manejo

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

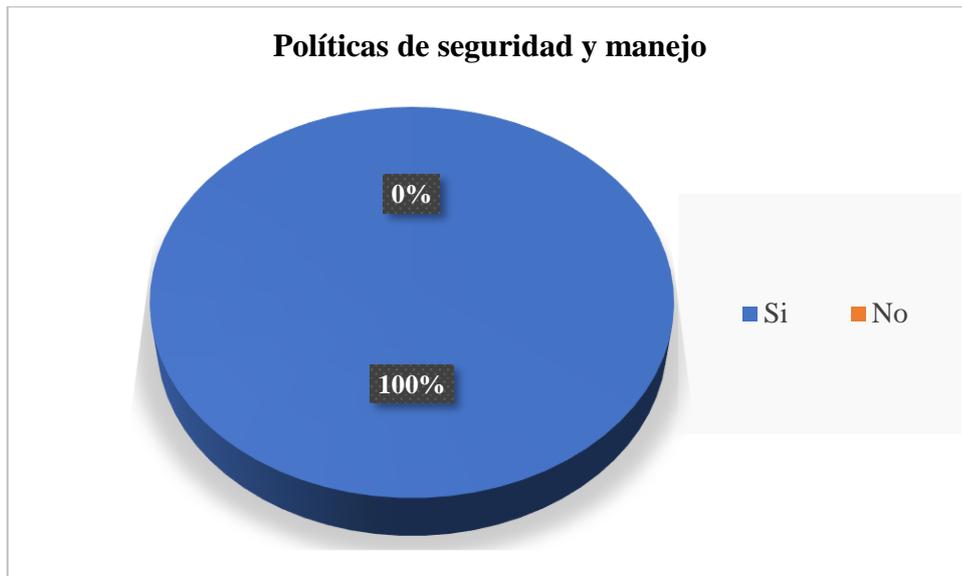


Gráfico 11-3: Políticas de seguridad y manejo

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 1 técnico informático que representa el 100% de encuestados, señala que, si existen políticas de seguridad y manejo de los equipos tecnológicos, dichas políticas brindan a la empresa pautas de seguridad necesarias hacia los usuarios-empleados que acceden a los equipos y la información que se encuentra dentro de la misma.

16. ¿El personal conoce de las políticas de seguridad y del buen manejo de los equipos?

Tabla 16-3: Conocimiento de las políticas de seguridad

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

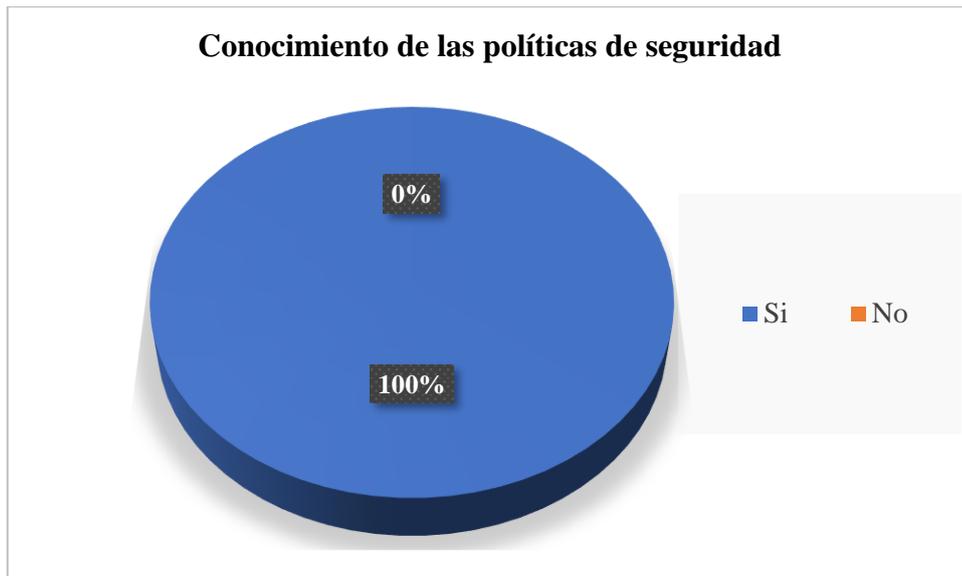


Gráfico 12-3: Conocimiento de las políticas de seguridad

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

El 1 técnico informático que representa el 100% de encuestados, determinó que el personal de la empresa Servisilva si tiene conocimiento de las políticas de seguridad que existen y del buen manejo de los equipos tecnológicos, reduciendo la posibilidad de que ocurran accidentes o riesgos en los equipos ya que tienen una instrucción de lo que se plantea en las políticas de seguridad.

17. ¿Cómo califica la calidad de servicio de internet que dispone la empresa?

Tabla 17-3: Calidad del internet

Respuestas	N° de Encuestas	Porcentaje
Excelente	1	100%
Bueno	0	0%
Regular	0	0%
Malo	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

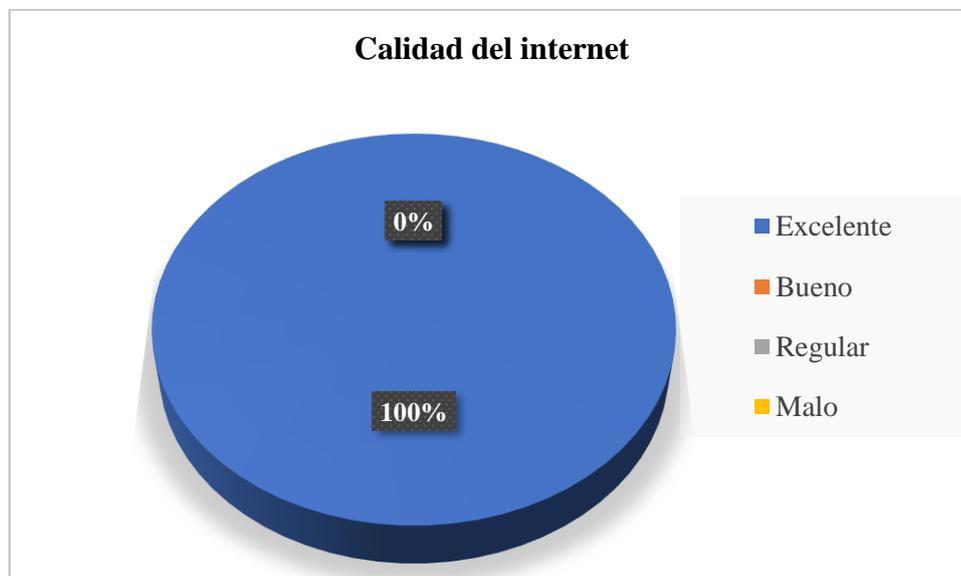


Gráfico 13-3: Calidad del internet

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

El 1 técnico informático que representa el 100% de encuestados, manifiesta que la empresa cuenta con una excelente calidad en el servicio de internet lo cual permite conectarse a los empleados entre sí, ya sea mediante equipos de cómputos o celulares. El proveedor de internet para Servisilva Cía. Ltda. es Puntonet con un plan corporativo ofreciendo 20 Mb.

18. ¿Los interruptores de energía y cables de red están debidamente etiquetados y protegidos?

Tabla 18-3: Interruptores de energía y cables de red

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

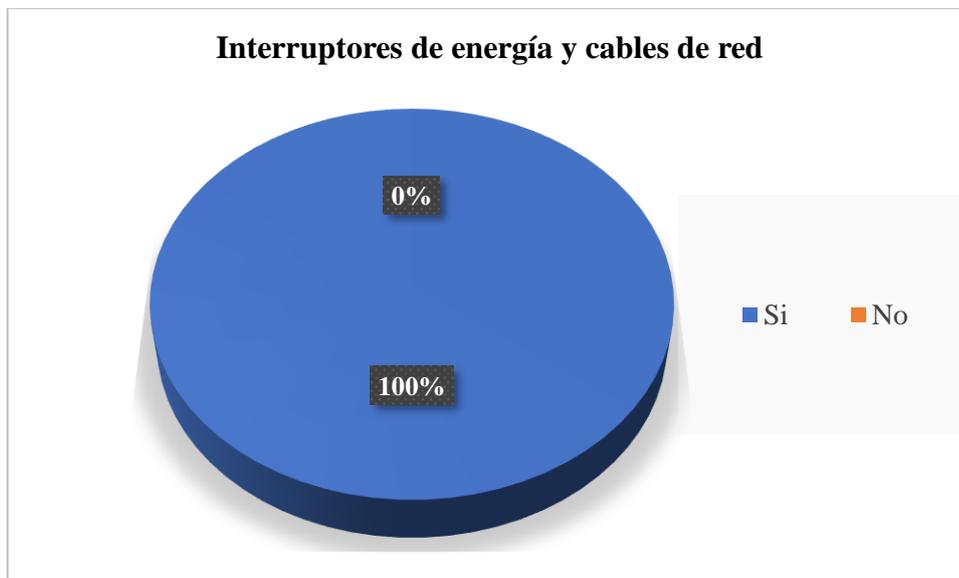


Gráfico 14-3: Interruptores de energía y cables de red

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

El 1 técnico informático que representa el 100% de encuestados, menciona que los interruptores de energía y cables de red si se encuentran debidamente etiquetados y protegidos considerándose como seguras, para que las actividades se desarrollen de la mejor manera sin la ocurrencia de posibles accidentes.

19. ¿La empresa cuenta con una página web o aplicación móvil?

Tabla 19-3: Página web

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

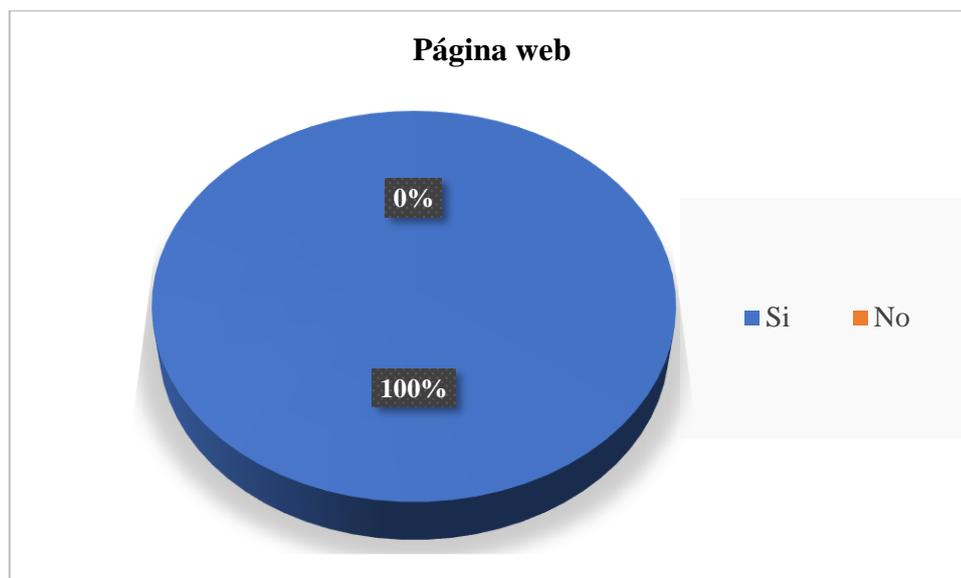


Gráfico 15-2: Página web

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

El 1 técnico informático que representa el 100% de encuestados, manifiesta que la Empresa Servisilva Cía. Ltda. sí cuenta con una página web, como así también dispone de una aplicación móvil para uso exclusivo de los empleados donde se comparte roles de pago, reglamentos, políticas y toda información relacionada a la empresa.

20. ¿Considera usted qué es necesario realizar una auditoría informática en la empresa, para contribuir al máximo aprovechamiento de los equipos tecnológicos?

Tabla 20-3: Necesario realizar auditoría informática

Respuestas	N° de Encuestas	Porcentaje
Si	1	100%
No	0	0%
Total	1	100%

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 16-3: Necesario realizar auditoría informática

Fuente: Encuesta aplicada al técnico informático de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

El 1 técnico informático que representa el 100% de encuestados, considera que si es necesario realizar una Auditoría Informática en la Empresa Servisilva Cía. Ltda., para así contribuir a la correcta utilización y máximo aprovechamiento de los equipos tecnológicos.

Por otra parte, se dan a conocer los resultados de la encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

1. ¿En el momento de realizar sus actividades diarias los equipos tecnológicos responden de manera oportuna a sus ocupaciones laborales?

Tabla 21-3: Desempeño de equipos tecnológicos

Respuestas	N° de Encuestas	Porcentaje
Siempre	9	39%
Casi Siempre	11	48%
A veces	3	13%
Nunca	0	0%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

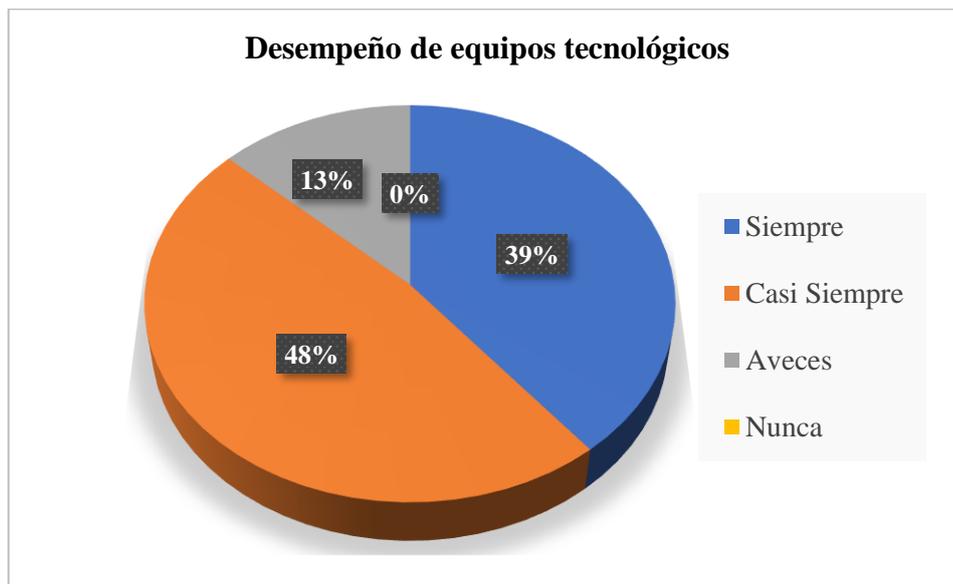


Gráfico 17-3: Desempeño de equipos tecnológicos

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 9 personas (39%) consideran que los equipos tecnológicos responden de manera oportuna en sus ocupaciones laborales Siempre, 11 personas (48%) mencionan que Casi Siempre, 3 personas (13%) responden que A veces, y no se obtuvieron respuestas en la alternativa de Nunca.

2. ¿Conoce usted de políticas que salvaguarden los equipos tecnológicos de la Empresa Servisilva Cía. Ltda.?

Tabla 22-3: Conocimiento de las políticas de seguridad

Respuestas	N° de Encuestas	Porcentaje
Si	10	43%
No	13	57%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

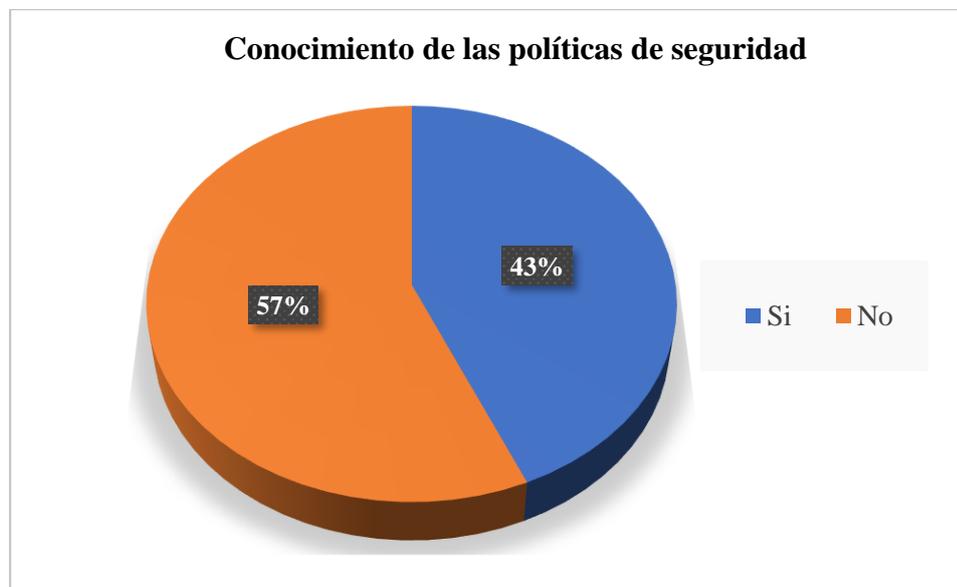


Gráfico 18-3: Conocimiento de las políticas de seguridad

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 10 personas (43%) afirman que Sí conocen de las políticas de seguridad que existen para los equipos tecnológicos, y 13 personas (57%) mencionan que No tienen conocimiento de estas políticas de seguridad hacia los equipos. La mayoría del personal de la empresa desconoce de políticas que salvaguarden los equipos tecnológicos.

3. ¿Cómo califica el estado actual de los equipos tecnológicos?

Tabla 23-3: Estado de los equipos tecnológicos

Respuestas	N° de Encuestas	Porcentaje
Excelente	4	17%
Bueno	14	61%
Regular	3	13%
Malo	2	9%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

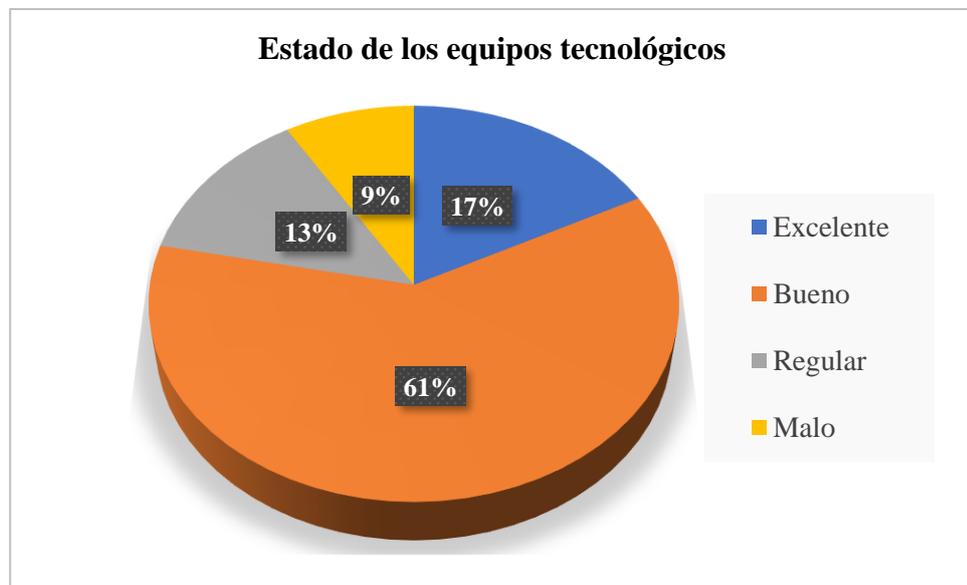


Gráfico 19-3: Estado de los equipos tecnológicos

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 4 personas (17%) coinciden de que los equipos tecnológicos se encuentran en un estado Excelente, 14 personas (61%) dicen que su estado es Bueno, 3 personas (13%) mencionan que es Regular y 2 personas (2%) evaluaron el estado de los equipos como malo. El personal calificó como Bueno el estado actual de los equipos previniendo posibles fallos o incidencias que puedan presentarse en estos.

4. ¿Las instalaciones eléctricas de los equipos tecnológicos se encuentran debidamente protegidas, sin ser un obstáculo en el desarrollo de sus actividades?

Tabla 24-3: Instalaciones eléctricas

Respuestas	N° de Encuestas	Porcentaje
Si	18	78%
No	5	22%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

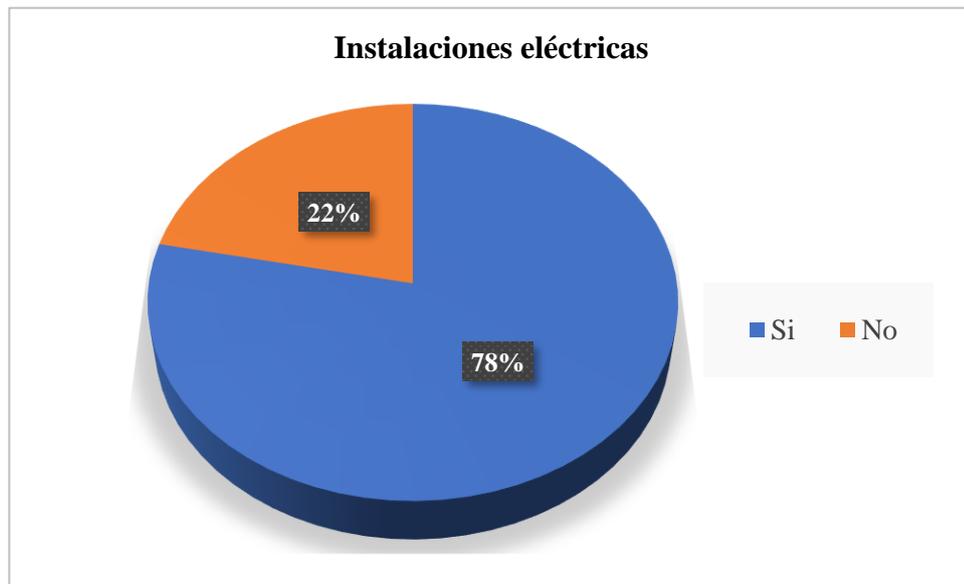


Gráfico 20-3: Instalaciones eléctricas

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 18 personas (78%) manifiestan que las instalaciones eléctricas Sí se encuentran debidamente protegidas, por otra parte, 5 personas (22%) dicen que las instalaciones eléctricas no se encuentran debidamente protegidas, por lo que llega a ser un obstáculo en la ejecución de sus actividades.

5. ¿El sistema informático que utiliza para el desarrollo de sus actividades y manejo de la información es?

Tabla 25-3: Sistema informático

Respuestas	N° de Encuestas	Porcentaje
Excelente	6	26%
Bueno	13	57%
Regular	4	17%
Malo	0	0%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

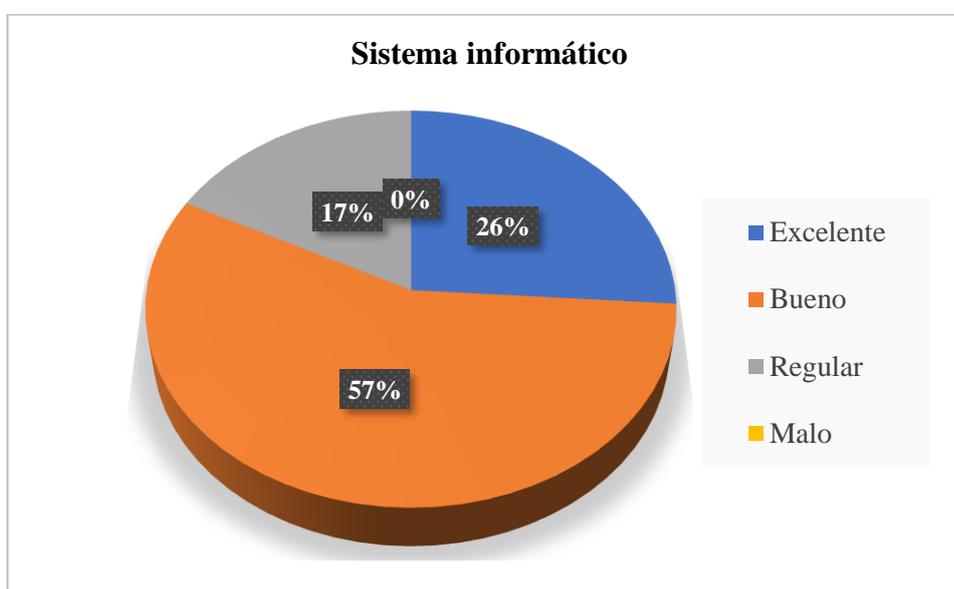


Gráfico 21-3: Sistema informático

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 6 personas (26%) mencionan que el sistema informático que se utiliza para el desarrollo de actividades es Excelente, 13 personas (57%) manifiestan que el sistema informático es Bueno, 4 personas (17%) mencionan que es Regular y no se cuenta con respuestas en la alternativa de Malo. Las respuestas por parte de la mayoría de los trabajadores expresan que el sistema informático es bueno, puesto que, ayuda de cierta manera en la gestión de tareas.

6. ¿Existen programas de protección en contra de softwares maliciosos para los sistemas informáticos?

Tabla 26-3: Programas de protección

Respuestas	N° de Encuestas	Porcentaje
Si	20	87%
No	3	13%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 22-3: Programas de protección

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 20 personas (87%) señalan que Sí se cuentan con programas de protección en contra de softwares maliciosos para los sistemas informáticos, y 3 personas (13%) manifiestan que no se cuentan con programas de protección. No obstante, mediante encuesta aplicada al técnico informático de la empresa comunicó que si tienen programas de protección, sin embargo, una cantidad mínima de trabajadores no tiene conocimiento de estos.

7. ¿Se realiza respaldos de información en un lugar diferente al equipo de cómputo de trabajo?

Tabla 27-3: Respaldos de información

Respuestas	N° de Encuestas	Porcentaje
Si	20	87%
No	3	13%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 23-3: Respaldos de información

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 20 personas (87%) señalan que Sí se cuentan con programas de protección en contra de softwares maliciosos para los sistemas informáticos, y 3 personas (13%) manifiestan que no se cuentan con programas de protección. No obstante, mediante encuesta aplicada al técnico informático de la empresa comunicó que si cuentan con respaldos de información en lugares externos.

8. ¿Se efectúan mantenimientos preventivos para verificar el buen estado de los equipos?

Tabla 28-3: Mantenimientos preventivos

Respuestas	N° de Encuestas	Porcentaje
Si	19	83%
No	4	17%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

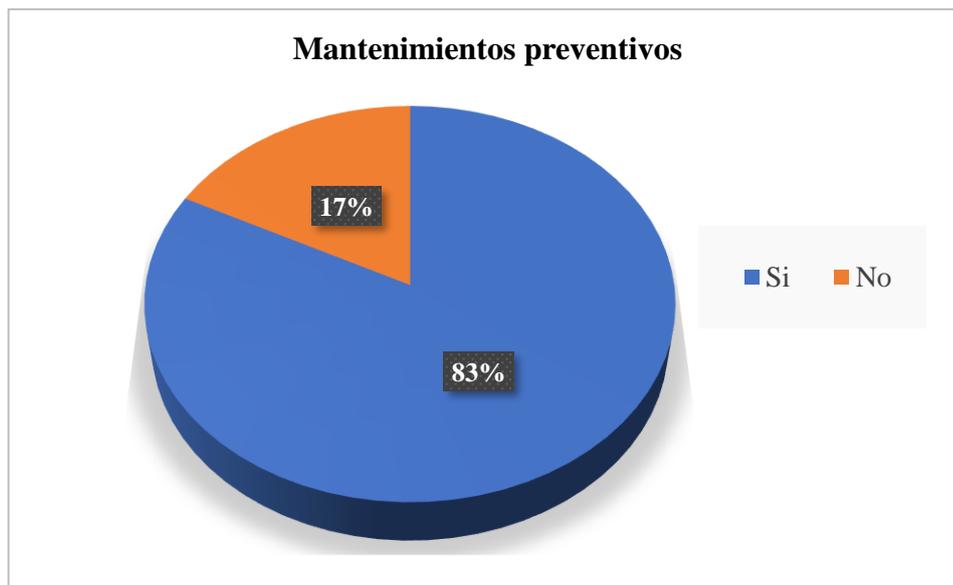


Gráfico 24-3: Mantenimientos preventivos

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 19 personas (83%) señalan que Sí se realizan mantenimientos preventivos a los equipos tecnológicos, y 4 personas (17%) manifiestan que No se realizan mantenimientos.

9. ¿Con qué frecuencia se realizan mantenimientos preventivos a los equipos tecnológicos?

Tabla 29-3: Frecuencia de mantenimientos preventivos

Respuestas	N° de Encuestas	Porcentaje
Semanal	1	4%
Mensual	2	9%
Trimestral	12	52%
Semestral	0	0%
Anual	1	4%
Cuando requiera	7	31%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

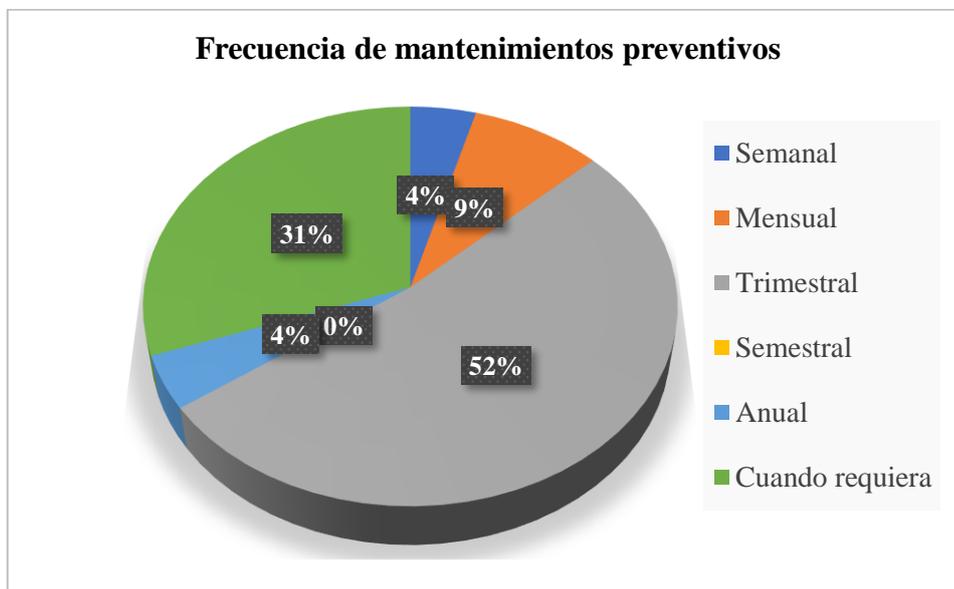


Gráfico 25-3: Frecuencia de mantenimientos preventivos

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 1 persona (4%) menciona que los mantenimientos preventivos a los equipos tecnológicos se los realiza de manera Semanal, 2 personas (9%) afirman que es mensual, 12 personas (52%) manifiestan que es Trimestral, 1 personas (4%) menciona que es Anual, 7 personas (31%) dicen que los mantenimientos se los lleva a cabo Cuando se requiera, no se cuenta con respuestas en la alternativa de Semestral.

10. ¿Se efectúan mantenimientos correctivos a los equipos tecnológicos?

Tabla 30-3: Mantenimientos correctivos

Respuestas	N° de Encuestas	Porcentaje
Si	23	100%
No	0	0%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

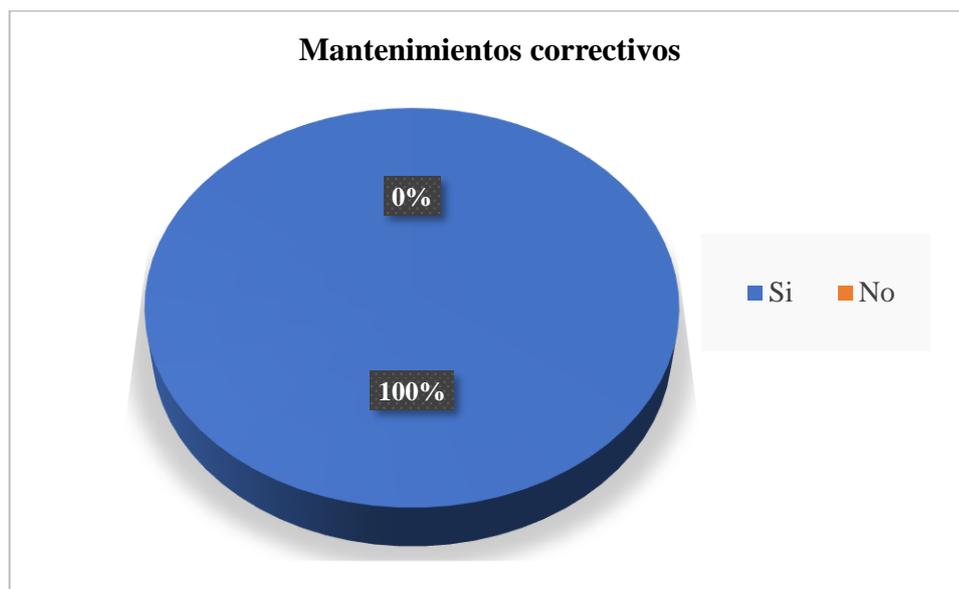


Gráfico 26-3: Mantenimientos correctivos

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

El 100% de los 23 empleados encuestados expresan que Sí se efectúan mantenimientos correctivos a los equipos tecnológicos, un mantenimiento adecuado permite alargar la vida útil obteniendo un mayor rendimiento durante el uso de estos equipos.

11. ¿Cuál es el tiempo promedio para implementar una solución en un mantenimiento correctivo?

Tabla 31-3: Tiempo para implementar mantenimiento correctivo

Respuestas	N° de Encuestas	Porcentaje
Un día o varios días	19	83%
Una semana o varias semanas	4	17%
Un mes o varios meses	0	0%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

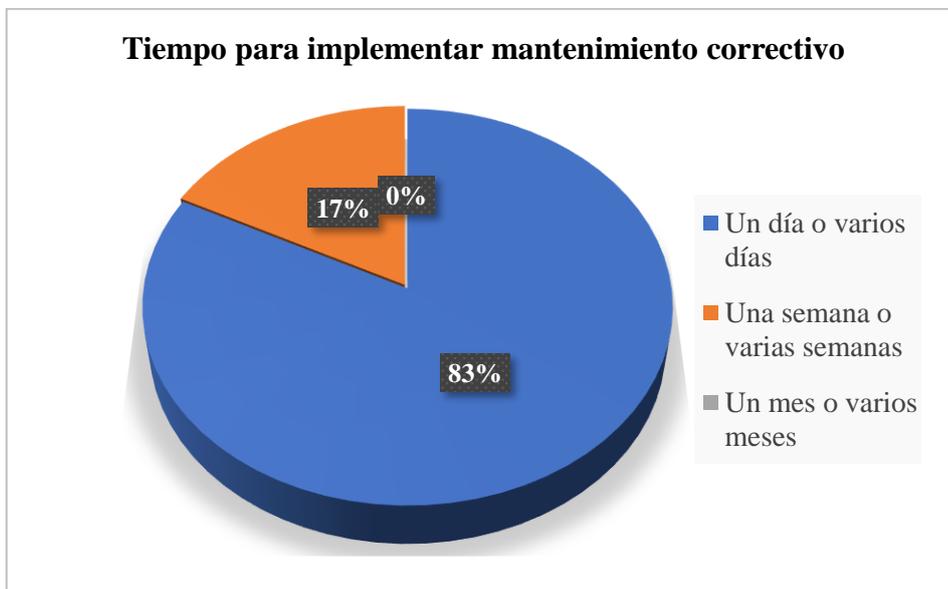


Gráfico 27-3: Tiempo para implementar mantenimiento correctivo

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 19 personas (83%) manifiestan que el tiempo promedio para implementar una solución en un mantenimiento correctivo es de uno o varios días, 4 personas (17%) dicen que el tiempo es de Una a varias semanas y no se obtuvieron resultados en la alternativa de Un mes o varios meses. La mayoría de los trabajadores respondió que los mantenimientos tienen una duración de uno o varios días por lo cual se encuentra en un nivel óptimo.

12. ¿A su criterio, el mantenimiento brindado a los equipos es?

Tabla 32-3: Calificación de mantenimientos brindados

Respuestas	N° de Encuestas	Porcentaje
Excelente	9	39%
Bueno	7	30%
Regular	7	31%
Malo	0	0%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

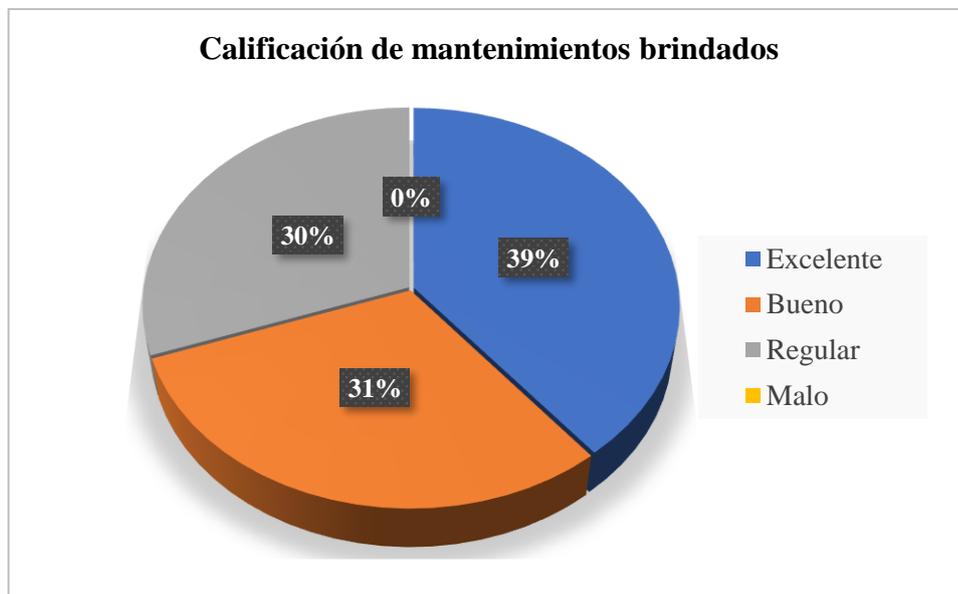


Gráfico 28-3: Calificación de mantenimientos brindados

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 9 personas (39%) manifiestan que el mantenimiento brindado a los equipos tecnológicos es Excelente, 7 personas (30%) dicen que el mantenimiento es Regular, 9 personas (39%) mencionan que es Regular y no se obtuvieron registros en la alternativa de Malo.

Se deduce que en su mayoría los mantenimientos son excelentes debido a que el técnico informático de la empresa ofrece un servicio de calidad proporcionando una respuesta inmediata contribuyendo de manera significativa en las actividades empresariales.

13. ¿Cuenta con una contraseña personal para el uso de plataformas y sistema informático de la empresa?

Tabla 33-3: Contraseñas

Respuestas	N° de Encuestas	Porcentaje
Si	21	91%
No	2	9%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 29-3: Contraseñas

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 21 personas (91%) dicen que Sí cuentan con una contraseña personal para el acceso del sistema informático y uso de plataformas y 2 personas (9%) manifiestan que No cuentan con una contraseña personal.

14. ¿La empresa cuenta con una página web o aplicación móvil?

Tabla 34-3: Página web o aplicación móvil

Respuestas	N° de Encuestas	Porcentaje
Si	22	96%
No	1	4%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

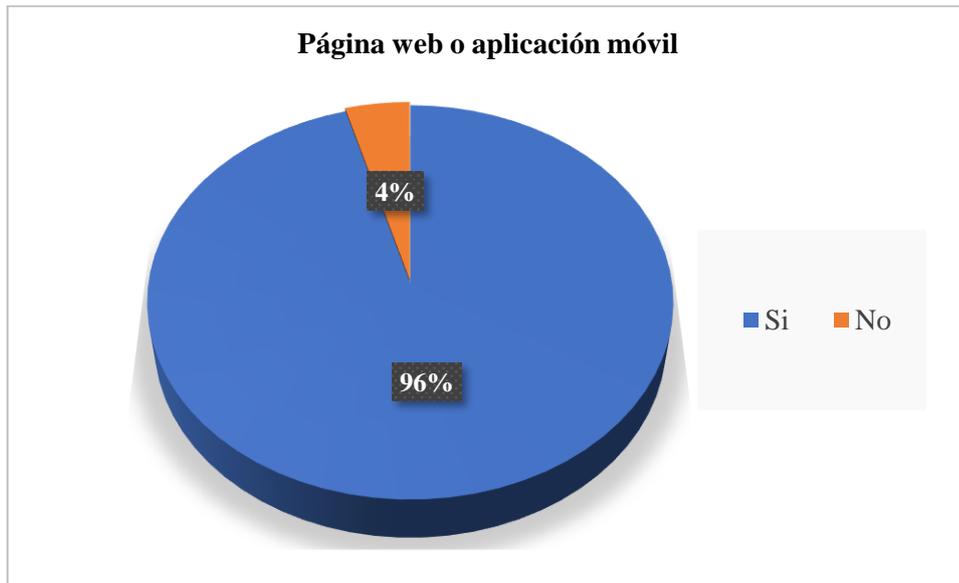


Gráfico 30-3: Página web o aplicación móvil

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 22 personas (96%) respondieron que la empresa Sí cuenta con una página web y aplicación móvil, por otra parte, 1 persona (4%) asegura que la empresa no cuenta con una página web y con una aplicación móvil.

15. ¿Cómo califica el servicio de internet que brinda la empresa?

Tabla 35-3: Servicio de internet

Respuestas	N° de Encuestas	Porcentaje
Excelente	6	26%
Bueno	12	52%
Regular	5	22%
Malo	0	0%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

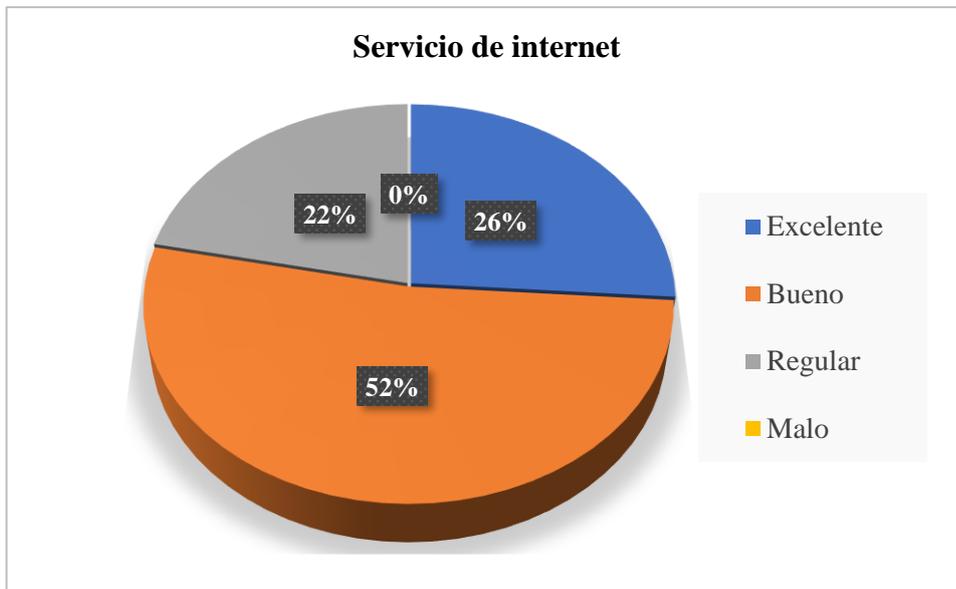


Gráfico 31-3: Servicio de internet

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 6 personas (26%) afirman que el servicio de internet que proporciona la empresa es Excelente, 12 personas (52%) evaluaron al servicio de internet como Bueno, 5 personas (22%) mencionan que es Regular, no se obtuvieron respuestas en la alternativa de Malo. Esto surge debido a que en ciertas áreas, la conectividad del internet es tardía interviniendo en la comunicación y desarrollo de actividades de los trabajadores.

16. ¿Considera usted qué es necesario realizar una auditoría informática en la empresa, para contribuir al máximo aprovechamiento de los equipos tecnológicos?

Tabla 36-3: Necesario realizar una auditoría informática

Respuestas	N° de Encuestas	Porcentaje
Si	19	83%
No	4	17%
Total	23	100%

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 32-3: Necesario realizar una auditoría informática

Fuente: Encuesta aplicada al personal administrativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 19 personas (83%) expresan que Sí es necesario realizar una Auditoría Informática en la empresa a fin de contribuir al máximo aprovechamiento de los equipos tecnológicos, y 4 personas (17%) manifiestan que no es necesario ejecutar una Auditoría Informática.

Por otra parte, se dan a conocer los resultados de la encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

1. ¿Conoce usted de políticas que salvaguarden los recursos tecnológicos de la Empresa Servisilva Cía. Ltda.?

Tabla 37-3: Conocimiento de las políticas de seguridad

Respuestas	N° de Encuestas	Porcentaje
Sí	29	49%
No	30	51%
Total	59	100%

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

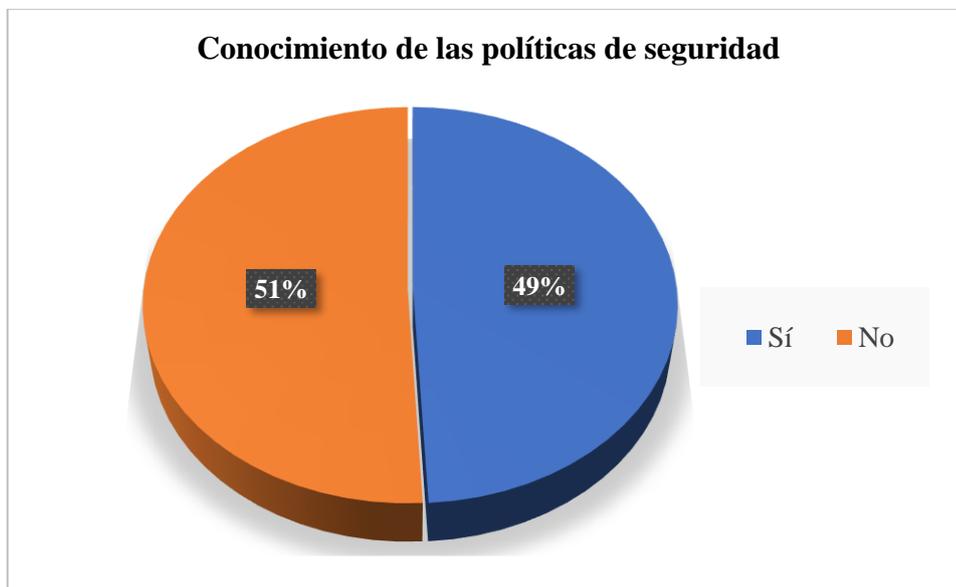


Gráfico 33-3: Conocimiento de las políticas de seguridad

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 59 empleados encuestados se obtiene que: 29 personas (49%) expresan que Sí tienen conocimiento de las políticas de seguridad que existen para los equipos tecnológicos, y 30 personas (51%) manifiestan que No conocen de dichas políticas. Por tanto, el técnico informático deberá brindar una capacitación en donde se den a conocer las políticas de seguridad de la empresa.

2. ¿La empresa posee una página web o aplicación móvil?

Tabla 38-3: Página web o aplicación móvil

Respuestas	N° de Encuestas	Porcentaje
Sí	39	66%
No	20	34%
Total	59	100%

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

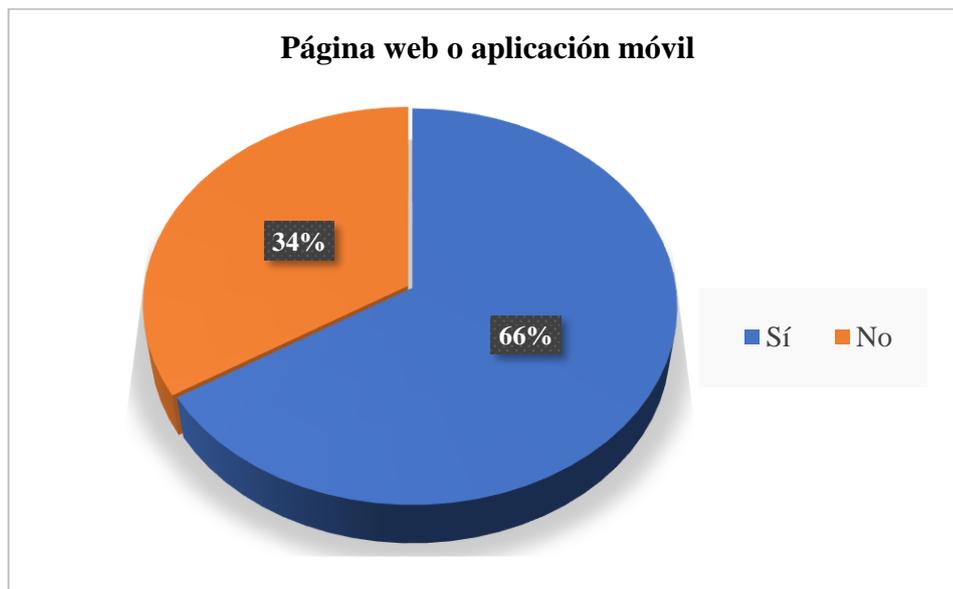


Gráfico 34-3: Página web o aplicación móvil

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación:

Según los resultados obtenidos de un total de 59 empleados encuestados se obtiene que: 39 personas (66%) respondieron que la empresa Sí cuenta con una página web y aplicación móvil, y 20 personas (34%) asegura que la empresa no cuenta con una página web y con una aplicación móvil.

3. ¿Las instalaciones eléctricas de los recursos tecnológicos se encuentran debidamente protegidas, sin ser un obstáculo en el desarrollo de sus actividades?

Tabla 39-3: Instalaciones eléctricas

Respuestas	N° de Encuestas	Porcentaje
Sí	44	75%
No	15	25%
Total	59	100%

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

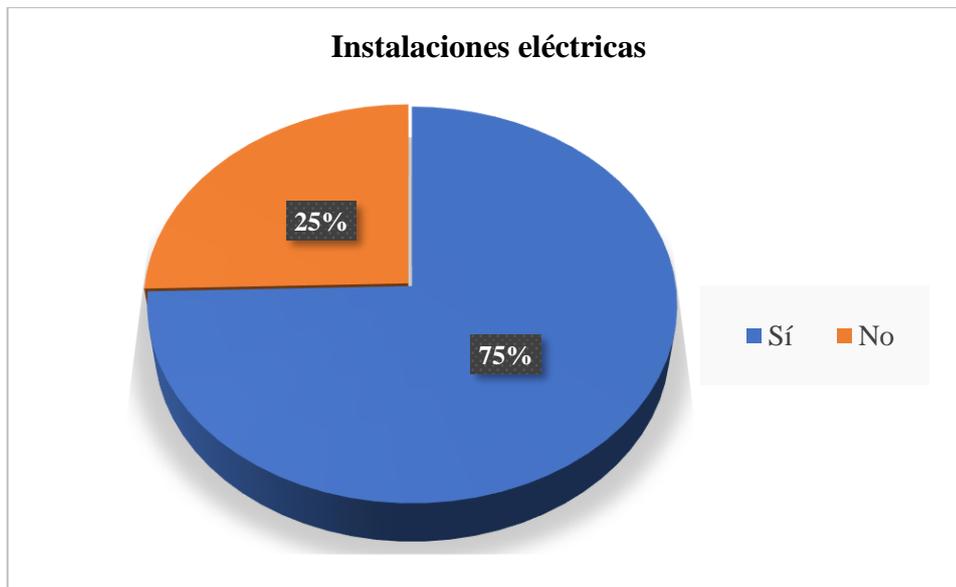


Gráfico 35-3: Instalaciones eléctricas

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 59 empleados encuestados se obtiene que: 44 personas (75%) manifiestan que las instalaciones eléctricas Sí se encuentran debidamente protegidas, por otra parte, 15 personas (25%) dicen que las instalaciones eléctricas no se encuentran debidamente protegidas, por lo que llega a ser un obstáculo en la ejecución de sus actividades.

4. ¿Cómo califica el servicio de internet que brinda la empresa?

Tabla 40-3: Servicio de internet

Respuestas	N° de Encuestas	Porcentaje
Excelente	9	15%
Bueno	27	46%
Regular	17	29%
Malo	6	10%
Total	59	100%

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

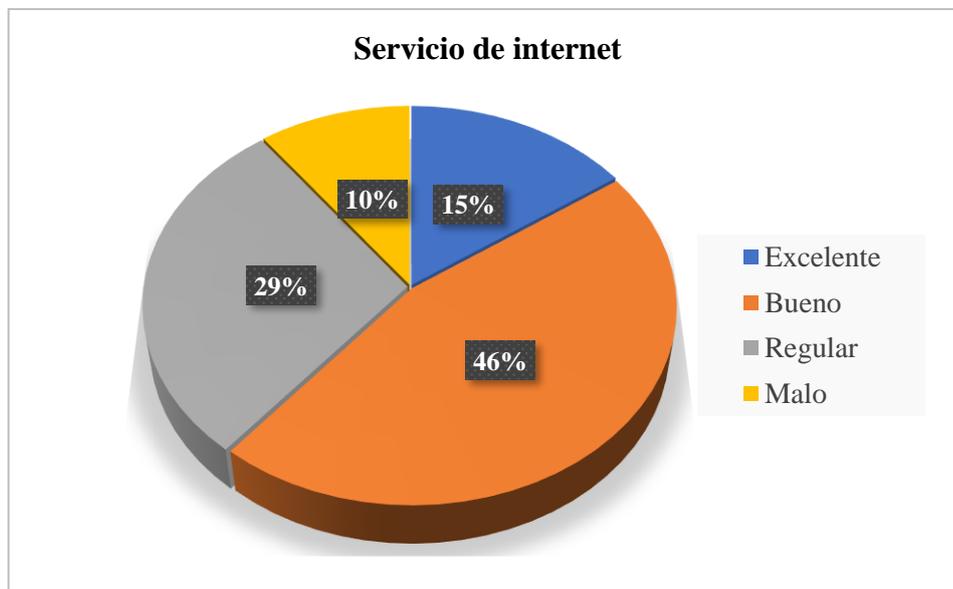


Gráfico 36-3: Servicio de internet

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 23 empleados encuestados se obtiene que: 6 personas (26%) afirman que el servicio de internet que proporciona la empresa es Excelente, 12 personas (52%) evaluaron al servicio de internet como Bueno, 5 personas (22%) mencionan que es Regular, no se obtuvieron respuestas en la alternativa de Malo. Se obtienen estos resultados puesto que el personal operativo desarrolla sus actividades en áreas alejadas causando una baja calidad en el internet e inconvenientes en la comunicación interna.

5. ¿Considera usted qué es necesario realizar una auditoría informática en la empresa, para contribuir al máximo aprovechamiento de los equipos tecnológicos?

Tabla 41-3: Ejecución de auditoría informática

Respuestas	N° de Encuestas	Porcentaje
Sí	58	98%
No	1	2%
Total	59	100%

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.



Gráfico 37-3: Ejecución de auditoría informática

Fuente: Encuesta aplicada al personal operativo de la Empresa Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Análisis e Interpretación

Según los resultados obtenidos de un total de 59 empleados encuestados se obtiene que: 58 personas (98%) expresan que Sí es necesario realizar una Auditoría Informática en la empresa a fin de contribuir al máximo aprovechamiento de los equipos tecnológicos, y 1 persona (2%) manifiesta que no es necesario ejecutar una Auditoría Informática.

3.2. Desarrollo de la propuesta

Auditoría Informática a la Empresa Servisilva Cía. Ltda. del cantón Francisco de Orellana, Provincia de Orellana, período 2020.

La presente Auditoría Informática se llevará a cabo mediante técnicas de Auditoría, efectuándose en función de la siguiente metodología:

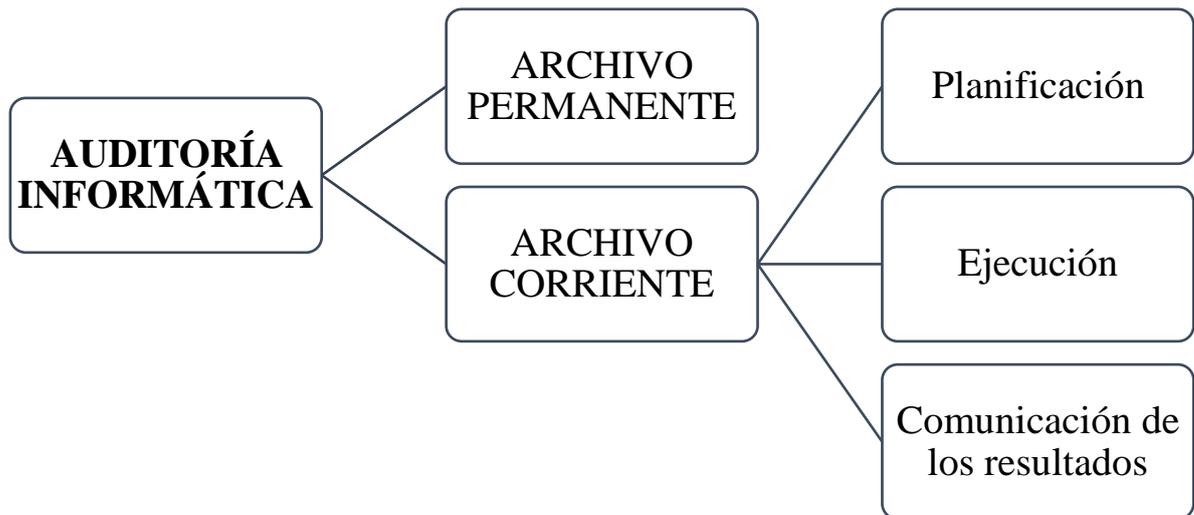


Figura 1-3: Metodología de Auditoría Informática

Fuente: Investigación de Campo

Realizado por: Jaramillo, P. 2023.

ARCHIVO PERMANENTE



CLIENTE:	Servisilva Cía. Ltda.
DIRECCIÓN:	Francisco de Orellana -Vía Lago Agrio Km 7 ½
TIPO DE AUDITORÍA:	Auditoría Informática
PERÍODO:	1 de enero al 31 de diciembre del 2020

Elaborado por: P.A.J.M	Fecha: 04-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 04-01-2022

Orden de Trabajo #001

Fco. de Orellana, 04 de enero del 2022

Mgs.
Ana Galeth Silva
GERENTE GENERAL DE SERVISILVA CÍA. LTDA.

Presente.-

De mi consideración:

De conformidad al plan anual de actividades para el año 2022 del equipo de auditoría, sírvase a realizar la Auditoría Informática a la Empresa Servisilva Cía. Ltda. del cantón Francisco de Orellana, Provincia de Orellana, período 2020, dicha auditoría se efectuará a fin de los siguientes objetivos:

Objetivo General

- Ejecutar una Auditoría Informática a la Empresa Servisilva Cía. Ltda., mediante la aplicación de técnicas de auditoría, a fin de obtener un informe que permita conocer los resultados en el manejo de los recursos tecnológicos, durante el período 2020.

Objetivos Específicos

- Elaborar la planificación de la auditoría estableciendo los procesos a realizar para alcanzar los objetivos planteados.
- Ejecutar la auditoría por medio el uso de los papeles de trabajo para identificar posibles riesgos existentes en el área de sistemas.

Elaborado por: P.A.J.M	Fecha: 04-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 04-01-2022

- Realizar informe emitiendo conclusiones y recomendaciones en base a los hallazgos obtenidos, que servirán de guía para establecer posibles soluciones que contribuyan al mejoramiento continuo de la entidad.

Por su atención, anticipo mi agradecimiento.

Atentamente,

Srta. Paula Jaramillo Moreira
AUTORA DE TESIS

Elaborado por: P.A.J.M	Fecha: 04-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 04-01-2022

SERVISILVA CÍA. LTDA.
PROPUESTA DE TRABAJO DE AUDITORÍA
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

Fco. de Orellana, 05 de enero del 2022

Mgs.
Ana Galeth Silva
GERENTE GENERAL DE SERVISILVA CÍA. LTDA.

Presente.-

De mi consideración:

Tengo el agrado de exponer a su consideración la propuesta de servicios para la ejecución de la Auditoría Informática a la Empresa Servisilva Cía. Ltda. del cantón Francisco de Orellana, Provincia de Orellana, período 2020, la misma que ha sido elaborada para cumplir con los requerimientos y demás disposiciones legales que regulan las actividades de la empresa.

1. Objetivo General

Ejecutar una Auditoría Informática a la Empresa Servisilva Cía. Ltda., mediante la aplicación de técnicas de auditoría, a fin de obtener un informe que permita conocer los resultados en el manejo de los recursos tecnológicos, durante el período 2020,

2. Objetivos Específicos

- Elaborar la planificación de la auditoría estableciendo los procesos a realizar para alcanzar los objetivos planteados.
- Ejecutar la auditoría por medio el uso de los papeles de trabajo para identificar posibles riesgos existentes en el área de sistemas.

Elaborado por: P.A.J.M	Fecha: 05-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 05-01-2022

SERVISILVA CÍA. LTDA.
PROPUESTA DE TRABAJO DE AUDITORÍA
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

- Realizar informe emitiendo conclusiones y recomendaciones en base a los hallazgos obtenidos, que servirán de guía para establecer posibles soluciones que contribuyan al mejoramiento continuo de la entidad.

3. Alcance

La Auditoría Informática se llevará a cabo en la Empresa Servisilva Cía. Ltda., ubicada en el cantón Fco. De Orellana, provincia de Orellana, correspondiente al período 1 de enero al 31 de diciembre del año 2020.

4. Plazo

El tiempo proyectado para la realización de la auditoría informática es de 50 días laborables, los mismos que se encuentran planificados de la siguiente manera:

Actividades	Días estimados
Planificación	12
Ejecución	27
Comunicación de Resultados	11
Total	50

5. Equipo de Trabajo

La firma auditora se encuentra conformada por las siguientes personas:

Nombres	Cargo
Ing. Hítalo Bolívar Veloz Segovia	Jefe de Equipo
Ing. Willian Geovanny Yanza Chávez	Supervisor
Srta. Paula Andrea Jaramillo Moreira	Auditor Senior

Elaborado por: P.A.J.M	Fecha: 05-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 05-01-2022

6. Metodología del Trabajo

Para la ejecución de la Auditoría Informática se aplicarán las Normas Técnicas de Control Interno establecidas por la Contraloría General del Estado

7. Recursos Materiales

Descripción	Cantidad
Esferos	3
Lápices	2
Archivador	1
Borrador	1
Paquete de hojas	1

8. Recursos tecnológicos

Descripción	Cantidad
Computador portátil	1
Cámara digital	1
Impresora	1

Atentamente,

Ing. Willian Yanza Chávez
SUPERVISOR

Elaborado por: P.A.J.M	Fecha: 05-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 05-01-2022



SERVISILVA CÍA. LTDA.
CARTA DE ACEPTACIÓN DE AUDITORÍA
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

CA
1/1



SERVISILVA CÍA. LTDA.
SERVICIOS INDUSTRIALES PETROLEROS
Dir. Vía Coca Lago Agrio Km.7 1/2 – Francisco de Orellana
Tel. 062378060 / 062378081 Email – silva@servisilva.com
Web: www.servisilva.com

Fco. De Orellana, 10 de enero del 2022

Srta.
Paula Jaramillo Moreira
AUTORA DE TESIS

Presente.-

De mi consideración:

Por medio de la presente, me permito manifestar que se ha resuelto brindar la apertura para dar inicio con el proyecto de investigación con el tema de: Auditoría Informática a la Empresa Servisilva Cía. Ltda. del cantón Francisco de Orellana, Provincia de Orellana, período 2020, en atención al Oficio de Orden de Trabajo #001 con fecha 04 de enero de 2022, el personal de la empresa colaborará y participará activamente durante el proceso, brindando las facilidades necesarias para el correcto desarrollo de la investigación.

Por la atención a la presente, nuestros más sinceros agradecimientos.

Atentamente,

Mgs. Ana Galeth Silva
GERENTE GENERAL DE SERVISILVA CÍA. LTDA.

Elaborado por: P.A.J.M	Fecha: 10-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-01-2022



SERVISILVA CÍA. LTDA.
CONTRATO DE AUDITORÍA
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

CA
1/2

En el cantón Francisco de Orellana, provincia de Orellana, a los once días del mes de enero de dos mil veinte dos, se procede a la celebración del presente instrumento denominado Contrato de prestación de servicios de auditoría externa contenido en las siguientes cláusulas:

PRIMERA: COMPARECIENTES

Se celebra el presente contrato entre la Mgs. Ana Galeth Silva, en calidad de Gerente General de Servisilva Cía. Ltda., que a partir de ahora se denominará “Contratante” y por otra parte el Ing. Willian Yanza, representante de la firma auditora, en adelante “Auditor” quienes convienen celebrar un Contrato Civil de Prestación de Servicios Profesionales.

SEGUNDA: ANTECEDENTES

De conformidad con las necesidades presentes de la Empresa Servisilva Cía. Ltda., se ha resuelto contratar los servicios de una Auditoría Informática para obtener un informe que permita conocer los resultados en el manejo de los equipos tecnológicos, durante el período comprendido del 1 de enero al 31 de diciembre del 2020.

TERCERA: OBJETO

El objeto del presente contrato es el desarrollo de la Auditoría Informática a la empresa Servisilva Cía. Ltda., para obtener un informe que permita conocer los resultados en el manejo de los equipos tecnológicos. Al finalizar se entregará un informe elaborado de acuerdo con las NAGAS y las Normas Técnicas de Control Interno, a fin de emitir una opinión profesional.

CUARTA: DURACIÓN

El plazo del presente contrato es de 50 días laborables, contados a partir de la fecha en que se firme dicho contrato. Mismo que será prorrogado 4 días a causa de hechos imprevistos que puedan presentarse en durante el desarrollo de la Auditoría.

Elaborado por: P.A.J.M	Fecha: 11-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 11-01-2022



SERVISILVA CÍA. LTDA.
CONTRATO DE AUDITORÍA

DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

CA

2/2

QUINTA: HONORARIOS

Cabe señalar que el desarrollo de la presente Auditoría Informática es con fines académicos que permitirá obtener el Título de Licenciada en Contabilidad y Auditoría CPA siendo un aporte a la Empresa Servisilva Cía. Ltda., por lo tanto, no existe un valor establecido.

SEXTA: OBLIGACIONES DEL CONTRATANTE

El “contratante” se compromete a entregar oportunamente la información que el “auditor” requiera para la ejecución de la auditoría para el normal desempeño de labores.

SÉPTIMA: OBLIGACIONES DEL AUDITOR

El “auditor” se compromete a desarrollar exclusivamente las actividades descritas en la propuesta de trabajo de Auditoría Informática y entregar el informe final y comunicar los resultados, así como emitir recomendaciones para la toma de decisiones.

OCTAVA: DOMICILIO

Las partes declaran su domicilio en la ciudad de Orellana, en donde se recibirán toda clase de comunicaciones, notificaciones y correspondencia en general.

NOVENA: ACEPTACIÓN

Para constancia de todas cláusulas antes descritas y de la condición para que sea reconocida judicialmente por las partes contratantes, se firma el presente contrato en la ciudad de Orellana, a los once días del mes de enero del 2022

Srta. Paula Jaramillo Moreira
AUTORA DE TESIS

Mgs. Ana Galeth Silva
**GERENTE GENERAL DE
SERVISILVA CÍA. LTDA.**

Elaborado por: P.A.J.M	Fecha: 11-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 11-01-2022



SERVISILVA CÍA. LTDA.
NOTIFICACIÓN DE INICIO DE AUDITORÍA
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

NI
1/1

Fco. De Orellana, 12 de enero del 2022

Mgs.
Ana Galeth Silva
GERENTE GENERAL DE SERVISILVA CÍA. LTDA.

Presente.-

De mi consideración:

Por medio de la presente y en calidad de representante de la firma auditora, me permito comunicar a usted que se iniciará con la Auditoría Informática en la Empresa Servisilva período 1 de enero al 31 de diciembre del 2020, la cual se desarrollará de acuerdo con las Normas Técnicas de Control Interno emitidas por la Contraloría General del Estado en lo referente a Tecnología de Información y Comunicación.

Solicito el apoyo y total colaboración por parte de todos los empleados de la empresa facilitando la información necesaria para la ejecución de la Auditoría Informática cumpliendo con los objetivos y procedimientos en el tiempo programado.

Atentamente,

Ing. Willian Yanza Chávez
SUPERVISOR

Elaborado por: P.A.J.M	Fecha: 12-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 12-01-2022



SERVISILVA CÍA. LTDA.
SOLICITUD DE INFORMACIÓN
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

SI 1/1

Fco. De Orellana, 12 de enero del 2022

Mgs.
Ana Galeth Silva
GERENTE GENERAL DE SERVISILVA CÍA. LTDA.

Presente.-

De mi consideración:

Me permito solicitar de la manera más comedida de su colaboración y colaboración del personal de la Empresa Servisilva Cía. Ltda. para acceder a la debida documentación pertinente como parte de la fase preliminar de la Auditoría Informática, por medio de la presente se sirva facilitar la siguiente información:

- ✚ Organigrama Estructural
- ✚ Base Legal
- ✚ Políticas y Reglamentos Internos
- ✚ Nómina de principales funcionarios
- ✚ Principios y valores corporativos

Agradeciendo de antemano, por la colaboración brindada.

Atentamente,

Srta. Paula Jaramillo Moreira
AUTORA DE TESIS

Elaborado por: P.A.J.M	Fecha: 12-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 12-01-2022



SERVISILVA CÍA. LTDA.
ÍNDICE DEL ARCHIVO PERMANENTE
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

I/AP 1/1

DESCRIPCIÓN	REF. P/T
ARCHIVO PERMANENTE	AP
Información General de la Empresa Servisilva Cía. Ltda.	IG
Hoja de Índices	HI
Hoja de Marcas	HM
Programa de Auditoría	PA

Elaborado por: P.A.J.M	Fecha: 12-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 12-01-2022

Reseña Histórica

Compañía de Servicios Generales Servisilva Cía. Ltda. es una empresa en Ecuador, se encuentra ubicada en la provincia de Orellana Vía Lago Agrio Km 7 ½ cuenta con una gran trayectoria en la industria de petróleo en reparación, construcción, revestimientos y alquiler de herramientas. Fue creada en sociedad de los hermanos Luis Silva e Icela Silva elevan a escritura pública un 28 de octubre de 1994 la constitución de la compañía en responsabilidad limitada, sin embargo, sus inicios de actividades fue un 28 de junio de 1995, fecha en la cual Servisilva Cía. Ltda. empezó a prestar sus servicios y participar en el ámbito del servicio y explotación petrolera. Actualmente emplea a 83 personas (2021). (Servisilva Cía. Ltda. , 2014)

Misión

Brindar el servicio de construcción, reparación y mantenimiento de herramientas, así como asesoramiento y desarrollo del sector petrolero, con tecnología de punta e innovación continua, satisfaciendo los requerimientos de nuestros clientes a través del cumplimiento de estándares internacionales de calidad, contando con personal competente, capacitado y motivado, orientado al logro de la excelencia.

Visión

Ser líderes en el servicio de construcción, reparación y mantenimiento de partes así como brindar asesoramiento y desarrollo de facilidades del sector petrolero, cumpliendo estándares internacionales de calidad, excediendo las expectativas del cliente contando con personal altamente competente, motivado y constantemente capacitado, generando riqueza empresarial y humana, contribuyendo al desarrollo económico del país, logrando un reconocimiento nacional e internacional.

Metas

-  Ser una de las mejores y reconocidas empresas que prestan servicios en el área petrolera a largo plazo.

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

- ✚ Alcanzar rendimiento laboral suficiente, eficiente y eficaz en los empleados año tras año.

Objetivos

- ✚ Alcanzar y mantener los más altos estándares de satisfacción al cliente en el sector petrolero, a través de nuestros servicios innovadores.
- ✚ Tener un desempeño eficiente a largo plazo, y ser la organización más recomendada en la industria.
- ✚ Asegurar la calidad de los productos.
- ✚ Incrementar la participación en el mercado.

Política de Calidad

Servisilva Cía. Ltda., se ha propuesto brindar el servicio de: Operaciones de máquinas herramientas en general; Construcción y reparación de: conexiones rotarias, conexiones en tubería de producción y revestimiento, así como sus herramientas accesorias, cumpliendo con los requerimientos del cliente, legales y reglamentarios, revisando y actualizando los objetivos de la calidad a través de la dirección estratégica, mejorando así continuamente la eficacia del sistema de gestión de calidad y comunicándolos adecuadamente a los miembros de la organización.

Ubicación

Servisilva Cía. Ltda. se encuentra ubicada en la provincia de Orellana, cantón Francisco de Orellana, ciudad Puerto Francisco de Orellana, sector Nuevo Paraíso en la Vía principal a Lago Agrio Km 7 ½.



Figura 2-3: Ubicación Empresa Servisilva Cía. Ltda.

Fuente: Google Maps

Realizado por: Jaramillo, P. 2023.

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

Provincia:	Orellana
Cantón:	Francisco de Orellana
Razón Social:	Servisilva Cía. Ltda.
Representante Legal:	Mgs. Ana Galeth Silva
Teléfono:	062378060/062378081
Correo electrónico:	lsilva@servisilva.com

Principios y valores corporativos

La empresa Servisilva Cía. Ltda. Procura fomentar sus actividades basadas en los siguientes valores y principios, mismos que son el pilar fundamental de la empresa, debido a que constituyen el punto de partida y establece la dirección sobre el cual se va dotando de contenido específico, para ganarse la confianza de los grupos de interés y mejorar de manera continua el servicio y productos que ofrece.

- **Honestidad**

Implica hacer las cosas a conciencia y con el respaldo de la objetividad e imparcialidad, siendo veraces al compartir los pensamientos y sentimientos a la vez que demuestren en las acciones diarias.

- **Trabajo en Equipo**

Permite obtener buenos y mejores resultados, ya que al lograr que todos los miembros de la empresa participen se adquirirá un mayor sentido de pertenencia uniendo esfuerzos para que el día a día sea cada vez más enriquecedor en cuanto a las metas propuestas.

- **Servicio al Cliente**

Un buen servicio al cliente puede llegar a ser un elemento promocional para las ventas de la empresa. atraer un nuevo cliente es aproximadamente seis veces más caro que mantener uno, por eso el comprador siempre está evaluando la forma como la empresa hace negocios, cómo tratan los otros clientes y cómo esperarían que lo trataran a él.

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

- **Calidad**

La presencia de la calidad es algo esencial para cuidar que la oferta de productos y servicios y la Atención al Cliente sea siempre la más adecuada a las necesidades de la empresa.

- **Rentabilidad**

Determina la eficiencia económica que la empresa realiza con un modelo de negocio sólido y así de futuro se fortalecerán las actividades de la empresa.

Logo



Figura 3-3: Logo Empresa Servisilva Cía. Ltda.

Fuente: Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

Base legal

La empresa Servisilva Cía. Ltda. desarrolla sus actividades bajo el siguiente marco legal:

Normas de Creación

- ✚ Constitución de la República del Ecuador
- ✚ Ley de Compañías

Normas de Regulación

- ✚ Ley Orgánica de Régimen Tributario Interno
- ✚ Código de Trabajo
- ✚ Ley del Instituto Ecuatoriano de Seguridad Social
- ✚ Ley de Gestión Ambiental

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

Reglamentos Internos

- ✚ Reglamento Orgánico Funcional por Procesos y de Gestión de Talento Humano de la Empresa Servisilva Cía. Ltda.
- ✚ Reglamento Interno de Trabajo
- ✚ Reglamento Administrativo Interno para el personal de área y de contrato de la Empresa Servisilva Cía. Ltda.

Principales Servicios

- ✚ Reparación de tuberías de producción (Tubing) y revestimiento (Casing).
- ✚ Construcción de roscas rotarias en Drill Collar, Heavy Weight, Drill Pipe, Rotary Sub.
- ✚ Construcción de Cross Over para producción y completación.
- ✚ Máquina para remoción y colocación de Coupling de 2 3/8" hasta 5 1/2"
- ✚ Máquina para aplicación de Bandas duras (Hardbanding).
- ✚ Servicios de taller: Fresadoras, Soldaduras, Prensas, Taladro radial.
- ✚ Working Gauge Ring y Plug para conexiones rotarias.
- ✚ Aplicación de Fosfato de Zinc.

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

SERVISILVA CÍA. LTDA.
INFORMACIÓN GENERAL

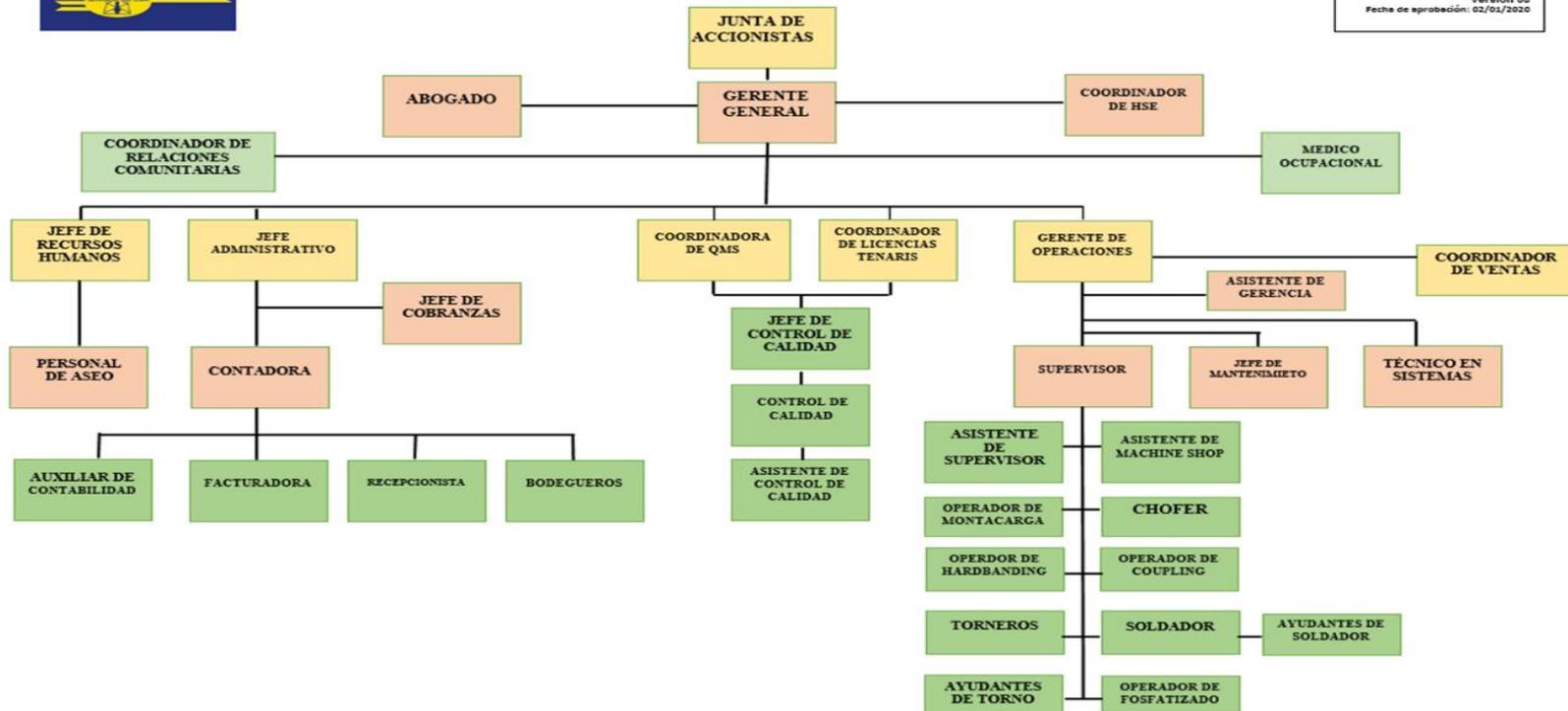
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

Organigrama Estructural



ESTRUCTURA ORGANIZACIONAL SERVISILVA CIA LTDA

Código: RRD-10-02
Versión: 03
Fecha de aprobación: 02/01/2020



Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

MARCA	SIGNIFICADO
AP	Archivo Permanente
IG	Información General
HI	Hoja de Índice
HM	Hoja de Marcas
AC	Archivo Corriente
PA	Programa de Auditoría
VP	Visita Preliminar
CCI	Cuestionario de Control Interno
MP	Memorando de Planificación
MCR	Matriz de Ponderación de Confianza y Riesgo
HH	Hoja de Hallazgos
IFA	Informe Final de Auditoría
PAJM	Paula Andrea Jaramillo Moreira
HBVS	Hítalo Bolívar Veloz Segovia
WGYCH	Willian Geovanny Yanza Chavez

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

SÍMBOLO	SIGNIFICADO
√	Revisado
@	Analizado
Σ	Sumatoria
*	Hallazgo
Ω	Sustentado con evidencia
D	Debilidad
Σ	Sumatoria

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

ARCHIVO CORRIENTE



CLIENTE:	Servisilva Cía. Ltda.
DIRECCIÓN:	Francisco de Orellana -Vía Lago Agrio Km 7 ½
TIPO DE AUDITORÍA:	Auditoría Informática
PERÍODO:	1 de enero al 31 de diciembre del 2020

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

SERVISILVA CÍA. LTDA.
ÍNDICE DEL ARCHIVO CORRIENTE
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

AC	Archivo Corriente
FASE I: PLANIFICACIÓN	
PA/PP	Programa de Auditoría
VP	Visita Preliminar
MP	Memorándum de Planificación
FASE II: EJECUCIÓN	
PA/EJC	Programa de Auditoría
CCI	Cuestionario de Control Interno
MCR	Matriz de Ponderación Confianza y Riesgo
HH	Hoja de Hallazgos
FASE III: COMUNICACIÓN DE RESULTADOS	
PA/CR	Programa de Auditoría
IF/AI	Informe Final de Auditoría Informática

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

FASE I: PLANIFICACIÓN

GAB



AUDITORES INDEPENDIENTES

Objetivo General:

Obtener un conocimiento general de las actividades que se llevan a cabo en el área de sistemas de la Empresa Servisilva Cía. Ltda. mediante visitas preliminares a dicha área para conocer el manejo de los recursos tecnológicos.

Objetivos Específicos:

- ✓ Conocer la situación actual de la empresa y el área de estudio a través de la técnica de observación a fin de ejecutar la auditoría informática.
- ✓ Presentar cédula narrativa acerca los equipos tecnológicos mediante técnica de observación en el área de sistemas percibiendo la realidad del departamento.

N°	PROCEDIMIENTO	REF.	ELABORADO POR	FECHA
1	Elabore el Programa de Auditoría	PA/PP	P.A.J.M	14-01-2022
2	Elabore Narrativa de la Visita Preliminar	NVP	P.A.J.M	14-01-2022
3	Desarrolle el Memorándum de Planificación	MP	P.A.J.M	18-01-2022

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022

Fecha de inicio: 14-01-2022

Fecha de finalización: 14-01-2022

DATOS DE LA INSTITUCIÓN	
Nombre de la Empresa:	SERVISILVA CÍA. LTDA.
Ubicación:	Francisco de Orellana - Orellana
Correo Electrónico:	lsilva@servisilva.com
Teléfono:	(06) 2378060 / (06) 2378081
Horario de Trabajo:	7h00 – 16h30

Se procedió un día Viernes 14 de enero del 2022, siendo las 14h00 de la tarde la visita a las instalaciones de la empresa de servicios petroleros Servisilva Cía. Ltda., ubicada en la Vía Lago Agrio Km 7 ½ margen izquierdo, en acompañamiento del Sr. Luis Silva Rodas quien es el Gerente de Operaciones y posteriormente con el Sr. Juan Molina quien es el Jefe del área de sistemas de dicha organización, en donde se pudo observar y captar información de gran importancia para el trabajo a desarrollar.



Figura 4-3: Vista Exterior Servisilva Cía. Ltda.

Fuente: Servisilva Cía. Ltda.

Realizado por: Jaramillo, P. 2023.

La empresa cuenta con infraestructura adecuada para el desarrollo de actividades administrativas y operativas, a pesar de ello, en el área de Machine Shop (taller) se observa en el suelo las instalaciones eléctricas de forma inadecuadas, por lo que los equipos tecnológicos corren riesgos. No se dispone de una buena cobertura de internet en zonas alejadas a las oficinas administrativas. Se cuentan con cámaras de seguridad en todas las instalaciones de la empresa, sin embargo, el área de sistemas no cuenta con ninguna de ellas.

Elaborado por: P.A.J.M	Fecha: 14-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 14-01-2022



SERVISILVA CÍA. LTDA.
MEMORÁNDUM DE PLANIFICACIÓN
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

MP
1/4

1. INFORMACIÓN DE LA EMPRESA

Razón Social: SERVISILVA CÍA. LTDA.

Sector: Prestación de servicios en el sector petrolero

Ubicación: Francisco de Orellana -Vía Lago Agrio Km 7 ½

Teléfono: (06) 2378060 / (06) 2378081

Correo electrónico: lsilva@servisilva.com

2. OBJETIVO DE LA AUDITORÍA

Ejecutar una Auditoría Informática a la Empresa Servisilva Cía. Ltda., mediante la aplicación de métodos de auditoría, para obtener un informe que permita conocer los resultados en el manejo de los equipos tecnológicos, durante el período 2020.

3. MOTIVO DE LA AUDITORÍA

Se realizará la Auditoría Informática a la Empresa Servisilva Cía. Ltda. a fin de conocer la gestión de los recursos tecnológicos de la misma.

4. ALCANCE

La Auditoría Informática se llevará a cabo en la Empresa Servisilva Cía. Ltda., ubicada en el cantón Fco. De Orellana, provincia de Orellana, correspondiente al período 1 de enero al 31 de diciembre del año 2020.

5. MISIÓN

Brindar el servicio de construcción, reparación y mantenimiento de herramientas, así como asesoramiento y desarrollo del sector petrolero, con tecnología de punta e innovación continua, satisfaciendo los requerimientos de nuestros clientes a través del cumplimiento de estándares internacionales de calidad, contando con personal competente, capacitado y motivado, orientado al logro de la excelencia.

Elaborado por: P.A.J.M	Fecha: 18-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 18-01-2022

6. VISIÓN

Ser líderes en el servicio de construcción, reparación y mantenimiento de partes así como brindar asesoramiento y desarrollo de facilidades del sector petrolero, cumpliendo estándares internacionales de calidad, excediendo las expectativas del cliente contando con personal altamente competente, motivado y constantemente capacitado, generando riqueza empresarial y humana, contribuyendo al desarrollo económico del país, logrando un reconocimiento nacional e internacional.

7. ACTIVIDAD PRINCIPAL

Proveer toda clase de productos y servicios que requieran las empresas petroleras: servicio de taladrado, torneado, fresado, erosión, soldadura, pulido, empalme, entre otros, de piezas de metal, realizadas a cambio de una retribución o contrato.

8. BASE LEGAL

- Constitución de la República del Ecuador
- Ley de Compañías
- Ley Orgánica de Régimen Tributario Interno
- Código de Trabajo
- Ley del Instituto Ecuatoriano de Seguridad Social
- Reglamento Orgánico Funcional por Procesos y de Gestión de Talento Humano de la Empresa Servisilva Cía. Ltda.
- Reglamento Interno de Trabajo
- Reglamento Administrativo Interno para el personal de área y de contrato de la Empresa Servisilva Cía. Ltda.

9. PLAZO

El plazo estimado para el desarrollo de la auditoría es de 50 días laborables. El plazo del contrato se extenderá por 4 días laborables adicionales por hechos imprevistos que puedan presentarse a partir del inicio del trabajo de auditoría.

Elaborado por: P.A.J.M	Fecha: 18-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 18-01-2022

10. FUNCIONARIOS PRINCIPALES

NOMBRE	CARGO
Ana Gissela Galeth Silva	Gerente General
Luis Eduardo Silva Rodas	Gerente de Operaciones
Ángel Rodolfo Jaramillo Arica	Jefe de Ventas
Henry Eduardo Sarango Agreda	Jefe de Recursos Humanos
Francisco Germán Galeth Silva	Jefe Administrativo
Yadira Herrera Cevallos Mendoza	Jefa Financiera

11. EQUIPO AUDITOR

Nombres	Cargo
Ing. Hítalo Bolívar Veloz Segovia	Jefe de Equipo
Ing. Willian Geovanny Yanza Chávez	Supervisor
Srta. Paula Andrea Jaramillo Moreira	Auditora Senior

12. RECURSOS MATERIALES Y TECNOLÓGICOS

Descripción	Cantidad
Esferos	3
Lápices	2
Archivador	1
Borrador	1
Paquete de hojas	1
Computador portátil	1
Cámara digital	1
Impresora	1

Elaborado por: P.A.J.M	Fecha: 18-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 18-01-2022

13. PLAN DE AUDITORÍA

A continuación se detallan las actividades a realizar mediante plan de auditoría:

NO.	ACTIVIDAD	RESPONSABLE	SEMANAS										
			1	2	3	4	5	6	7	8	9		
1	Elaborar plan de auditoría.	Paula Jaramillo Moreira											
2	Aprobar plan de auditoría.	Ing. Hítalo Veloz Segovia											
3	Preparar instrumentos de investigación.	Paula Jaramillo Moreira											
4	Realizar visita preliminar.	Paula Jaramillo Moreira											
5	Inicia Auditoría Informática – Aplicar Cuestionarios.	Paula Jaramillo Moreira											
6	Auditar los recursos tecnológicos de la Empresa.	Paula Jaramillo Moreira											
7	Presentar borrador del Informe.	Paula Jaramillo Moreira											
8	Emitir Informe Final.	Paula Jaramillo Moreira											
9	Comunicar resultados.	Paula Jaramillo Moreira											

14. RESULTADO A OBTENERSE

El resultado del trabajo de auditoría se precisa en el informe final, el mismo que será entregado a la representante legal de la empresa.

 Ing. Willian Yanza Chávez
SUPERVISOR

 Srta. Paula Jaramillo Moreira
AUTORA DE TESIS

Elaborado por: P.A.J.M	Fecha: 18-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 18-01-2022

FASE II: EJECUCIÓN

GAB



AUDITORES INDEPENDIENTES

Objetivo General:

Revisar y evaluar de forma específica el sistema de control interno y emitir informe sobre los resultados obtenidos mediante la evaluación.

Objetivos Específicos:

- ✓ Evaluar los recursos tecnológicos de la empresa mediante aplicación de cuestionarios de control interno, para sustentación de hallazgos.
- ✓ Determinar hallazgos en base de los resultados y evidencia obtenida a fin de emitir recomendaciones que contribuyan al mejoramiento de tareas en el área informática.

N°	PROCEDIMIENTO	REF.	ELABORADO POR	FECHA
1	Elabore el Programa de Auditoría	PA	P.A.J.M	19-01-2022
2	Aplique Cuestionario de Control Interno por componente - COSO II	E/CCI	P.A.J.M	21-01-2022
3	Elabore Matriz de Ponderación Confianza y Riesgo	MCR	P.A.J.M	26-01-2022
4	Desarrolle Hoja de Hallazgos	HH	P.A.J.M	02-02-2022

Elaborado por: P.A.J.M	Fecha: 19-01-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 19-01-2022

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Ambiente de Control					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿La empresa Servisilva Cía. Ltda. posee un código de ética?	X			
2	¿Se cuenta con un manual de tareas plenamente identificadas para el área de sistemas?	X			
3	¿Existe una estructura organizativa definida?	X			
4	¿La empresa tiene el personal adecuado en el área de sistemas para llevar a cabo su función?		X		D1: El jefe del área de sistemas no cuenta con un título profesional a fin.
5	¿Se evalúa el desempeño del personal del área de sistemas?	X			
6	¿Existen políticas de seguridad en el área de sistemas y se verifica su cumplimiento?	X			
7	¿Se realizan capacitaciones a los empleados de Servisilva sobre el uso correcto de los equipos tecnológicos?	X			
8	¿El área de sistemas cuenta con un plan estratégico difundido de manera interna y externa?		X		D2: El área de sistemas no posee de un plan estratégico.
9	¿Las actividades que se llevan a cabo en el área de sistemas son planificadas, ejecutadas y controladas para el logro de los objetivos?	X			
10	¿Cuándo existen problemas en los equipos tecnológicos se los resuelve de forma inmediata?	X			
	TOTAL Σ	8	2		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{8}{10} \right) \times 100\%$	$NR = 100 - 80$
$NC = 80\%$	$NR = 20\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
95% - 76%	75% - 51%	50% - 15%
5% - 24%	25% - 50%	51% - 85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

A través de la aplicación del cuestionario se determinó un nivel de confianza alto de 80%, debido a que cuenta correcta estructura organizativa, manual de funciones y un adecuado establecimiento de políticas, por otra parte, se presenta un nivel de riesgo bajo del 20% con un nivel bajo, puesto que el área de sistemas no cuenta con un plan estratégico y no posee personal con una formación adecuada de tercer nivel.

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Establecimiento de Objetivos					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Los objetivos del área de sistemas contribuyen al cumplimiento de la misión de la empresa?	X			
2	¿Se han establecido políticas, normas y procedimientos en el área de sistemas? ¿Con qué frecuencia se actualizan estos para contribuir al alcance de objetivos del área?		X		D3: Las políticas, normas y procedimientos del área de sistemas no han sido parte de una actualización desde 2016
3	¿Existe participación de los trabajadores de la empresa para el logro de los objetivos?	X			
4	¿Se evalúa el cumplimiento y el grado de logro de los objetivos?	X			
5	¿Se establecen objetivos con indicadores de gestión en el área de sistemas?		X		D4: Ausencia de objetivos con indicadores de gestión en el área de sistemas.
	TOTAL Σ	3	2		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{3}{5} \right) \times 100\%$	$NR = 100 - 60$
$NC = 60\%$	$NR = 40\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
95% - 76%	75% - 51%	50% - 15%
5% - 24%	25% - 50%	51% - 85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

Se puede observar que mediante aplicación de cuestionario de control interno del componente de establecimiento de objetivos, se expuso un nivel de confianza moderado del 60%, por otra parte, el nivel de riesgo es de 40% dado que sus políticas, normas y procedimientos no se encuentran actualizados, y existe una ausencia de objetivos con indicadores en el área de sistemas.

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Identificación de los Riesgos					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen mecanismos para identificar riesgos tanto internos como externos en el área de sistemas?	X			
2	¿Se han identificado y analizado riesgos informáticos potenciales que afecten los equipos tecnológicos, y por ende el logro de los objetivos y desarrollo de actividades?	X			Se presentó una infección en los servidores de la empresa por parte de ransomware.
3	¿Existe confiabilidad de la metodología utilizada para identificar riesgos en el área?		X		D5: No existe una metodología previa para la identificación de riesgos.
4	¿El sistema informático de la empresa se encuentra acorde a las necesidades?	X			
5	¿La empresa cuenta con la elaboración de un análisis FODA en el área de sistemas?	X			
TOTAL Σ		4	1		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{4}{5} \right) \times 100\%$	$NR = 100 - 60$
$NC = 80\%$	$NR = 20\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
95% - 76%	75% - 51%	50% - 15%
5% - 24%	25% - 50%	51% - 85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

Una vez aplicado el cuestionario de control interno del componente de identificación de riesgos, se puede evidenciar un nivel de confianza alto del 80% puesto que posee un sistema informático acorde a las necesidades y un análisis FODA para el área de sistemas, mientras que el nivel de riesgo es del 20% considerado como un nivel bajo, a lo que significa que en el área de sistemas no cuenta con una metodología para la identificación de posibles riesgos que pueden suscitarse.

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Evaluación de los Riesgos					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿En el área de sistemas cuando se identifican riesgos, la empresa realiza una evaluación de los mismos?	X			
2	¿Se evalúa los riesgos informáticos periódicamente para conocer la forma en que estos impactan en la consecución de objetivos y desarrollo de actividades de la empresa?	X			
3	¿Al realizar cambios en el sistema informático y equipos tecnológicos la empresa analiza el impacto de posibles riesgos?	X			
4	¿Se llevan a cabo evaluaciones al personal en el conocimiento de riesgos informáticos?	X			Se aplican las evaluaciones mediante la plataforma de la empresa.
	TOTAL Σ	4	1		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{4}{4} \right) \times 100\%$	$NR = 100 - 100$
$NC = 100\%$	$NR = 0\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
100% - 95% - 76%	75% - 51%	50% - 15%
0% - 5% - 24%	25% - 50%	51% - 85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

Una vez realizado el cuestionario de control interno del componente de evaluación de los riesgos, se determinó un nivel de confianza del 100% que tiende a ser un nivel alto, a fin de que se evalúan de manera periódica los riesgos informáticos, además, de cuando se realizan cambios en los recursos tecnológicos se evalúa su impacto en posibles riesgos.

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Respuesta a los Riesgos					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Se encuentra elaborado un plan de contingencias para afrontar riesgos que se susciten en equipos tecnológicos de la empresa?		X		D6: Se carece de un plan de contingencias para afrontar posibles riesgos en los equipos.
2	¿Se aplican los correctivos necesarios en el caso de detección de riesgos en los equipos?	X			
3	¿Existe un proceso a seguir para brindar respuesta hacia un posible riesgo?	X			
4	¿Al identificarse un riesgo potencial en los equipos tecnológicos, se evalúa posibles respuestas, cómo evitarlo, reducirlo o aceptarlo?	X			
	TOTAL Σ	3	1		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{3}{4} \right) \times 100\%$	$NR = 100 - 75$
$NC = 75\%$	$NR = 25\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
95% - 76%	75% - 51%	50% - 15%
5% - 24%	25% - 50%	51% - 85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

Se puede observar mediante evaluación de cuestionario de control interno del componente respuesta a los riesgos, se posee un nivel de confianza moderado del 75%, y un nivel de riesgo del 25% lo que significa que el área de sistemas de la empresa no cuenta con un plan de contingencias para afrontar riesgos informáticos.

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Actividades de Control					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Se realizan constataciones físicas de los equipos tecnológicos de la empresa?	X			
2	¿Se llevan a cabo actividades de control que incluyen mantenimientos preventivos y correctivos a los equipos?		X		D7: Inexistencia de informes, bitácoras y fichas en donde se detallen el control del mantenimiento brindado.
3	¿Se han establecido controles generales sobre la seguridad, adquisición y mantenimiento de los equipos tecnológicos?	X			
4	¿Se realiza capacitaciones de software y hardware al personal nuevo y antiguo de la empresa?	X			
5	¿Existe un diagrama de red que muestre las conexiones física y lógicas?	X			
6	¿Se encuentra monitoreado el acceso al área de ubicación del servidor?		X		D8: Ausencia de cámaras de seguridad.

7	¿Se tiene asignado un lugar externo para respaldo de información de la empresa en caso de riesgos en los equipos tecnológicos?	X			
8	¿Se cumplen las condiciones adecuadas (temperatura, humedad) para un adecuado manejo de los equipos tecnológicos?	X			
9	¿Se cuenta con un proceso para brindar mantenimiento al hardware y software?	X			
10	¿Existen controles para que solo personal autorizado tenga acceso a los equipos?	X			
11	¿Se realizan respaldos periódicos de la base de datos?	X			
12	¿Existen planos de los puntos de red de la empresa?	X			
13	¿Las instalaciones eléctricas (interruptores de energía, cables de red) se encuentran debidamente protegidos?		X		D9: En determinados espacios, se presentan instalaciones eléctricas inadecuadas.
14	¿Se cuenta con programa de antivirus para la protección de información?	X			
15	¿La empresa cuenta con una buena cobertura en la red inalámbrica de internet?		X		D10: En áreas finales de la empresa la conexión es baja.
	TOTAL Σ	11	4		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{11}{15} \right) \times 100\%$	$NR = 100 - 73.33$
$NC = 73\%$	$NR = 27\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
95% - 76%	75% - 51%	50% - 15%
5% - 24%	25% - 50%	51% - 85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

Una vez realizado el cuestionario de control interno de componente actividades de control, se determinó un nivel de confianza moderado del 73%, y un nivel de riesgo del 27% señalado como un nivel moderado, en consecuencia que en el área de sistemas no se lleva un correcto control y seguridad de los equipos tecnológicos de la empresa.

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Información y Comunicación					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿La comunicación de información al personal, facilita cumplir actividades de forma eficiente y eficaz?	X			
2	¿La empresa utiliza algún sitio web para comunicación interna?	X			Mediante la plataforma de la empresa.
3	¿La información constituye una herramienta de supervisión, para conocer si se han logrado los objetivos de la empresa?	X			
4	¿Los sistemas de información son ágiles y flexibles para integrarse eficazmente en la empresa?	X			
5	¿Se cuentan con sistemas informáticos que aseguran la confiabilidad de la información?	X			
6	¿La comunicación interna se alinea con los diferentes niveles de la empresa?	X			
7	¿El área de sistemas mantiene comunicación constante con el personal de la empresa para asegurar una adecuada operatividad en los equipos?	X			
	TOTAL Σ	7	0		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{7}{7} \right) \times 100\%$	$NR = 100 - 100$
$NC = 100\%$	$NR = 0\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
100% - 95% - 76%	75% - 51%	50% - 15%
0% - 5% - 24%	25% - 50%	51% - 85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

Una vez realizado el cuestionario de control interno de componente de información y comunicación, se determinó un nivel de confianza alto del 100% debido a que la empresa posee una plataforma web para la comunicación interna entre todo el personal tanto administrativo como operativo, asegurando la confiabilidad de la información.

CUESTIONARIO DE CONTROL INTERNO					
Empresa: Servisilva Cía. Ltda.					
Tipo de examen: Auditoría Informática					
Componente: Supervisión y Monitoreo					
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Se evalúa y supervisa el desempeño de los equipos tecnológicos?	X			
2	¿Se realizan inspecciones rutinarias para identificar deficiencias en equipos?	X			
3	¿La administración realiza un monitoreo en el área de sistemas y proporciona recomendaciones sobre riesgos corporativos?	X			
4	¿Se hace evaluaciones de control interno en el área de sistemas?		X		D11: No se realizan evaluaciones de control interno.
5	¿Se investiga y se corrigen las deficiencias encontradas dentro del sistema informático?	X			
	TOTAL Σ	4	1		

NIVEL DE CONFIANZA	NIVEL DE RIESGO
$NC = \left(\frac{\text{Total de SI}}{\text{Total de respuestas}} \right) \times 100\%$	$NR = 100\% - \text{Nivel de confianza}$
$NC = \left(\frac{4}{5} \right) \times 100\%$	$NR = 100 - 80$
$NC = 80\%$	$NR = 20\%$

NIVEL DE CONFIANZA		
ALTO	MODERADO	BAJO
95%-76%	75%-51%	50%-15%
5%-24%	25%-50%	51-85%
BAJO	MODERADO	ALTO
NIVEL DE RIESGO		

Interpretación:

Una vez realizado el cuestionario de control interno de componente supervisión y monitoreo, se determinó un nivel de confianza alto del 80%, y un nivel de riesgo del 20% señalado como un nivel bajo, en razón de que no se han llevado a cabo evaluaciones de control interno.



AUDITORES INDEPENDIENTES

SERVISILVA CÍA. LTDA.
MATRIZ DE PONDERACIÓN CONFIANZA Y RIESGO
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

MCR
1/1

MATRIZ DE EVALUACIÓN DE CONTROL INTERNO – COSO II					
N°	COMPONENTE	% NC	CONFIANZA	% NR	RIESGO
1	Ambiente de Control	80%	Alto	20%	Bajo
2	Establecimiento de Objetivos	60%	Moderado	40%	Moderado
3	Identificación de los Riesgos	80%	Alto	20%	Bajo
4	Evaluación de los Riesgos	100%	Alto	0%	Bajo
5	Respuesta a los Riesgos	75%	Moderado	25%	Moderado
6	Actividades de Control	73%	Moderado	27%	Moderado
7	Información y Comunicación	100%	Alto	0%	Bajo
8	Supervisión y Monitoreo	80%	Alto	20%	Bajo
	TOTAL	81%	Alto	19%	Bajo

Interpretación:

A nivel general mediante evaluación de los 8 componentes del COSO II se obtuvo un nivel de confianza de 81% el cual es considerado como nivel alto, por otra parte, se posee un nivel de riesgo del 19% considerado como bajo. Por tal motivo, se establece que existen ciertas deficiencias en el área de sistemas las cuales deberán ser corregidas y mitigadas para una mejor administración en dicho departamento.

Título
Existencia de personal no calificado en el área de sistemas.
Condición
El Jefe del área de sistemas no cuenta con un título profesional a fin a las actividades que desarrolla en la empresa.
Criterio
De acuerdo con la norma 410-02 “Segregación de Funciones” de Control Interno de la Contraloría General del Estado señala que: “Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo”
Causa
Debido a que la persona que labora en el área de sistemas ha ofrecido sus servicios a largo de cuatro años en Servisilva Cía. Ltda., no se ha realizado seguimiento en cuanto su formación.
Efecto
Al no contar el Jefe de área de sistemas con una instrucción adecuada, se le pueden presentar dificultades en el rendimiento de sus actividades diarias ya sea de instalación, gestión de cuentas o realización mantenimientos.
Conclusión:
El jefe del área de sistemas no posee la formación idónea en tecnologías de la información u otros campos relacionados
Recomendación:
<ul style="list-style-type: none"> Al encargado del área de sistemas seguir con su formación académica de tercer nivel y demás capacitaciones, cumpliendo así apropiadamente con su perfil y manual de funciones establecidos por la empresa.

Título
Falta de un plan estratégico informático.
Condición
No se encuentra establecido un plan estratégico en el área de sistemas que contribuya al adecuado manejo y uso de los equipos tecnológicos existentes en la empresa.
Criterio
De acuerdo con la norma 410-03 “ Plan Informático Estratégico de la Tecnología ” de Control Interno de la Contraloría General del Estado señala que: “La Unidad Tecnológica de la Información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional.” “La descripción documentada y aprobada de los puestos de trabajo que conforman la Unidad de Tecnología de Información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesaria en cada posición, a base de las cuales se realizará la evaluación del desempeño.”
Causa
No se ha elaborado un debido plan estratégico informático que contribuya como una herramienta de apoyo para la dirección de los equipos tecnológicos de la empresa.
Efecto
Con la ausencia de un plan estratégico en el área, los equipos tecnológicos se encuentran sin un adecuado control que garantice su seguridad para el correcto desarrollo de actividades.
Conclusión:
La empresa no tiene establecido un plan estratégico informático en donde se contemplen estrategias organizacionales con los procesos referentes al área de sistemas.
Recomendación:
<ul style="list-style-type: none"> Al encargado del área de sistemas elaborar un plan estratégico enfocado a proporcionar información relevante y comunicativa acerca del sistema informático de la empresa Servisilva Cía. Ltda.

Título
No se han realizado actualizaciones en las políticas, normas y procedimientos
Condición
Las políticas, normas y procedimientos del área de sistemas no han sido parte de una actualización desde 2016.
Criterio
De acuerdo con la norma 410-04 “ Políticas y procedimientos ” de Control Interno de la Contraloría General del Estado manifiesta que: “La Unidad Tecnológica de Información definirá, documentará y difundir a las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, esto se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución.”
Causa
El encargado del área de sistemas no considera que las políticas, normas y procedimientos requieran de una actualización, sin embargo esta es una actividad de suma importancia.
Efecto
La desactualización de las políticas y procedimientos conllevan a que los funcionarios de la empresa no tengan conocimientos de las normas a seguir para el correcto manejo de los equipos tecnológicos y sistema informático, dificultando el cumplimiento de actividades.
Conclusión:
Al no tener una debida actualización de las políticas y procedimientos del área de sistemas, cada empleado labora a su criterio sin tomar en cuenta los lineamientos a seguir en cuanto al manejo y uso los equipos tecnológicos.
Recomendación:
<ul style="list-style-type: none"> Al encargado del área de sistemas actualizar y difundir las políticas y procedimientos para que el personal de la empresa realice y cumpla con sus actividades de manera oportuna, contribuyendo así a la consecución de objetivos institucionales.

Título
Ausencia de objetivos con indicadores de gestión en el área de sistemas.
Condición
El área de sistemas no ha establecido indicadores de gestión para áreas que requieren de la utilización de equipos tecnológicos.
Criterio
De acuerdo con la norma 410-13 “ Monitoreo y evaluación de los procesos y servicios ” de Control Interno de la Contraloría General del Estado manifiesta que: “La Unidad Tecnológica de Información de cada organización definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión toma los correctivos que se requieran.”
Causa
No se han establecido indicadores de gestión, por lo cual no se evalúa y mide el grado de cumplimiento de actividades en términos de eficiencia, eficacia y economía, en consecuencia, conlleva a que no se cumplan con los objetivos establecidos por Servisilva Cía. Ltda.
Efecto
No se conoce el impacto y desempeño de los equipos tecnológicos en la empresa y ocasiona que no garantice contra con la información precisa en aspecto de eficiencia y eficacia de la gestión de los equipos.
Conclusión:
El área de sistemas no cuenta con indicadores de gestión de los equipos tecnológicos el mismo que por falta de ellos no se puede llegar a medir el desempeño y monitorear la gestión y tomar correctivos que requieran estos.
Recomendación:
<ul style="list-style-type: none"> Al encargado del área de sistemas implementar indicadores de gestión, para que estos supervisen el cumplimiento de los objetivos planteados y contribuyan al desempeño empresarial.

Título
No existe una metodología previa para la identificación de riesgos.
Condición
Falta de metodología para la identificación de riesgos informáticos que puedan suscitarse en la empresa Servisilva Cía. Ltda.
Criterio
De acuerdo con la norma 410-06 “ Administración de proyectos tecnológicos ” de Control Interno de la Contraloría General del Estado manifiesta que: La Unidad Tecnológica de Información definir los mecanismos que faciliten la administración de todos los proyectos de informáticos que ejecuten las diferentes áreas que conforman dicha unidad: <ol style="list-style-type: none"> 1. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrado sin considerados para la planificación de otros futuros.
Causa
Por falta de protección y seguridad no se ha implementado una metodología de identificación de riesgos informáticos para los equipos tecnológicos.
Efecto
Ocurrencia de daños y pérdida de información en los equipos tecnológicos de la empresa debido a que no se presenta una acción preventiva para el reconocimiento de riesgos.
Conclusión:
En caso de posibles riesgos que puedan suscitarse referente a las operaciones del área de sistemas, no existe una metodología previa para la identificación de los mismos, por lo tanto, la solución de riesgos informáticos de manera correctiva y no preventiva.
Recomendación:
<ul style="list-style-type: none"> • Al encargado del área de sistemas implementar metodología en donde se identifique y analice riesgos y amenazas de manera que se determine las medidas de seguridad para afrontar posibles riesgos existentes.

Título
Falta de plan de contingencia.
Condición
Se carece de un plan de contingencias para afrontar posibles riesgos en los equipos tecnológicos.
Criterio
De acuerdo con la norma 410-11 “ Plan de contingencias ” de Control Interno de la Contraloría General del Estado menciona que: “Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contención que describa las acciones se tomará en caso de una emergencia o suspensión de procesamiento de la información por problemas en los equipos, programas o personal relacionado.”
Causa
No se tiene establecido un plan de contingencias en donde se detallen las acciones a seguir en caso de emergencia, esto con el objetivo de poder minimizar riesgos.
Efecto
Al no contar con un plan de contingencias ocasiona que no se obtengan respuestas a riesgos, mismas en donde se describen las acciones a tomar en casos de presentarse fallos en los recursos tecnológicos.
Conclusión:
La empresa no dispone de un plan de contingencias que especifique acciones en caso de presentarse una emergencia, el mismo que corresponde al departamento de sistemas la realización de este.
Recomendación:
<ul style="list-style-type: none"> • Al encargado del área de sistemas, desarrollar un plan de contingencias para su debido aprobación y difusión de acuerdo con la normativa legal, el mismo que debe ser evaluado y actualizado periódicamente. • Al gerente de operaciones aprobar dicho plan de contingencias para que se ejecute en la empresa.

Título
Falta de control en los mantenimientos brindados a los equipos tecnológicos.
Condición
Inexistencia de informes, bitácoras y fichas en donde se detallen el control de mantenimientos correctivos y preventivos brindados a los equipos tecnológicos de Servisilva Cía. Ltda.
Criterio
De acuerdo con la norma 410-09 “Mantenimiento y control de la infraestructura tecnológica” de Control Interno de la Contraloría General del Estado manifiesta que: “La Unidad Tecnológica de Información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.” El tema por considerar: <ol style="list-style-type: none"> 1. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implementación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estos serán registrados en su correspondiente bitácora e informados a todos los actores usuarios finales relacionados adjuntando las respectivas evidencias
Causa
Se llevan a cabo los mantenimientos a los equipos tecnológicos, sin embargo no existe un documento que avale el control de que si se esté realizando dichos mantenimiento preventivo y correctivo.
Efecto
Fallo en el control y manejo de información del área de sistemas en consecuencia que no existe un registro de que si se realizan estos mantenimientos
Conclusión:
No se dispone de un control para mantenimiento preventivo y correctivo de forma documentada, mismo que sirve de soporte para información del área de sistemas
Recomendación:
<ul style="list-style-type: none"> • Al encargado del área de sistemas mantener un control de los mantenimientos otorgados a los equipos tecnológicos mediante bitácoras de registro a fin de tener un adecuado manejo y control de los problemas presentes en los equipos.

Título
Ausencia de cámaras de seguridad.
Condición
El acceso al área de sistemas de la empresa no se encuentra asegurada.
Criterio
De acuerdo con la norma 410-10 “Seguridad de tecnología de información” de Control Interno de la Contraloría General del Estado manifiesta que: “La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesan mediante sistemas informáticos.”
<ol style="list-style-type: none"> 1. Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas. 2. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros.
Causa
Descuido por parte del personal no establecer una medida adicional de seguridad para la protección del servidor
Efecto
Pérdida de equipos tecnológicos que se encuentren el área de sistemas, debido a que no existe la correcta seguridad para proteger dichos equipos. Por otra parte, se puede suscitar hechos de sustracción de información de carácter confidencial para la empresa.
Conclusión: El área de sistemas no cuenta con una cámara de videovigilancia que permita que los equipos tecnológicos, servidor, entre otros se encuentren seguros y a bajo recaudo, ocasionando pérdida de equipos y toma de información.
Recomendación:
<ul style="list-style-type: none"> • Al encargado del área de sistemas solicitar la instalación de cámaras de videovigilancia para el área correspondiente contribuyendo así a una mayor seguridad de los recursos tecnológicos, evitando así posibles pérdidas.

Título
Instalaciones eléctricas inadecuadas.
Condición
Las instalaciones eléctricas de determinadas áreas de la empresa no se encuentran en condiciones adecuadas para el funcionamiento adecuado de los recursos tecnológicos.
Criterio
De acuerdo con la norma 410-10 “ Seguridad de tecnología de información ” de Control Interno de la Contraloría General del Estado manifiesta que: “La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesan mediante sistemas informáticos.” 1. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros.
Causa
Despreocupación por parte del personal en realizar mantenimientos y verificar las condiciones de la infraestructura eléctrica para posteriormente tomar medidas inmediatas.
Efecto
Las malas instalaciones eléctricas han provocado que los empleados se tropiecen en cables de los equipos tecnológicos y por ende se proceden a desconectarse, ocasionado daños en los equipos de cómputo provocando que no trabajen de manera correcta.
Conclusión: Las instalaciones eléctricas de la empresa es de suma importancia debido a que si no se encuentran en buenas condiciones e instaladas correctamente, se corre el riesgo de que existan daños que no puedan solucionarse.
Recomendación:
<ul style="list-style-type: none"> • Al encargado del área de sistemas verificar las condiciones adecuadas para el apropiado desarrollo de actividades y buen funcionamiento de los equipos. • Al Gerente de Operaciones, asignar un personal capacitado para que se efectúe mantenimiento en las instalaciones eléctricas e infraestructura.

Título
Cobertura de red inalámbrica y servicios de red inestables
Condición
Áreas posteriores de la empresa cuentan con servicio y cobertura de red inestable.
Criterio
De acuerdo con la norma 410-14 “ Sitios web, servicios de internet e intranet ” de Control Interno de la Contraloría General del Estado manifiesta que: “La Unidad de Tecnología de Información, considerará el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general.” “Elaborará normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de los requerimientos de los usuarios externos e internos”
Causa
No se han realizado las adquisiciones e instalaciones debidas de puntos de red en las áreas posteriores de la empresa.
Efecto
Retraso de comunicación e intercambio de información entre trabajadores.
Conclusión: En el área de suelda y fosfatizado que se encuentran en las partes posteriores de la empresa la cobertura de la red inalámbrica y los servicios de red son de mala calidad, en consecuencia la comunicación interna se dificulta siendo un factor importante.
Recomendación:
<ul style="list-style-type: none"> Al encargado del área de sistemas, solicitar nuevos puntos de red mediante routers los mismos que deberán ser instalados en las áreas posteriores de la empresa.

Título
No se realizan evaluaciones de control interno.
Condición
Inexistencia de informes de control de los equipos tecnológicos de Servisilva Cía. Ltda.
Criterio
De acuerdo con la norma 600 “Seguimiento” de Control Interno de la Contraloría General del Estado manifiesta que: “La máxima autoridad y los directivos de la entidad, establecerán procedimientos de seguimiento continuo, evaluaciones periódicas o una combinación de ambas para asegurar la eficacia del sistema de control interno”
Causa
No existe una persona delegada o encargada de elaborar evaluaciones e informe de control concerniente al área de sistemas.
Efecto
Los problemas que surgen en el área de sistemas, se solucionan en base de acciones correctivas según estas van apareciendo, al contrario de ser obtenidos en base a un informe técnico de control interno.
Conclusión: No se llevan a cabo evaluaciones y emisión de informes de control interno de manera periódica que sirvan de base para la corrección de fallos en los procedimientos o actividades que se perciban en el área de sistemas.
Recomendación:
<ul style="list-style-type: none"> • Al gerente de la empresa, asignar una persona encargada de realizar la emisión de control en los diferentes procesos del área, a fin de obtener información competente y actualizada. • Al encargado del área de sistemas, solicitar los informes de control interno con el objetivo de tomar las decisiones oportunas en base a los resultados obtenidos mediante evaluación.

FASE III: COMUNICACIÓN DE RESULTADOS



AUDITORES INDEPENDIENTES

Objetivo General:

Elaborar el informe final de Auditoría Informática conforme los requerimientos y normas de auditoría a fin de dar a conocer las conclusiones y recomendaciones del trabajo de investigación a los miembros de la empresa.

N°	PROCEDIMIENTO	REF.	ELABORADO POR	FECHA
1	Elabore el Programa de Auditoría	PA/CR	P.A.J.M	04/02/2022
2	Realice la Convocatoria para Lectura del Informe Final de Auditoría	CLI	P.A.J.M	07/02/2022
3	Redacte la Carta de Presentación del Informe	CP	P.A.J.M	10/02/2022
4	Elabore Informe Final de Auditoría Informática en base a los resultados obtenidos.	IFAI	P.A.J.M	10/02/2022

Elaborado por: P.A.J.M	Fecha: 04-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 04-02-2022



SERVISILVA CÍA. LTDA.
CONVOCATORIA DE LECTURA DEL INFORME
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

CLI 1/1

DE: Equipo de Trabajo GAB “Auditores Independientes”

PARA: Mgs. Ana Galeth Silva - GERENTE GENERAL DE SERVISILVA CÍA. LTDA.

ASUNTO: Lectura Informe de Auditoría

FECHA: Fco. De Orellana, 07 de febrero 2022

De conformidad a lo estipulado en el contrato de servicios profesionales y programa de auditoría, me permito convocar a la conferencia de lectura del Informe de Auditoría Informática a la Empresa Servisilva Cía. Ltda., ubicada en el cantón Francisco de Orellana, provincia de Orellana, misma a realizarse el día 10 de febrero del 2022 en la sala de reuniones de la empresa.

Atentamente,

Ing. Hítalo Veloz Segovia

JEFE DE EQUIPO

Elaborado por: P.A.J.M	Fecha: 07-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 07-02-2022



SERVISILVA CÍA. LTDA.
CARTA DE PRESENTACIÓN
DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2020

CP
1/1

Fco. De Orellana, 10 de febrero 2022

Mgs.
Ana Galeth Silva
GERENTE GENERAL DE SERVISILVA CÍA. LTDA.
Presente.-

De mi consideración:

Se ha efectuado la Auditoría Informática a la empresa SERVISILVA CÍA. LTDA., comprendida entre el período del 01 de enero al 31 de diciembre del 2020.

El trabajo permitió la utilización de las Normas de Control Internos emitidas por la Contraloría General del Estado en lo concerniente a Tecnología de Información y Comunicación (410) las cuales demandan que cada actividad sea planificada y efectuada en el tiempo establecido, de esta manera ofrecen seguridad razonable en cada proceso existente en la empresa.

Nuestra responsabilidad se basa en expresar una opinión acerca del manejo de los equipos tecnológicos realizada por el encargado del área de sistemas basada en la auditoría efectuada que se encuentra sustentada con evidencia suficiente, pertinente y competente. Además, se verificó que las responsabilidades asignadas a cada miembro de trabajo sean realizadas con cautela y cumpliendo con la seriedad respectiva, para lo cual se analizó y evaluó documentación y archivos de la empresa Servisilva Cía. Ltda.

Los resultados encontrados mediante ejecución de auditoría se encuentran interpretados en las conclusiones y recomendaciones que constan en el presente informe.

Atentamente,

Ing. Willian Yanza Chávez
SUPERVISOR

Elaborado por: P.A.J.M	Fecha: 10-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-02-2022

SERVISILVA CÍA. LTDA.



**INFORME DE AUDITORÍA INFORMÁTICA
DEL 1 DE ENERO AL 31 DE DICIEMBRE
DEL 2020**

RIOBAMBA – ECUADOR

2022

CAPÍTULO I

MOTIVO DE LA AUDITORÍA

El trabajo se efectúa a razón de que la empresa Servisilva Cía. Ltda. no ha sido objeto de una auditoría informática que permita evaluar y conocer los resultados en el manejo de los equipos tecnológicos de la institución.

OBJETIVOS DE LA AUDITORÍA

Objetivo General

Ejecutar una Auditoría Informática a la Empresa Servisilva Cía. Ltda., mediante la aplicación de métodos de auditoría, para obtener un informe que permita conocer los resultados en el manejo de los equipos tecnológicos, durante el período 2020.

Objetivos Específicos

- Elaborar la planificación de la auditoría estableciendo los procesos a realizar para alcanzar los objetivos planteados.
- Ejecutar la auditoría por medio el uso de los papeles de trabajo para identificar posibles riesgos existentes en el área de sistemas.
- Realizar informe emitiendo conclusiones y recomendaciones en base a los hallazgos obtenidos, que servirán de guía para establecer posibles soluciones que contribuyan al mejoramiento continuo de la entidad.

ALCANCE

La Auditoría Informática se llevará a cabo en la Empresa Servisilva Cía. Ltda., ubicada en el cantón Fco. De Orellana, provincia de Orellana, correspondiente al período 1 de enero al 31 de diciembre del año 2020.

BASE LEGAL

Elaborado por: P.A.J.M	Fecha: 10-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-02-2022

1. Constitución de la República del Ecuador
2. Ley de Compañías
3. Ley Orgánica de Régimen Tributario Interno
4. Código de Trabajo
5. Ley del Instituto Ecuatoriano de Seguridad Social
6. Reglamento Orgánico Funcional por Procesos y de Gestión de Talento Humano de la Empresa Servisilva Cía. Ltda.
7. Reglamento Interno de Trabajo
8. Reglamento Administrativo Interno para el personal de área y de contrato de la Empresa Servisilva Cía. Ltda.

CAPÍTULO II

RESULTADOS DE LA AUDITORÍA INFORMÁTICA

Existencia de personal no calificado en el área de sistemas

Conclusión

El jefe del área de sistemas no posee la formación idónea en tecnologías de la información u otros campos relacionados.

Recomendación:

Al encargado del área de sistemas seguir con su formación académica de tercer nivel y demás capacitaciones, cumpliendo así apropiadamente con su perfil y manual de funciones establecidos por la empresa.

Falta de un plan estratégico informático

Conclusión

La empresa no tiene establecido un plan estratégico informático en donde se contemplen estrategias organizacionales con los procesos referentes al área de sistemas.

Elaborado por: P.A.J.M	Fecha: 10-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-02-2022

Recomendación

Al encargado del área de sistemas elaborar un plan estratégico enfocado a proporcionar información relevante y comunicativa acerca del sistema informático de la empresa Servisilva Cía. Ltda.

No se han realizado actualizaciones en las políticas, normas y procedimientos

Conclusión

Al no tener una debida actualización de las políticas y procedimientos del área de sistemas, cada empleado labora a su criterio sin tomar en cuenta los lineamientos a seguir en cuanto al manejo y uso los equipos tecnológicos.

Recomendación

Al encargado del área de sistemas actualizar y difundir las políticas y procedimientos para que el personal de la empresa realice y cumpla con sus actividades de manera oportuna, contribuyendo así a la consecución de objetivos institucionales.

Ausencia de objetivos con indicadores de gestión en el área de sistemas

Conclusión

El área de sistemas no cuenta con indicadores de gestión de los equipos tecnológicos el mismo que por falta de ellos no se puede llegar a medir el desempeño y monitorear la gestión y tomar correctivos que requieran estos.

Recomendación

Al encargado del área de sistemas implementar indicadores de gestión, para que estos supervisen el cumplimiento de los objetivos planteados y contribuyan al desempeño empresarial.

Elaborado por: P.A.J.M	Fecha: 10-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-02-2022

No existe una metodología previa para la identificación de riesgos

Conclusión

En caso de posibles riesgos que puedan suscitarse referente a las operaciones del área de sistemas, no existe una metodología previa para la identificación de los mismos, por lo tanto, la solución de riesgos informáticos de manera correctiva y no preventiva.

Recomendación

Al encargado del área de sistemas implementar metodología para identificación de riesgos que se requiere para los equipos tecnológicos.

Falta de plan de contingencia

Conclusión

La empresa no dispone de un plan de contingencias que especifique acciones en caso de presentarse una emergencia, el mismo que corresponde al departamento de sistemas la realización de este.

Recomendación

Al encargado del área de sistemas, desarrollar un plan de contingencias para su debido aprobación y difusión de acuerdo con la normativa legal, el mismo que debe ser evaluado y actualizado periódicamente.

Al gerente de operaciones aprobar dicho plan de contingencias para que se ejecute en la empresa.

Falta de control en los mantenimientos brindados a los equipos tecnológicos

Conclusión

No se dispone de un control para mantenimiento preventivo y correctivo de forma documentada, mismo que sirve de soporte para información del área de sistemas

Recomendación

Al encargado del área de sistemas mantener un control de los mantenimientos otorgados a los equipos tecnológicos, para así tener un mejor manejo y control de los problemas presentes en los equipos.

Elaborado por: P.A.J.M	Fecha: 10-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-02-2022

Ausencia de cámaras de seguridad

Conclusión

El área de sistemas no cuenta con una cámara de videovigilancia que permita que los equipos tecnológicos, servidor, entre otros se encuentren seguros y a bajo recaudo, ocasionando pérdida de equipos y toma de información.

Recomendación

Al encargado del área de sistemas solicitar cámaras de videovigilancia para el área correspondiente contribuyendo así a una mayor seguridad, evitando posibles pérdidas

Instalaciones eléctricas inadecuadas

Conclusión

Las instalaciones eléctricas de la empresa son de suma importancia debido a que si no se encuentran en buenas condiciones e instaladas correctamente, se corre el riesgo de que existan daños que no puedan solucionarse.

Recomendación

Al encargado del área de sistemas verificar las condiciones adecuadas para el apropiado desarrollo de actividades y buen funcionamiento de los equipos.

Al Gerente de Operaciones, asignar un personal capacitado para que se efectúe mantenimiento en las instalaciones eléctricas e infraestructura.

No se realizan evaluaciones de control interno

Conclusión

No se llevan a cabo evaluaciones y emisión de informes de control interno de manera periódica que sirvan de base para la corrección de fallos en los procedimientos o actividades que se perciban en el área de sistemas.

Elaborado por: P.A.J.M	Fecha: 10-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-02-2022

Recomendación

Al gerente de la empresa, asignar una persona encargada de realizar la emisión de control en los diferentes procesos del área, a fin de obtener información competente y actualizada.

Al encargado del área de sistemas, solicitar los informes de control interno con el objetivo de tomar las decisiones oportunas en base a los resultados obtenidos mediante evaluación.

Cobertura de red inalámbrica y servicios de red inestables

Conclusión

En el área de suelda y fosfatizado que se encuentran en las partes posteriores de la empresa la cobertura de la red inalámbrica y los servicios de red son de mala calidad, en consecuencia la comunicación interna se dificulta siendo un factor importante.

Recomendación

Al encargado del área de sistemas, solicitar nuevos puntos de red mediante routers los mismos que deberán ser instalados en las áreas posteriores de la empresa.

Elaborado por: P.A.J.M	Fecha: 10-02-2022
Revisado por: H.V.S / W.V.Y.CH	Fecha: 10-02-2022

CONCLUSIONES

- La auditoría realizada a la empresa Servisilva Cía. Ltda. De la ciudad de Francisco de Orellana, provincia de Orellana, por el período 2020, detectó falencias en el manejo de recursos tecnológicos e instalaciones, consecuencia de la inexistencia de controles de riesgos informáticos y de seguridad física y lógica.
- La empresa Servisilva Cía. Ltda., no cuenta con políticas de seguridad, manuales, planes y normas actualizadas, que ayuden a un correcto manejo de la infraestructura informática, por tal motivo la seguridad de los recursos informáticos se encuentran en riesgo afectando la confiabilidad y disponibilidad de la información.
- La empresa Servisilva Cía. Ltda. no cuenta con una adecuada identificación de los factores de riesgos internos y externos, que conlleven daños o pérdidas de los recursos tecnológicos.
- Los hallazgos presentados en el informe de auditoría sirven como soporte y guía para las autoridades y personal del área de sistemas de la empresa Servisilva Cía. Ltda. en el desarrollo de procesos eficientes que aprovechen los recursos tecnológicos.

RECOMENDACIONES

- A los directivos de la empresa disponer de la realización de auditorías de manera periódica, que permitan detectar de manera oportuna las deficiencias de control interno informático y de manera recurrente ejercer acciones para corregir errores que puedan afectar los resultados de la gestión empresarial.
- Al personal del área de sistemas y directivos de la institución diseñar e implementar políticas, plan estratégico, sistema de control y manuales informáticos con la finalidad de garantizar la seguridad de los recursos tecnológicos y de la información que maneja Servisilva Cía. Ltda., permitiendo identificar riesgos y contribuyendo al desarrollo de actividades con óptimos resultados.
- Al personal del área de sistemas diseñar e implementar medidas que favorezcan en la identificación de riesgos informáticos recurrentes en la empresa para brindar soluciones eficientes y eficaces.
- Al personal del área de sistemas y directivos de la institución recepten y apliquen las recomendaciones descritas en el informe de auditoría, a fin de establecer medidas correctivas para la protección y seguridad de los recursos tecnológicos, permitiendo la adopción de las decisiones y el cumplimiento de los objetivos de la empresa.

GLOSARIO

Amenazas: acciones que pueden producir consecuencias negativas en las operaciones de una empresa resultando daños en los recursos informáticos, pueden ser de carácter físico o lógico (Voutssas, 2010, pág. 12).

Auditor: persona con atributos personales y aptitudes demostradas para aplicar conocimientos y habilidad para llevar a cabo una auditoría (OHSAS 18001, 2015).

Control interno: proceso que tiene como objeto asegurar la protección de todos los recursos informáticos, mejorando los índices operativos de economía, eficiencia y eficacia (Marcano, 2017, pág. 3).

Riesgo: probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la institución (Metodología para la Gestión de la Seguridad Informática, 2013, pág. 8).

Seguridad física: aquellas que protegen el acceso físico a los activos y las condiciones ambientales en las que estos se utilizan (Imbaquingo, PUSDÁ, & Jácome, 2016, pág. 71).

Seguridad informática: proceso de establecer estrategias, políticas y procedimientos con el fin de salvaguardar de daños a los recursos informáticos de una organización (Voutssas, 2010, pág. 5).

Sistema informático: conjunto de partes interrelacionadas que emplea un ordenador que usa dispositivos programables para capturar, almacenar y procesar datos (Raya, Raya, & Zurdo, 2014, pág. 18).

Seguridad lógica: se encargan de proteger los activos a través de herramientas, técnicas y programas informáticos. (Imbaquingo, PUSDÁ, & Jácome, 2016, pág. 71).

Virus: programas maliciosos establecidos para manipular los sistemas informáticos, sin el conocimiento ni consentimiento de los usuarios (Santos, 2015, pág. 124).

BIBLIOGRAFÍA

- Acosta, E., & Almeida, M. (2013). *Informe Coso II*. Recuperado de <https://www.auditool.org/blog/control-interno/290-el-informe-coso-i-y-ii>
- Arens, A., Elder, R., & Beasley, M. (2007). *Auditoría un enfoque integral*. México: Pearson Educación.
- Baca, G. (2016). *Introducción a la Seguridad Informática* (1ª ed.). México: Patria.
- Blanco, L. (2008). *Auditoría y Sistemas Informáticos* (1ª ed.). La Habana: Félix Varela.
- Calapucha, A. (2020). *Auditoría Informática a la Unidad de Tecnologías de la Información y Comunicación del Gobierno Autónomo Descentralizado Municipal del cantón Loreto, provincia de Orellana, período 2018*. (Tesis de pregrado). Escuela Superior Politécnica de Chimborazo, Riobamba.
- Carrillo, K. (2018). *Evaluación del Riesgo Informático en el centro de cómputo de la biblioteca de la UTMACH*. (Tesis de pregrado). Universidad Técnica de Machala, Machala.
- COBIT 5. (2012). *IT Governance Institute*. EEUU: ISACA.
- Contraloría General del Estado. (2011). *Ejecución del Trabajo*. Recuperado de <http://www.contraloria.gob.ec/documentos/normatividad/MGAG-Cap-VI.pdf>
- Echenique, J. (2001). *Auditoría informática*. Recuperado de <https://es.slideshare.net/underman/libro-auditoria-informatica-jose-antonio-echenique>
- Echenique, J. (2013). *Auditoría en Informática* (2ª ed.). México: McGraw-Hill.
- Hermoso, J. (2013). *Informática aplicada a la gestión de las empresas*. México: ESIC.
- Imbaquingo, D., PUSDÁ, M., & Jácome, J. (2016). *Fundamentos de Auditoría Informática basada en riesgos*. (Tesis de pregrado). Universidad Técnica del Norte, Ibarra.
- López, P. (2004). Población muestra y muestreo. *Scielol*, 1.
- Marcano, P. (2017). *Control Interno y Control Interno Informático*. México: ISSUU.
- (2013). *Metodología para la Gestión de la Seguridad Informática*. Recuperado de <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf>
- Muñoz, C. (2002). *Auditoría en Sistemas Computacionales* (1ª ed.). México: Pearson Educación.
- Neira, M. (2019). *Auditoría Informática a la Unidad Educativa Fiscomisional "San Vicente de Paúl" del cantón Riobamba, provincia de Chimborazo, períodos 2016 - 2017*. (Tesis de pregrado). Escuela Superior Politécnica de Chimborazo, Riobamba.
- OHSAS 18001. (2015). *El auditor según la norma OHSAS 18001:2007*. Recuperado de <https://www.nueva-iso-45001.com/2015/01/auditor-norma-ohsas-18001-2007/>
- Piattini, M., Navarro, E., & Ruiz, M. (2015). *Auditoría de tecnologías y sistemas de información*. Madrid: Ra-Ma. Recuperado de <https://elibro.net/es/ereader/epoch/106490>

- Quintuña, V. (2012). *Auditoría Informática a la Superintendencia de Telecomunicaciones*. Recuperado de <https://dspace.ucuenca.edu.ec/bitstream/123456789/652/1/ts205.pdf>
- Raya, J., Raya, L., & Zurdo, J. (2014). *Sistemas Informáticos*. España: Ra-Ma.
- Salgado, M., Osuna, N., Sevilla, M., & Morales, J. (2017). La Auditoría Informática en las organizaciones. *Scielo*, 4(8).
- Sánchez, W. (2021). *Teoría de la Auditoría* (1ª ed.). Bogotá: Nueva Legislación SAS.
- Sandoval, H. (2012). *Introducción a la Auditoría* (1ª ed.). México: Red Tercer Milenio.
- Santos, J. (2015). *Seguridad Informática*. Madrid: Ra-Ma.
- Tamayo, A. (2001). *Auditoría de Sistemas una visión práctica* (1ª ed.). Colombia: UNC
- Tendencias & Innovación. (2018). *Pasos para realizar una auditoría informática*. Recuperado de <https://www.obsbusiness.school/blog/que-es-una-auditoria-informatica-y-que-debes-saber-sobre-ella>
- Villena, J. (2019). *Auditoría Informática a la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal del cantón San Pedro de Pelileo, provincia de Tungurahua, período 2016*. (Tesis de pregrado). Escuela Superior Politécnica de Chimborazo, Riobamba.
- Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Scielo*, 24(50).

ANEXOS

ANEXO A: DOCUMENTACIÓN

410-1 Organización informática. - Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo. Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-2 Segregación de funciones.- Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal. La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplar los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

410-03 Plan informático estratégico de tecnología.- La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario. La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia. Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico. El plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos serán analizados y aprobados por la máxima autoridad de la organización e incorporados al presupuesto anual de la organización; se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.

410-04 Políticas y procedimientos.- La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran. Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información. Será necesario establecer procedimientos de comunicación, difusión

y coordinación entre las funciones de tecnología de información y las funciones propias de la organización. Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos. Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos. La unidad de tecnología de información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.

410-05 Modelo de información organizacional.- La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes. El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentado de forma permanente, incluirá las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente. Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad.

410-06 Administración de proyectos tecnológicos.- La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

- Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.
- Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.
- La formulación de los proyectos considerará el Costo Total de Propiedad CTP; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.
- Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o

líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.

- Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.
- El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.
- Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.
- Se deberá monitorear y ejercer el control permanente de los avances del proyecto.
- Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.
- El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

410-07 Desarrollo y adquisición de software aplicativo.- La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

- La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.
- Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.
- Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.
- Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

- En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la organización.
- En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.
- En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.
- La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.
- Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.
- Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.
- Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.

410-8 Adquisiciones de infraestructura tecnológica.- La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

- Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.
- La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.
- En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.
- Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante.

410-9 Mantenimiento y control de la infraestructura tecnológica.- La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.

Los temas a considerar son:

- Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.
- Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e

informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.

- Control y registro de las versiones del software que ingresa a producción.
- Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
- Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.
- Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
- Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.
- El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

410-10 Seguridad de tecnología de información.- La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

Para ello se aplicarán al menos las siguientes medidas:

- Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;
- Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;
- En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.
- Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;
- Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.

- Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;
- Consideración y disposición de sitios de procesamiento alternativos.
- Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

410-11 Plan de contingencias.- Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Los aspectos a considerar son:

- Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.
- Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.
- Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en una data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.
- Plan de recuperación de desastres que comprenderá:
 - ✓ Actividades previas al desastre (bitácora de operaciones)
 - ✓ Actividades durante el desastre (plan de emergencias, entrenamiento)
 - ✓ Actividades después del desastre.
- Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.
- El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.
- El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o

cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

410-12 Administración de soporte de tecnología de información.- La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

Los aspectos a considerar son:

- Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
- Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.
- Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.
- Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.
- Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.
- Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.
- Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.
- Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.
- Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.
- Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

- Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

410-13 Monitoreo y evaluación de los procesos y servicios.- Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran. La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos. La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

410-14 Sitio web, servicios de internet e intranet.- Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

410-15 Capacitación informática.- Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano.



Razón Social COMPANIA DE SERVICIOS GENERALES SILVA RODAS SERVISILVA CIA. LTDA.	Número RUC 1791293878001
---	------------------------------------

Representante legal
• GALETH SILVA ANA GISSELA

Estado ACTIVO	Régimen REGIMEN GENERAL
-------------------------	-----------------------------------

Inicio de actividades 04/07/1995	Reinicio de actividades No registra	Cese de actividades No registra
--	---	---

Fecha de constitución
04/07/1995

Jurisdicción ZONA 2 / ORELLANA / ORELLANA	Obligado a llevar contabilidad SI
---	---

Tipo SOCIEDADES	Agente de retención SI
---------------------------	----------------------------------

Domicilio tributario

Ubicación geográfica

Provincia: ORELLANA **Cantón:** ORELLANA **Parroquia:** NUEVO PARAÍSO (CAB. EN UNIÓN CHIMBORAZO)

Dirección

Calle: VIA LAGO AGRIO **Número:** S/N **Intersección:** SECUNDARIA **Carretera:** MARGEN IZQUIERDO **Kilómetro:** 7 1/2 **Número de piso:** 0 **Referencia:** A CUATROCIENTOS METROS DE LA COMPAÑIA METROLOGIC

Actividades económicas

• C13130301 - SERVICIO DE IMPERMEABILIZADO, REVESTIMIENTO, CAUCHUTADO O IMPREGNACIÓN DE PRENDAS REALIZADO POR TERCEROS A CAMBIO DE UNA RETRIBUCIÓN O POR CONTRATO.

Establecimientos

Abiertos 2	Cerrados 0
----------------------	----------------------

Obligaciones tributarias

- ANEXO TRANSACCIONAL SIMPLIFICADO
- ANEXO ACCIONISTAS, PARTÍCIPES, SOCIOS, MIEMBROS DEL DIRECTORIO Y ADMINISTRADORES – ANUAL
- 1031 - DECLARACIÓN DE RETENCIONES EN LA FUENTE
- ANEXO DE DIVIDENDOS, UTILIDADES O BENEFICIOS - ADI
- 1021 - DECLARACIÓN DE IMPUESTO A LA RENTA SOCIEDADES
- ANEXO RELACIÓN DEPENDENCIA

Razón Social
COMPANIA DE SERVICIOS GENERALES
SILVA RODAS SERVISILVA CIA. LTDA.

Número RUC
1791293878001

- 4150 CONTRIBUCION UNICA Y TEMPORAL PARA SOCIEDADES CON INGRESOS MAYORES O IGUALES A USD 1 MILLON
- 2011 DECLARACION DE IVA

i Las obligaciones tributarias reflejadas en este documento están sujetas a cambios. Revise periódicamente sus obligaciones tributarias en www.sri.gob.ec.

Números del RUC anteriores

No registra



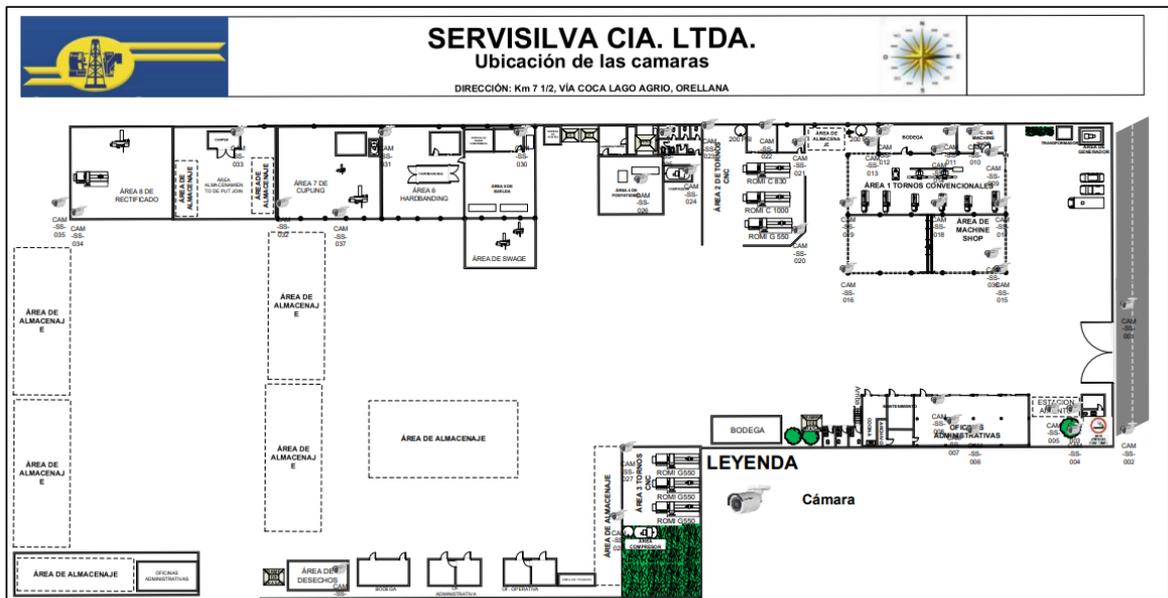
Código de verificación: CATRCR2021002115641
Fecha y hora de emisión: 13 de septiembre de 2021 08:03
Dirección IP: 190.110.222.148

Validez del certificado: El presente certificado es válido de conformidad a lo establecido en la Resolución No. NAC-DGERCGC15-00000217, publicada en el Tercer Suplemento del Registro Oficial 462 del 19 de marzo de 2015, por lo que no requiere sello ni firma por parte de la Administración Tributaria, mismo que lo puede verificar en la página transaccional SRI en línea y/o en la aplicación SRI Móvil.

ANEXO C: FICHA MANTENIMIENTO CORRECTIVO A COBERTURA DE RED

 TicketSoft		Ecuador, Orellana, 20-12-2021	
Ticket N° : 220		Creado por: Juan Molina Creado: 2020-07-15 22:52:05	
PROBLEMA: Sistema con problemas			
CLIENTE NOMBRE: Juan Molina CORREO: jmolina@servsilva.com TELEFONO: 062378060 CELULAR: 0967001659		TECNICO NOMBRE: Felipe Varela FECHA ASIG: 17-07-2020 19:37:54 TIPO REQ: Requerimiento de Hardware ESTADO: ATENDIDO	
AREA: CNC COMPUTARIZADO			
Horario	Descripción	Fecha Terminado	
08:00AM - 12:00PM	problemas con el internet en fosfatizado y integracion de switch de cnc	29-07-2020 21:22:52	
EMPRESA: Servsilva			
COMENTARIO			
se reparo la linea de internet desde machine shop hasta suelda con exito!			

ANEXO D: CÁMARAS DE SEGURIDAD



Elaborado Por: Mgs. Klever Montes.

Aprobado Por: Mgs. Ana Galeth Silva.

ANEXO E: FICHA DE INVENTARIO



TicketSoft

Ticket Nº : 238

Ecuador, Orellana, 31-12-2020

Creado por: Juan Molina
Creado: 2020-12-28 07:19:28

ENTREGA DE EQUIPO A PERSONA

PERSONA	TECNICO
NOMBRE: Samanta Urgiles CORREO: samy201430@hotmail.com RUC/CEDULA: 2200156392 EMPRESA: Servisilva	NOMBRE: Juan Molina CORREO: jmolina@servisilva.com
AREA: Contabilidad	

Equipo	Cantidad	Fecha de Entrega
 Mouse Pad-PAD	1	2020-12-28 07:19:28

EMPRESA: Servisilva
 NUEVO USADO

COMENTARIO


 Firma

jmolina@servisilva.com
https://www.servisilva.com/

ANEXO F: POLÍTICAS DE SEGURIDAD INFORMÁTICAS

 <p style="margin-top: 20px;">POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI) Servisilva Cia. Ltda.</p>	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">CONTENIDO</th> <th style="text-align: right;">Pág.</th> </tr> </thead> <tbody> <tr> <td>INTRODUCCIÓN.....</td> <td style="text-align: right;">3</td> </tr> <tr> <td>1. GENERALIDADES.....</td> <td style="text-align: right;">4</td> </tr> <tr> <td>2. POLÍTICAS DE SEGURIDAD INFORMÁTICA.....</td> <td style="text-align: right;">5</td> </tr> <tr> <td> 2.1. DEFINICIÓN.....</td> <td style="text-align: right;">5</td> </tr> <tr> <td> 2.2. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA.....</td> <td style="text-align: right;">5</td> </tr> <tr> <td> 2.3. PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD.....</td> <td style="text-align: right;">6</td> </tr> <tr> <td> 2.4. PLAN DE TRABAJO PARA ESTABLECER POLÍTICAS DE SEGURIDAD.....</td> <td style="text-align: right;">7</td> </tr> <tr> <td> 2.5. RECOMENDACIONES PARA IMPLANTAR LAS POLÍTICAS.....</td> <td style="text-align: right;">8</td> </tr> <tr> <td>3. PRIVACIDAD EN LA RED Y CONTROL DE INTRUSOS.....</td> <td style="text-align: right;">8</td> </tr> <tr> <td> 3.1. Privacidad en la Red.....</td> <td style="text-align: right;">8</td> </tr> <tr> <td> 3.1.1. Generalidades.....</td> <td style="text-align: right;">8</td> </tr> <tr> <td> 3.2. DEFINICIÓN DE PRIVACIDAD DE LAS REDES.....</td> <td style="text-align: right;">9</td> </tr> <tr> <td> 3.3. REQUISITOS PARA MANTENER LA PRIVACIDAD DE LAS REDES.....</td> <td style="text-align: right;">9</td> </tr> <tr> <td> 3.4. RIESGOS O AMENAZAS A LA PRIVACIDAD DE LAS REDES.....</td> <td style="text-align: right;">10</td> </tr> <tr> <td>4. NORMAS Y PROCEDIMIENTOS.....</td> <td style="text-align: right;">13</td> </tr> <tr> <td> 4.1. Reglamento Interno.....</td> <td style="text-align: right;">13</td> </tr> <tr> <td> 4.2. Procedimientos.....</td> <td style="text-align: right;">13</td> </tr> <tr> <td> 4.2.1. Solicitud de Proceso.....</td> <td style="text-align: right;">14</td> </tr> <tr> <td> 4.2.2. Orden de Trabajo.....</td> <td style="text-align: right;">14</td> </tr> <tr> <td> 4.2.3. Orden de Movilización.....</td> <td style="text-align: right;">14</td> </tr> <tr> <td> 4.2.4. Seguridad.....</td> <td style="text-align: right;">14</td> </tr> <tr> <td>5. FUNCIONES DEL DEPARTAMENTO.....</td> <td style="text-align: right;">15</td> </tr> <tr> <td> 5.1. Principales funciones y servicios que ofrece.....</td> <td style="text-align: right;">15</td> </tr> <tr> <td>6. METAS Y OBJETIVOS.....</td> <td style="text-align: right;">16</td> </tr> <tr> <td>7. CONCLUSIONES.....</td> <td style="text-align: right;">17</td> </tr> <tr> <td>8. BIBLIOGRAFIA.....</td> <td style="text-align: right;">18</td> </tr> </tbody> </table>	CONTENIDO	Pág.	INTRODUCCIÓN.....	3	1. GENERALIDADES.....	4	2. POLÍTICAS DE SEGURIDAD INFORMÁTICA.....	5	2.1. DEFINICIÓN.....	5	2.2. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA.....	5	2.3. PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD.....	6	2.4. PLAN DE TRABAJO PARA ESTABLECER POLÍTICAS DE SEGURIDAD.....	7	2.5. RECOMENDACIONES PARA IMPLANTAR LAS POLÍTICAS.....	8	3. PRIVACIDAD EN LA RED Y CONTROL DE INTRUSOS.....	8	3.1. Privacidad en la Red.....	8	3.1.1. Generalidades.....	8	3.2. DEFINICIÓN DE PRIVACIDAD DE LAS REDES.....	9	3.3. REQUISITOS PARA MANTENER LA PRIVACIDAD DE LAS REDES.....	9	3.4. RIESGOS O AMENAZAS A LA PRIVACIDAD DE LAS REDES.....	10	4. NORMAS Y PROCEDIMIENTOS.....	13	4.1. Reglamento Interno.....	13	4.2. Procedimientos.....	13	4.2.1. Solicitud de Proceso.....	14	4.2.2. Orden de Trabajo.....	14	4.2.3. Orden de Movilización.....	14	4.2.4. Seguridad.....	14	5. FUNCIONES DEL DEPARTAMENTO.....	15	5.1. Principales funciones y servicios que ofrece.....	15	6. METAS Y OBJETIVOS.....	16	7. CONCLUSIONES.....	17	8. BIBLIOGRAFIA.....	18
CONTENIDO	Pág.																																																						
INTRODUCCIÓN.....	3																																																						
1. GENERALIDADES.....	4																																																						
2. POLÍTICAS DE SEGURIDAD INFORMÁTICA.....	5																																																						
2.1. DEFINICIÓN.....	5																																																						
2.2. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA.....	5																																																						
2.3. PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD.....	6																																																						
2.4. PLAN DE TRABAJO PARA ESTABLECER POLÍTICAS DE SEGURIDAD.....	7																																																						
2.5. RECOMENDACIONES PARA IMPLANTAR LAS POLÍTICAS.....	8																																																						
3. PRIVACIDAD EN LA RED Y CONTROL DE INTRUSOS.....	8																																																						
3.1. Privacidad en la Red.....	8																																																						
3.1.1. Generalidades.....	8																																																						
3.2. DEFINICIÓN DE PRIVACIDAD DE LAS REDES.....	9																																																						
3.3. REQUISITOS PARA MANTENER LA PRIVACIDAD DE LAS REDES.....	9																																																						
3.4. RIESGOS O AMENAZAS A LA PRIVACIDAD DE LAS REDES.....	10																																																						
4. NORMAS Y PROCEDIMIENTOS.....	13																																																						
4.1. Reglamento Interno.....	13																																																						
4.2. Procedimientos.....	13																																																						
4.2.1. Solicitud de Proceso.....	14																																																						
4.2.2. Orden de Trabajo.....	14																																																						
4.2.3. Orden de Movilización.....	14																																																						
4.2.4. Seguridad.....	14																																																						
5. FUNCIONES DEL DEPARTAMENTO.....	15																																																						
5.1. Principales funciones y servicios que ofrece.....	15																																																						
6. METAS Y OBJETIVOS.....	16																																																						
7. CONCLUSIONES.....	17																																																						
8. BIBLIOGRAFIA.....	18																																																						

ANEXO G: ETIQUETAS DE RESPALDOS DE BASE DE DATOS POR ÁREA

Etiquetas de respaldos fechas y servidores				
23-02-2021 SocSe-ver	27-07-2021 Co Labd-Tercera	11-03-2021 Orma Marista	24-03-2021 Francisco Galdeh	27-10-2021 Luis 29.02.21
21-02-2021 Correas Marich	12-03-2021 Erika Imbag	26-02-2021 Erika Imbag	08-06-2021 Luis 29.02.21	29-05-2021 Luis 29.02.21
20-05-2021 Marcela Rivas	03-07-2021 Mercedes C.	20-02-2021 Sancanta U.	14-03-2021 Yadira Herrera	01-10-2019 Respaldos-2019
18-12-2018 Respaldos-SocSe	03-01-2018 Félix Principal	26-08-2019 Programas SocSe	09-09-2019 Respaldos SocSe	21-12-2017 Respaldos SocSe
01-10-2018 Respaldos PC'S	03-01-2018 Respaldos Financ	18-07-2018 Respaldos C. Celis	15-05-2017 Respaldos SocSe	20-12-2017 Respaldos SocSe
11-09-2019 Respaldos SocSe	05-01-2018 Toshiba Data	25-01-2018 Video-Program	09-09-2020 USB SocSe	11-09-2019 Respaldos SocSe
09-09-2020 Respaldos Yovani	09-09-2020 Respaldos Yovani	13-09-2019 Respaldos Financ	25-12-2017 Respaldos SocSe	02-09-2019 Respaldos SocSe
09-09-2020 Kevin Galdeh	09-09-2020 Financ 2020	09-09-2020 Respaldos Digital	26-10-2020 Respaldos SocSe	09-09-2020 Respaldos Galdeh
20-02-2020 Respaldos Alex G.	22-04-2020 Respaldos SocSe	09-09-2020 Data Ortega	09-10-2020 Resp. Montalvo	01-02-2020 Respaldos SocSe
21-01-2020 Respaldos R. Rivas	23-02-2021 Respaldos R. Rivas			