UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA

AUDITORÍA INFORMÁTICA A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN A "YERAY ELECTRODOMÉSTICOS"

AUTOR

ANDRADE FARIAS DAVID AGUSTIN

TUTOR

A.S MINAYA MACIAS RENELMO WLADIMIR, MG.

EL CARMEN, AGOSTO 2024

Uleam

CERTIFICACIÓN DEL TUTOR

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor de la Extensión El Carmen, de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de investigación, bajo la autoría del estudiante **ANDRADE FARIAS DAVID AGUSTÍN**, legalmente matriculado en la carrera de Tecnologías de la Información, período académico 2023(2)-2024(1), cumpliendo el total de 384 horas, bajo la opción de titulación de trabajo de Investigación, cuyo tema del proyecto es "Auditoría Informática a la Gestión de Seguridad de la Información a "Yeray Electrodomésticos"".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 26 de Julio del 2024.

Lo certifico,

Wladimir Minaya Macías, Mg.
Docente Tutor
Área: Sistemas

Uleam
Extensión El Carmen

TRIBUNAL DE SUSTENTACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con modalidad Proyecto Integrador, titulado: AUDITORÍA INFORMÁTICA A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN A "YERAY ELECTRODOMÉSTICOS" cuya autoría es del señor: Andrade Farías David Agustín estudiante de la Carrera de Ingeniería en Tecnologías de la información, y como Tutor de Trabajo de Titulación al A.S Minaya Macías Renelmo Wladimir, Mg.

Para constancia firman.

Ing. Clara Pozo Hernández. Mg
Presidente de tribunal

A.S Wladimir Minaya Macías.Mg
Docente tutor

Ing. Bladimir Mora Marcillo.Mg
Primer miembro del tribunal

Ing. Rocio Mendoza Villamar.Mg
Segundo miembro del tribunal

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, con el siguiente tema: AUDITORÍA INFORMÁTICA A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN A "YERAY ELECTRODOMÉSTICOS", corresponde exclusivamente a: Andrade Farias David Agustín con cédula de ciudadanía N° 1312257015, y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí

Andrade Farias David Agustín
C.C 1312257015

DEDICATORIA

Dedico este trabajo de investigación a mi amada familia, cuyo apoyo incondicional y comprensión han sido mi mayor fortaleza durante este arduo proceso. Agradezco profundamente a mis respetados docentes, cuya dedicación y sabiduría han guiado mi camino académico y enriquecido mi aprendizaje. Asimismo, dedico este trabajo a la academia en general, como una contribución modesta hacia el avance del conocimiento en el campo de la seguridad informática. Que este trabajo sirva como un faro para las nuevas generaciones, inspirándolas y guiándolas en su camino hacia el descubrimiento y la innovación en este apasionante campo del saber.

Andrade Farías David Agustín

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a Dios, quien me ha otorgado la vida y la sabiduría para llevar a cabo este proyecto de investigación. A mis amados hijos, esposa, padres y demás familiares, les agradezco de todo corazón por su constante apoyo, aliento y amor incondicional, que han sido el motor que me impulsó a alcanzar este sueño y lograr el título profesional. También extiendo mi gratitud a todas las personas que han sido parte importante de este proceso. Gracias a todos por creer en mí y acompañarme en este viaje hacia mis metas.

Andrade Farías David Agustín

ÍNDICE GENERAL

PORTADA I

CERTIFICACIÓN DEL TUTOR II

TRIBUNAL DE SUSTENTACIÓN ..... **¡Error! Marcador no definido.**

DECLARACIÓN DE AUTORÍA IV

DEDICATORIA V

AGRADECIMIENTO VI

ÍNDICE GENERAL VII

ÍNDICE DE TABLAS XIV

ÍNDICE DE ILUSTRACIONES XV

ÍNDICE DE ANEXOS XVI

RESUMEN XVII

ABSTRACT XVIII

CAPÍTULO I 1

1 INTRODUCCIÓN 1

1.1 Introducción 1

1.2 Presentación del tema 2

1.3 Ubicación y contextualización de la problemática 2

1.4 Planteamiento del problema 3

1.4.1 Problematización 3

1.4.2 Génesis del problema 4

1.4.3 Estado actual del problema 4
1.5 Diagrama causa – efecto del problema 5
1.6 Objetivos 6
1.6.1 Objetivo general 6
1.6.2 Objetivos específicos 6
1.7 Justificación 6
1.8 Impactos esperados 7
1.8.1 Impacto tecnológico 7
1.8.2 Impacto social 7
1.8.3 Impacto ecológico 8
CAPÍTULO II 9
2 MARCO TEÓRICO 9
2.1 Antecedentes históricos 9
2.2 Antecedentes de investigaciones relacionadas al tema presentado 10
2.3 Definiciones conceptuales 12
2.3.1 Auditoría informática 12
2.3.1.1 De los orígenes de la auditoría 12
2.3.1.2 Código deontológico de la función de auditoría 12
2.3.1.3 Criterios por seguir para la composición del equipo auditor 13
2.3.1.4 Relación de los distintos tipos de auditoría en el marco de los sistemas de información 13
2.3.1.5 Tipos de pruebas a realizar en el marco de una auditoría 13

2.3.1.6 Tipos de muestreo a aplicar durante el proceso de auditoría 14

2.3.1.7 Identificación y evaluación de riesgos de auditoría 14

2.3.1.8 Fases generales de una auditoría 15

2.3.1.9 Explicación de los requerimientos que deben cumplir los hallazgos de auditoría 15

2.3.1.10 El informe de auditoría 16

2.3.2 Gestión de seguridad 16

2.3.2.1 Incidentes de seguridad 16

2.3.2.2 Respuesta ante incidentes de seguridad 17

2.3.2.3 Políticas de seguridad 17

2.3.2.4 Gestión de incidentes de seguridad 17

2.3.2.5 La gestión del riesgo 18

2.3.2.6 Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención 18

2.3.2.7 La seguridad en los elementos físicos existentes en una red 19

2.3.2.8 El problema de la seguridad en la conexión a internet 19

2.3.2.9 Seguridad de la información (ISO 27001) 19

2.3.2.10 Planes de cumplimiento normativo 20

2.4 Conclusiones del marco teórico 20

CAPÍTULO III 21

3 MARCO INVESTIGATIVO 21

3.1 Introducción 21

3.2 Tipo de investigación 21
3.2.1 Investigación documental 21
3.2.2 Investigación de campo 22
3.2.3 Investigación explicativa 22
3.3 Métodos de investigación 23
3.3.1 Método analítico-sintético 23
3.3.2 Método deductivo 23
3.4 Fuentes de información de datos 24
3.4.1 Encuesta 24
3.4.2 Entrevista 24
3.5 Estrategia operacional para la recolección de datos 25
3.5.1 Población y muestra 25
3.5.1.1 Población 25
3.5.1.2 Muestra 26
3.5.2 Análisis de las herramientas de recolección de datos a utilizar 26
3.5.2.1 Encuesta 26
3.5.2.2 Entrevista 28
3.5.2.3 Encuesta dirigida a clientes de la organización 29
3.5.2.4 Estructura de los instrumentos de recolección de datos aplicados 31
3.5.3 Plan de recolección de datos 31
3.6 Análisis y presentación de resultados 32

3.6.1 Análisis de encuesta dirigida a los empleados de Electrodomésticos Yeray.....32

3.6.2 Análisis de encuesta aplicada a clientes de Yeray electrodomésticos 36

3.6.3 Análisis de entrevista aplicada al gerente y secretaria de Yeray Electrodomésticos 38

3.6.4 Presentación y descripción de los resultados obtenidos 40

3.6.5 Informe final del análisis de los datos.....41

CAPÍTULO IV.....42

4 MARCO PROPOSITIVO 42

4.1 Introducción 42

4.2 Descripción de la propuesta 42

4.3 Determinación de recursos 43

4.3.1 Humanos 43

4.3.2 Tecnológicos.....43

4.3.3 Económicos.....43

4.4 Información de la institución.....43

4.4.1 Reseña histórica de la institución.....43

4.4.2 Misión 44

4.4.3 Visión.....44

4.4.4 Organigrama institucional.....45

4.5 Etapas de acción para el desarrollo de la propuesta (auditoría) 45

4.5.1 Planificar.....45

4.5.1.1 Programa de auditoría.....45

4.5.2 ISO 27001 46
4.5.3 Fases de la Norma ISO 27001 47
4.5.4 Fase 1 Auditoria Inicial ISO 27001 47
4.5.5 Análisis de brechas GAP 48
4.5.6 Requisitos evaluados 48
4.5.7 Instrumento para evaluación de requisitos 49
4.5.8 Instrumentos para evaluación de cumplimiento de controles 50
4.5.9 Hacer 50
4.5.9.1 Aplicación 50
4.5.9.2 TABULACIÓN DE DATOS 54
4.5.9.3 ANALISIS DE RESULTADOS 54
CAPÍTULO V 57
5 INTRODUCCIÓN 57
5.1 EVALUACIÓ DE RESULTADOS 57
5.2 Informe final de auditoría 57
5.2.1 Dirigido a 57
5.2.2 Motivo 57
5.2.3 Objetivo 57
5.2.4 Alcance 58
5.2.5 Personal involucrado 58
5.2.6 Hallazgos 58

5.2.6.1 Nivel de madurez por el cumplimiento de los requisitos de la ISO 27001 58

5.2.6.2 Cumplimiento de controles establecidos por la ISO 27001 63

5.2.7 Opinión 70

5.2.7.1 Estado del cumplimiento de los requisitos establecidos por ISO 27001 para la seguridad de la información en Yeray Electrodomésticos.....70

5.2.7.2 Cumplimiento de controles de seguridad establecidos por la ISO 27001 para una buena gestión de seguridad de la información en Yeray Electrodomésticos 70

5.2.8 Conclusiones y recomendaciones de auditoría 71

5.2.8.1 Conclusiones.....71

5.2.8.2 Recomendaciones 71

CAPÍTULO VI.....72

6 CONCLUSIONES Y RECOMENDACIONES.....72

6.1 Conclusiones 72

6.2 Recomendaciones.....73

7 REFERENCIAS BIBLIOGRÁFICAS.....74

ANEXOS 77

ÍNDICE DE TABLAS

Tabla 1. Plan de recolección de datos 32
Tabla 2. Análisis encuesta empleados 36
Tabla 3. Análisis encuesta clientes 38
Tabla 4. Análisis de entrevistas 39
Tabla 5. Recursos tecnológicos 43
Tabla 6. Recursos económicos 43
Tabla 7. Requisitos evaluados 49
Tabla 8. Instrumento de requisitos evaluados 49
Tabla 9. Instrumento cumplimiento de controles 50
Tabla 10. Escala de evaluación cumplimiento de requisitos. 52
Tabla 11. Rangos de estado del cumplimiento 53
Tabla 12. Resumen resultados nivel de madurez 55
Tabla 13. Resumen cumplimiento de controles. 56
Tabla 14. Personal involucrado 58

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Ubicación empresa Yeray 3
Ilustración 2. Organigrama empresarial 45
Ilustración 3. Fases ISO 27001 47
Ilustración 4. Entrevista de evaluación de controles 51
Ilustración 5. Tabulación información auditoría inicial 52
Ilustración 6. Tabulación de datos auditoría 53
Ilustración 7. Matriz de tabulación de datos 54
Ilustración 8. Resultados cumplimiento de requisitos 59
Ilustración 9.Resultados total controles evaluados. 63

ÍNDICE DE ANEXOS

Anexo A. Reporte anti-plagio Urkund 77
Anexo B. Fotografías 78
Anexo C. Aplicación de entrevistas 79
Anexo D. Manual de Políticas de buenas prácticas para la Gestión de Seguridad 80

RESUMEN

La investigación se originó en el contexto actual, donde la protección de la información se ha convertido en un activo invaluable para las organizaciones. Se establecieron objetivos para evaluar el cumplimiento de requisitos, la brecha GAP y los controles de seguridad en Repuestos y Electrodomésticos Yeray. Este análisis incluyó recorridos por las instalaciones, entrevistas con administradores responsables de la gestión de la información y encuestas a empleados y clientes.

A través de estas actividades, se obtuvo un diagnóstico sobre la forma en que la organización manejaba la información y protegía sus recursos. El proyecto de auditoría informática se fundamentó en la metodología y los formularios proporcionados por la norma ISO 27001, un estándar internacional para la implementación, gestión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).

Los resultados de los Checklist revelaron que Yeray Electrodomésticos tenía un cumplimiento de requisitos de seguridad del 37%, con una brecha GAP del 63%. Además, se identificó un incumplimiento del 63% en la evaluación de los controles de seguridad. Estos hallazgos destacaron un estado preocupante de vulnerabilidad en la empresa, lo que la hacía susceptible a riesgos de seguridad informática. Bajo estos hallazgos se recomendó la implementación de un Manual de Políticas de Buenas Prácticas para abordar las deficiencias encontradas y fortalecer las medidas existentes para proteger la información.

ABSTRACT

The research originated in the current context, where the protection of information has become an invaluable asset for organizations. Objectives were established to evaluate compliance with requirements, the GAP analysis, and security controls at Repuestos y Electrodomésticos Yeray. This analysis included walkthroughs of the facilities, interviews with administrators responsible for information management, and surveys of employees and customers.

Through these activities, a diagnosis was obtained regarding how the organization managed information and protected its resources. The IT audit project was based on the methodology and forms provided by ISO 27001, an international standard for implementing, managing, maintaining, and improving an Information Security Management System (ISMS).

The results of the checklists revealed that Yeray Electrodomésticos had a 37% compliance rate with security requirements, with a 63% GAP. Additionally, a 63% non-compliance was identified in the evaluation of security controls. These findings highlighted a concerning state of vulnerability in the company, making it susceptible to cybersecurity risks. Based on these findings, the implementation of a Manual of Good Practice Policies was recommended to address identified deficiencies and strengthen existing measures to protect information.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Introducción

En la era actual, la información se ha convertido en uno de los activos más valiosos para las organizaciones, siendo esencial para su operación y toma de decisiones. Paralelamente, las herramientas tecnológicas continúan evolucionando, proporcionando mecanismos avanzados para la manipulación y gestión de datos. Esta tendencia ha generado no solo mejoras significativas en múltiples sectores, sino también un aumento en la exposición a vulnerabilidades que pueden comprometer la seguridad de la información.

Esta investigación se centra en analizar y evaluar el cumplimiento de la norma ISO 27001 en Yeray Electrodomésticos, con el objetivo de asegurar prácticas efectivas en la gestión de la seguridad de la información. El propósito es mitigar riesgos y garantizar la integridad de los datos en un entorno donde la información se ha convertido en un activo crucial para las organizaciones.

El trabajo está compuesto por seis capítulos, cada uno abordando aspectos fundamentales del proyecto. El primer capítulo presenta la problematización, analizando las causas y efectos que motivan este estudio. En el segundo capítulo, se desarrolla el soporte teórico basado en publicaciones recientes de autores con no más de cinco años de antigüedad, lo cual garantiza un respaldo científico actualizado para la investigación. El tercer capítulo se enfoca en la metodología de investigación, describiendo las herramientas y tipos de investigación utilizados para llevar a cabo el estudio de manera efectiva.

En el cuarto capítulo, se expone la propuesta de solución, orientada a resolver la problemática identificada inicialmente. Posteriormente, el quinto capítulo presenta un análisis de los resultados obtenidos, con especial énfasis en la evaluación de la seguridad en Yeray Electrodomésticos. Finalmente, el sexto capítulo incluye un manual de políticas destinado a la implementación de mejoras, junto con los anexos pertinentes que complementan el proyecto.

1.2 Presentación del tema

Auditoría informática a la gestión de seguridad de la información a "Yeray electrodomésticos"

1.3 Ubicación y contextualización de la problemática

La empresa Yeray Electrodomésticos es una compañía que surge desde el 25 de octubre del año 2011 ubicada en la provincia de Santo Domingo de los Tsáchilas, ciudad de Santo Domingo de los Colorados, en la avenida Tsáfiqui 140 y Augusto Gachet, dedicada a la actividad comercial de venta al por mayor y menor de electrodomésticos en establecimientos especializados: en línea blanca y café.

Comenzó sus actividades con un numero de 34 trabajadores en distintas áreas funcionales con lo cual se abrió espacio en el mercado comercial, actualmente cuenta con 29 colaboradores que desempeñan funciones en distintas áreas las cuales van desde agentes de ventas, despachadores, personal de servicio técnico, secretaria y cajera.

Como una compañía dinámica en el ámbito comercial, con un alto grado de actividad económica, genera, procesa y distribuye una gran cantidad de información. Debido a la naturaleza financiera de estas actividades, su manejo requiere de especial cautela. Sin embargo, se ha detectado una reiterada inconsistencia de datos al comparar la información de los productos que se registran en la base de datos con la realidad física y cuantitativa en los almacenes. Este desajuste provoca problemas y discrepancias al realizar despachos de mercadería y subsiguientes informes acerca del inventario remanente en los almacenes.

Ilustración 1. Ubicación empresa Yeray

1.4 Planteamiento del problema

1.4.1 Problematización

La problemática específica que enfrenta se centra en una falta de precisión y consistencia en la gestión de información. Las discrepancias evidentes entre los datos almacenados en la base de datos corporativa y el inventario real de las bodegas indican un problema crítico de concordancia. Este desfase en los registros plantea serios obstáculos para una operación eficiente y confiable, dificultando la planificación precisa del inventario y la toma de decisiones basada en datos.

Dada la situación descrita anteriormente, la empresa enfrenta posibles riesgos de pérdida de información, lo cual puede resultar en una disminución de la competitividad. Esta eventualidad podría precipitar desequilibrios económicos, con posibles consecuencias tales

como reducción de personal y disminución de las actividades comerciales. Es crucial, por tanto, que la información generada y procesada en todos los ámbitos de la organización sea coherente y uniforme, garantizando la estabilidad y sostenibilidad de su operación comercial.

1.4.2 Génesis del problema

Este problema remonta a hace unos 8 años, cuando la empresa comenzó a digitalizar la gestión de información tras adquirir e implementar el software de facturación y control de productos PEGASUS. La motivación para esta adquisición fue mantenerse a la vanguardia de las nuevas tecnologías y agilizar los procesos internos de la compañía. Sin embargo, desde su implementación, se ha observado una discordancia persistente entre la información registrada en la base de datos del software y los inventarios físicos de los almacenes, creando un problema de consistencia de datos que persiste hasta los tiempos actuales.

1.4.3 Estado actual del problema

Existe un desafío crítico debido a la discrepancia existente entre la información almacenada en la base de datos y el inventario físico presente en los almacenes. Esta incongruencia se origina de varias fuentes, como errores humanos en la introducción de datos, potenciales fallos en los equipos informáticos, deficiencias en la gestión del inventario y la pérdida o robo de productos no reflejados en el sistema. Este conjunto de factores desencadena una serie de efectos negativos en la operación.

El desequilibrio en la información fomenta la toma de decisiones operativas erróneas, lo que, a su vez, limita las oportunidades de negocio y propicia un aumento en la ineficiencia. Adicionalmente, si la situación se hace pública, la reputación se vería amenazada, lo que podría deteriorar las relaciones con clientes y proveedores.

Por ende, es imperativo abordar este problema para preservar la integridad, efectividad y rentabilidad de las operaciones comerciales. La solución a este desafío no solo optimizará el rendimiento, sino que también fortalecerá la posición competitiva en el mercado.

1.5 Diagrama causa – efecto del problema

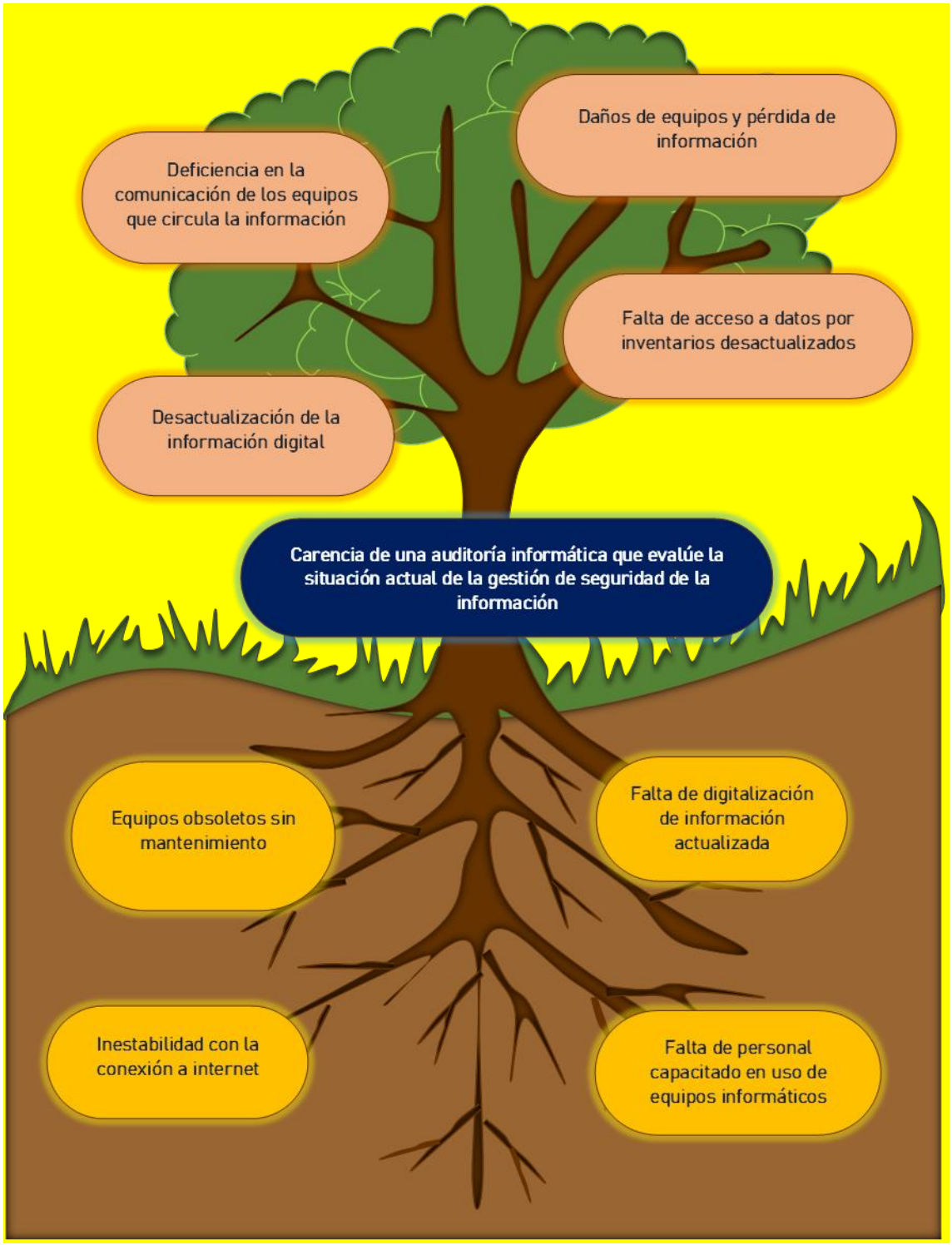


Ilustración 2. Árbol de problemas

1.6 Objetivos

1.6.1 Objetivo general

Efectuar una auditoría informática sobre la gestión de seguridad de la información en "Yeray Electrodomésticos"

1.6.2 Objetivos específicos

- Conocer mediante un análisis exhaustivo el estado actual de la organización, identificando las problemáticas subyacentes que orientarán y definirán el enfoque de la investigación técnica.
- Realizar el soporte teórico de la investigación profunda sobre libros que fomenten al sustento de las variables que sostienen esta investigación las cuales son auditoría y gestión de seguridad.
- Ejecutar un estudio técnico-analítico sobre la gestión actual de la seguridad de la información en el almacén Yeray.
- Conducir una auditoría basada en la metodología de la norma ISO 27001 para evaluar las prácticas de gestión de seguridad de la información en la organización.
- Proponer, a partir de los resultados de la auditoría, la creación de una guía o manual de procedimientos destinado a optimizar los procesos en almacén Yeray.

1.7 Justificación

Una evaluación sistemática de la gestión de seguridad de la información puede exponer potenciales vulnerabilidades y lagunas en las medidas protectoras establecidas. Esta evaluación es un componente esencial para el diseño de una estrategia robusta de seguridad de la información, dado que resulta imperativo reconocer y comprender los riesgos inherentes a los activos informacionales para poder mitigarlos adecuadamente. Mediante la auditoría, la organización podrá diagnosticar áreas de mejora y, consecuentemente, optimizar sus protocolos de seguridad. Además, dicha evaluación permite una apreciación objetiva del rendimiento y eficacia de las políticas y controles de seguridad ya instaurados.

El objetivo principal de este proyecto es discernir cualquier desviación o incumplimiento con respecto a los estándares de seguridad de la información preestablecidos. Para "Yeray Electrodomésticos", garantizar la conformidad con estos estándares no solo es esencial para evitar sanciones regulatorias, sino también para preservar y fortalecer su reputación en el mercado, considerando que las repercusiones de no conformidad podrían acarrear costos

financieros y de reputación significativamente mayores que aquellos asociados a la implementación de mejoras en la seguridad.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

El uso eficiente de las herramientas tecnológicas actuales tiene un impacto significativo en cualquier organización. Es vital comprender y controlar los tipos de servicios disponibles, ya que estos son cruciales para el rendimiento y la gestión de dichas herramientas. El mantenimiento adecuado del hardware es un factor fundamental, ya que el estado físico de los equipos puede influir directamente en la ejecución de los sistemas de gestión de información.

Conocer e implementar los protocolos adecuados en situaciones de potencial vulnerabilidad de la información se convierte en un factor esencial para minimizar los riesgos y garantizar la integridad de los datos. Es necesario conocer y entender a profundidad los servicios asociados, un mantenimiento correcto del hardware y un manejo efectivo de las posibles amenazas a la seguridad de la información. Esta combinación de elementos contribuye a una gestión tecnológica más eficaz y segura, optimizando el rendimiento de la organización y reduciendo la posibilidad de pérdida o compromiso de los datos vitales.

1.8.2 Impacto social

La educación y formación en el uso de recursos tecnológicos, tanto físicos como digitales, en una organización es considerable y reviste varios aspectos técnicos esenciales. Al proporcionar a los usuarios potenciales un conocimiento adecuado de las tecnologías con las que la empresa cuenta, se fomentan hábitos de buenas prácticas, lo que contribuye a una gestión más eficiente de los sistemas y equipos disponibles y minimiza el riesgo de fallos derivados de errores humanos.

Realizar capacitación técnica sobre los sistemas de gestión de información puede optimizar y agilizar los procesos internos de la organización, al reducir los fallos actuales o las inconsistencias de información. Los miembros de la organización adquieren las habilidades necesarias para manipular de manera eficaz estos sistemas, lo que mejora la calidad del trabajo, aumenta la productividad y puede incluso favorecer la innovación. Al reducir las

inconsistencias y los fallos de información, la empresa puede mantener una comunicación más efectiva y precisa con sus socios comerciales, lo que a su vez puede aumentar la satisfacción y la confianza.

1.8.3 Impacto ecológico

El impacto ecológico de la investigación en cuestión es notable, especialmente en cuanto a la promoción de la sostenibilidad y la reducción de la huella ambiental. La eficiencia en el uso de los sistemas de gestión de información tiene la capacidad de reducir drásticamente el consumo de papel, contribuyendo así a la conservación de los recursos naturales necesarios para su producción y minimizando la deforestación y la contaminación resultante de su manufactura y desecho. El manejo adecuado de los equipos tecnológicos disponibles tiene el potencial de fortalecer la seguridad de la información generada y procesada dentro de la organización. Esta eficiencia no solo optimiza las operaciones, sino que también contribuye a reducir la generación de desechos electrónicos, que son notoriamente dañinos para el medio ambiente debido a su contenido de sustancias tóxicas y su complejidad para su disposición y reciclaje adecuado.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

Referirse a auditoria es mencionar un término tan antiguo como son los seres humanos, esto tuvo su aparición formal en el ámbito de la contabilidad siendo consciente de la evolución mundial en cuanto a temas de contabilidad económica por parte de las entidades financiera para llevar control de sus recursos y mantener seguridad de quienes los están gestionando. (Rivas, 1988)

Una vez en marcha la década de los 90 comenzó entre los profesionales que manejan información su interés por las auditorías sobre auditorías de la gestión de información, bajo estos antecedes se comienza a ser más llamativos los interese por cómo se da gestión a la información dentro de las organizaciones. Para llevar a cabo este tipo de prácticas fue necesario pasar por un transcurso largo de tiempo puesto que en el caso de la auditoría informática puesto que es una herramienta mediante la cual se analiza, evalúa y verifica que los sistemas de información dentro de las organizaciones estén cumpliendo con los objetivos planteados. (Comamala, 2015)

Aunque el termino de gestión de seguridad de la información sea algo reciente, posee historia que remonta a épocas lejanas un ejemplo es durante la guerra fría cuando las agencias de seguridad y defensa norteamericanas comenzaron a desarrollar técnicas para lograr un cifrado de información eficiente que resguarde la comunicación y por ende los datos que se transmitían.

Con el avance de las tecnologías lo hicieron de manera similar y con un incremento alarmante los riesgos de ciberataques y demás daños sofisticados, esto dio mayo impulso a concretar intereses por la forma de gestionar la seguridad dentro de las organizaciones. Actualmente existen herramientas y organizaciones dedicadas a brindar apoyo en cuanto a la gestión de seguridad de la información como lo son las Normas ISO concretamente en 2005 se lanzó la ISO 27001 que brinda un marco estandarizado para identificar, gestionar y minimizar los riesgos de seguridad de la información. (Castro, 2018)

2.2 Antecedentes de investigaciones relacionadas al tema presentado

Auditoría informática según la Norma ISO 27001 para mejorar la seguridad de la información en el Departamento de TIC del Centro de Investigación y Desarrollo FAE.

Este trabajo de investigación tuvo lugar en la ciudad de Ambato, Ecuador durante el año 2022 y tuvo como objetivo *"minimizar riesgos y brindar seguridad a la información que se maneja diariamente en el Departamento de Tics del Centro de Investigación y Desarrollo FAE"* para lo cual se aplicaron políticas de seguridad establecidas en la norma ISO 27001 que brinda un estándar sistemático para la gestión de seguridad de la información. Estuvo estructurado mediante los ciclos Deming metodología que consta de cuatro fases (Planear, Implementar, Verificar y Actuar) cada una de estas con tareas técnicas específicas que fueron desarrollando durante el proceso de investigación, la investigación tuvo como resultado la elaboración de un Plan de Seguridad de Información en el cual según el autor Remigio Chagmana se podrá "*definir el Alcance, Caracterización, Análisis de Riesgos y la Creación de nuevas Políticas de Seguridad de la Información*" con lo que se espera la organización auditada den cumplimiento para un mejor control de seguridad y detección rápida de posibles falencias. (Pomaquero, 2022)

Auditoría de seguridad informática en la Dirección Distrital 02D03 Chimbo-San Miguel-Educación, implementando el enfoque COBIT 5.0.

Este trabajo de investigación se desarrolló durante el periodo de gestión 2016-2017 dentro de la dirección Distrital 02D03 de Chimbo- San Miguel, basado en la metodología ABR Auditoría Basada en Riesgos e implementado en tres fases Planeación, Ejecución y comunicación de resultados sustentados por las bases teóricas de COBIT 5.0 Dentro de la ejecución se desarrolló una matriz de riesgos con la cual evaluar los procesos más críticos de la entidad y poder enfocar a ellos la evaluación de auditoría. Según Angel Palacios Bayas coautor de la investigación como resultados y basados en la matriz de riesgos aplicada para así *"calcular el riesgo inherente y riesgo residual, en base a los umbrales de riesgo, considerando las perspectivas de: Probabilidad e Impacto"* obteniendo los siguientes datos: **Probabilidad:** Posible (3), Probable (2) y Remota (1) - **Impacto:** Alto (3), Moderado (2) y Bajo (1) (Muñoz Vega, y otros, 2015), evidenciando falencias latentes que pueden estar

poniendo en riesgo la consecución de las actividades de la institución auditada. (Angel Palacios, 2018)

Marco de Gestión de la Seguridad de Datos para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001

María Pardo Cuenca desarrolló una investigación con el título "modelo de Gestión de Seguridad basado en la norma ISO 27001 en la Universidad Nacional de Loja" en la cual destaca a la información como el bien más importante en las organizaciones, para su estudio usó la metodología MAGERIT v3 que es una herramienta idónea para la gestión de riesgos que hayan sido identificados durante el análisis. El propósito de la investigación es la implementación de un Sistema de Gestión de Seguridad de la Información considerando la norma ISO 27001. El estudio concluyo con la elaboración de un Manual de Políticas de Seguridad de la Información, como una oportunidad para controlar y mitigar los riesgos que puedan estar atentando contra los activos de información de la institución objeto de estudio. (Cuenca., 2015)

Marco para la administración de la seguridad de la información y los riesgos vinculados a su utilización

La gestión de información en las instituciones es un tema de constante preocupación por la sensibilidad de los datos que se procesan por ello y con el fin de comprobar que tan efectivo es el proceso de gestión de seguridad de la información y los riesgos asociados a su uso, la Universidad Estatal Península Santa Elena desarrolló un modelo de gestión de seguridad para analizar las redes y computadoras. Al incorporar protocolos de seguridad tanto globales como locales, el modelo presenta una descripción general holística de las medidas de seguridad, ya sean digitales o físicas. Describe las acciones que se deben tomar en cada caso, simplificando el proceso de seguridad sin introducir métodos novedosos. Su foco está en la automatización, integración e integración, haciendo más eficiente la gestión de la seguridad de la información en las redes informáticas. Como resultado se lograr constatar que aplicando el modelo se logra automatizar procesos, operación de controles y revisión de estos, lo que se refleja en una efectividad proporcional del control de seguridad dentro de la gestión de seguridad de la información y los riesgos que presentan en su uso. (Luca, 2019)

2.3 Definiciones conceptuales

2.3.1 Auditoría informática

La auditoría informática es una práctica meticulosa y técnica destinada a sensibilizar a las organizaciones sobre los riesgos inherentes en sus procesos de manejo y tratamiento de la información digital. Esta revisión sistemática evalúa no solo la conformidad con normativas y estándares relevantes en materia de seguridad y administración de recursos tecnológicos, sino que también se asegura de que los sistemas de información estén optimizados para procesar y gestionar data crucial. Adicionalmente, esta auditoría garantiza la salvaguarda íntegra de la información, consolidándose como una herramienta esencial para el buen funcionamiento y seguridad de cualquier entidad que opere en el ámbito digital. (Rivas, 1988)

2.3.1.1 De los orígenes de la auditoría

La auditoría tuvo sus orígenes en el Reino Unido, impulsada por la necesidad de establecer un control más riguroso en el sector financiero. Aunque existían sistemas de control desde tiempos anteriores, su principal finalidad era verificar la integridad de aquellos responsables de manejar fondos. La prevención de fraudes también fue un catalizador crucial en la formación de lo que hoy conocemos como auditoría. Con el tiempo, el concepto de auditoría ha evolucionado, adaptándose a diversas áreas y evaluando procesos en instituciones amplias, tanto del sector público como del privado. (Sánchez Ch., 2021)

2.3.1.2 Código deontológico de la función de auditoría

En auditoría como en toda rama de estudio debe existir un código deontológico que este regido por cuestiones éticas y morales que deben ser pilares que guíen a los profesionales que se preparan en dicha ciencia. Dentro del código deontológico de la auditoria informática se presentan algunos principios que deben ser marcas representativas en la hoja de vida profesional de los auditores, dichos principios buscan garantizar la integridad, seguridad y calidad de las auditorías. Para los profesionales en auditorías se presentan los siguientes aspectos que deben cumplir a cabalidad dentro de su vida profesional y en cada trabajo que realicen y estos son: integridad, objetividad, confidencialidad, competencia, calidad profesional, transparencia, responsabilidad profesional, respeto, independencia y respeto a la ley. Es esencial que cada profesional auditor sepa de estos principios éticos y morales que van a garantizar su profesión a lo largo de la misma. (Menéndez, 2022)

2.3.1.3 Criterios por seguir para la composición del equipo auditor

Es imperativo establecer una planificación meticulosa, definiendo claramente los objetivos que se aspiran lograr y delineando los procedimientos que guiarán la consecución de dichos objetivos. Una pieza clave en esta preparación es la elección de un equipo auditor competente, dado que el éxito de la auditoría dependerá en gran medida de su experticia y habilidad.

Es importante respaldar al personal no solo con certificados y documentación que confirmen su capacitación y habilidades técnicas, sino también asegurándose de que tengan muy claros sus deberes y responsabilidades en lo que respecta a la auditoría. Las personas encargadas de esta tarea requieren un conjunto diverso de habilidades; necesitan una buena formación técnica y experiencia, la capacidad de comunicarse de manera eficiente, un conocimiento actualizado de las reglas y estándares que pertenecen a su trabajo y un enfoque justo e imparcial que evite posibles conflictos. También deben ser hábiles para analizar y evaluar la información y, sobre todo, deben comportarse con un fuerte sentido ético y concienzudo. (Chicano, 2015)

2.3.1.4 Relación de los distintos tipos de auditoría en el marco de los sistemas de información

En la era actual, la tecnología impulsa rápidamente el progreso científico, ampliando continuamente las áreas de estudio y especialización, como IT y ciberseguridad. Esta expansión ha llevado a la aparición de diversos tipos de auditorías, adaptadas según el área a evaluar. Estas auditorías pueden ser internas, realizadas por el personal de la organización, o externas, realizadas por auditores independientes. Las auditorías externas pueden ser de segunda parte, contratadas por la propia empresa, o de tercera parte, realizadas por entidades reguladoras certificadas. Independientemente del tipo, el propósito central de la auditoría es asegurar el cumplimiento de las normas y estándares actuales. (Arantes, 2023)

2.3.1.5 Tipos de pruebas a realizar en el marco de una auditoría

Dentro de los procesos de auditorías que se llevan a cabo dentro de las organizaciones un factor importante son los tipos de pruebas que se aplican durante el proceso de auditoría estas con el fin de verificar aplicaciones, sistemas operativos con datos en función de pruebas.

Estas se ejecutan mediante el análisis de datos de entrada, salida y datos esperados de esta manera comprobar la efectividad y eficacia de los sistemas que han sido objetos de evaluación durante el proceso. Entre las pruebas que se pueden aplicar durante un proceso de auditoría se destacan las sustantivas aplicadas para identificar errores provocados por la ineficiente seguridad existente y las pruebas de cumplimiento que determina si los controles aplicados están respondiendo de forma adecuada a los requerimientos de las organizaciones. (Rivas, 1988)

2.3.1.6 Tipos de muestreo a aplicar durante el proceso de auditoría

Dentro de un proceso de auditoría es un requisito estricto que los auditores deben demostrar con evidencia documentada usada durante su análisis dentro de las organizaciones bajo los cuales se establecen conclusiones y recomendaciones. Estas evidencias deben ser de comprobatorias, competentes y suficientes para sustentar sus aseveraciones luego de realizar el estudio. En ese contexto en auditoría se cuenta con la herramienta conocida como el muestreo la cual lleva a determinar y orientar al profesional auditor sobre qué áreas de la institución auditada requiere de un análisis más exhaustivo y cuales no requieren de mayor consideración, garantizando así la veracidad y efectividad de la auditoría efectuada. Un método de muestreo es el estadístico que sirve como respaldo para los criterios vertidos por el auditor. (Chicano, 2015)

2.3.1.7 Identificación y evaluación de riesgos de auditoría

Cuando se da un proceso de auditoría en una entidad sin considerar su actividad es supremamente importante tener en cuenta cuales sería los posibles riesgos potenciales a los que se deben poner mayor atención ya que por grado de riesgos son más posibles de materializarse y provocar daños en las organizaciones tales como la pérdida de información o llegar a una suspensión de sus actividades. Una vez que se han identificado estos riesgos el profesional auditor podrá trazar rutas de trabajos con procedimientos técnicos acordes a cada uno de estos y así lograr dar una opinión más formada basada en datos técnicos y reales sobre la situación presentada. Es importante considerar que riesgos significativos son aquellos que están directamente relacionados con transacciones y procesos significativos e importantes. (Públicos, 2020)

2.3.1.8 Fases generales de una auditoría

Como todo proceso de investigación de campo lleva un control de fases que realizan para lograr el objetivo final que es brindar resultados, la auditoría también cuenta con una serie de fases que son quienes encaminan un estudio de esta índole en cualquier tipo de organización. Según (Menéndez Arantes, 2022) las fases de auditoría son las siguientes:

- Planificación inicial y objetivos de alcance: aquí se da una reunión con el cliente durante la cual se establecen alcances y límites para el estudio.
- Análisis de riesgos y amenazas: se efectúa un exhaustivo análisis sobre cuáles serían los posibles riesgos o amenazas a los que podría estar expuesta la organización.
- Definir soluciones necesarias: con datos obtenidos por los estudios de análisis y factibilidad se procede a identificar y recomendar soluciones objetivas que ayuden a mitigar los riesgos encontrados.
- Implantar cambios necesarios: en esta fase y mediante un calendario adecuado de implantación se procede a poner en marcha las soluciones brindadas mediante estudios de factibilidad.
- Monitorización y evaluación de resultados: se debe hacer un monitoreo sobre cómo está funcionando a partir de las soluciones dadas la organización y sus sistemas y si estas están cumpliendo con los objetivos planteados.

2.3.1.9 Explicación de los requerimientos que deben cumplir los hallazgos de auditoría

En auditoría se usa el termino de hallazgos para hacer énfasis en de información recolectada durante el proceso recolectando información específica, acerca del estudio, tareas y procesos auditados mismos que van a ser analizados y evaluados de esta forma puede ser tomado en cuenta como un factor de interés para la organización. Estos hallazgos se presentan como un instrumento de crítica en los que se presentan información sobre las falencias o debilidades encontradas durante el estudio y se incluyen en el documento oficial que se presenta como informe de la auditoría. Es importante tener en cuenta que estos hallazgos también pueden ser factores positivos por lo tanto estos no definen conclusiones del profesional auditor, sino que solo contribuyen a sustentar hechos que se presentan en el informe pasados por análisis técnicos. (Tejada, 2023)

2.3.1.10 El informe de auditoría

Al llevarse a cabo un estudio este debe ser documentado en todas sus etapas y procesos describiendo las metodologías usadas y practicas técnicas que llevaron a las conclusiones vertidas. En el caso de la auditoría a este documento se denomina Informe final de auditoría. En la auditoría informática se deben presentar dos documentos de los que uno será técnico y otro de índole ejecutivo de manera que todas las partes interesadas logren comprender el trabajo entregado por el profesional auditor. Como ya se ha mencionado en ese documento o informe se deben presentar los procesos y sus plazos, las normativas y estándares que fueron usadas como herramientas que rigieron la investigación y un glosario de las palabras pocos comunes en el lenguaje diario, en si el informe es un resumen de los realizado, pero con detalles exactos y con conclusiones y recomendaciones, firmado por el auditor y entregado al cliente. (Públicos, 2020)

2.3.2 Gestión de seguridad

La gestión de seguridad hace referencia a una serie de técnicas y procesos que se deben llevar a cabo de manera constante dentro de las organizaciones con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información. Actualmente dentro de las compañías la información es considerado uno de los activos más valiosos por lo cual esta debe implementar medidas de seguridad tanto preventivas, de reacción y correctivas para saber gestionar de manera adecuada los posibles incidentes que pongan en evidencias vulneraciones este bien corporativo. La gestión de seguridad es proceso adaptivo capaz de responder a cualquier amenaza o desafíos presentados a diarios por el constante avance de la era digital. (Sevillano, 2020)

2.3.2.1 Incidentes de seguridad

Incidente de seguridad es considerado a cualquier evento que pueda llegar a ocasionar interrupciones o disminución de calidad en servicios que son llevados a cabo por un sistema o en casos mayores estos logren afectar la integridad de la información disponible. Estos pueden ser provocados por personas internas a la organización afectada o a su vez externas con distintos fines maliciosos entre los que se encuentran; utilizar, manipular, alterar o tener acceso a recursos valiosos como la información. Se debe considerar que los incidentes de seguridad pueden ocurrir también por errores humanos dentro de la organización o factores fueras de la

intuición humana como son los desastres naturales entre estos incendios, inundaciones, tormentas o fallas en la electricidad para esto importante que las organizaciones cuenten con políticas de seguridad listas para mitigar los efectos de los riesgos mencionados. (Vieites, 2015)

2.3.2.2 Respuesta ante incidentes de seguridad

Saber controlar los incidentes de seguridad debe ser un objetivo fundamental en todas las organizaciones y no solo en las que cuentan con grandes dimensiones estructurales, para responder a los incidentes de seguridad las empresas den contar con personas capacitadas con conocimientos técnicos en el manejo y gestión de incidentes de seguridad. En ocasiones el tamaño de las empresas impide contar con recursos como estos para mantener niveles de seguridad altos y confiables, para eso se recomienda periódicamente contratar personal externo que efectúe revisiones en todos los sistemas en los que transita información o se llevan procesos sensibles de la organización. (Tejada, 2023)

2.3.2.3 Políticas de seguridad

Un documento de políticas es un registro formal que detalla las directrices, requisitos y prácticas específicas que deben observarse de manera rigurosa en una organización. La creación de políticas desempeña un papel fundamental en la gestión de una organización, ya que permite la formulación de estrategias para mitigar posibles vulnerabilidades administrativas y optimizar la administración de recursos, en particular, el recurso humano. Estas políticas representan herramientas cruciales para la gestión de la seguridad dentro de las organizaciones y se componen de tres elementos esenciales. En primer lugar, se encuentra el título o declaración, que consiste en la presentación del enunciado de la política junto con un resumen conciso de su contenido total. (Sevillano, 2020)

2.3.2.4 Gestión de incidentes de seguridad

La gestión de incidentes de seguridad engloba una serie de buenas prácticas para logar combatir y mitigar cualquier tipo de amenaza de seguridad mismos que pueden afectar sistemas, redes de internet, aplicaciones o información dentro de una organización. Para evitar que los incidentes de seguridad detectados causen daños mayores dentro de los procesos de las organizaciones, existe una serie de actividades que deben llevar a cabo para gestionar los

incidentes, el personal encargado debe comenzar por aislar los equipos afectados y respaldar la información con copias de seguridad, capturar y proteger la evidencia, analizar el tipo de información que se procesa para dar con la razón y tipo de incidente, comunicar a todas las partes interesadas, participar de las investigaciones legales, aplicar soluciones emergentes y eliminar intrusos para de esta forma finalmente lograr recuperar la información y equipos afectados. (Vieites, 2015)

2.3.2.5 La gestión del riesgo

Gestionar los riesgos se define como una serie de procesos estructurados que se llevan a cabo para identificar, sacar diagnósticos y mitigar los riesgos que se puedan estar presentes y que atenten contra la seguridad de la información. Para esto se comienza por identificar y poner bajo buen recaudo los activos dentro de las organizaciones tales como; sistemas de información, datos de la organización y las redes de amenazas y vulnerabilidades que tiendan a comprometer la integridad, disponibilidad y confidencialidad de la información. Como ya hemos mencionado para gestionar los riesgos lleva unos procesos y se comienza por identificar y salvaguardar los activos, identificar las amenazas, analizar los impactos, priorización de amenazas, identificar técnicas de mitigación y evaluar el riesgo residual. (Arantes, 2023)

2.3.2.6 Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención

Según la norma ISO 27701:2005, un incidente de seguridad es cualquier amenaza que ponga en riesgo las operaciones y la información de una organización. Los intentos de intrusión son actividades que buscan comprometer sistemas o procesos, afectando la disponibilidad, integridad y confidencialidad de la información. Estas amenazas pueden surgir de usuarios no autorizados, usuarios autorizados con privilegios, o usuarios con actividades específicas. Para prevenir estas vulnerabilidades, se utilizan sistemas de detección de intrusiones (IDS) que proporcionan seguridad adicional a equipos y redes, especialmente ante el gran tráfico de información en los sistemas de gestión. (Chicano, 2015)

2.3.2.7 La seguridad en los elementos físicos existentes en una red

Al hablar del os elementos físicos de una red se engloba a una serie de productos y herramientas que complementan este servicio de red tales como; maquinas, routers, switches entre otros, todos estos dispositivos tienen una menor capacidad de control ya que son monitoreados mediante la programación de un software, sin embargo, esto no altera en nada su función como elementos de importancia en red. Para las organizaciones es fundamental tomar en cuenta su seguridad ya que son consideradas una parte fundamental y de ingreso a los sistemas de una organización. Estos equipos mantienen un sistema de comunicación entre sí y generalmente están comunicados mediante cables como medios de transmisión de los cuales existen unos más susceptibles a otros a caer en vulnerabilidades de ataques de inseguridad. (Gil & Orueta, 2014)

2.3.2.8 El problema de la seguridad en la conexión a internet

Como ya es conocido internet es una red de utilidad común que empezó desde una forma bastante limitada, comparados a los que hay disponibles en la actualidad, pues a sus inicios la capacidad de los equipos era bastante limitada, con algunas versiones menos que a las que se cuentan actualmente. Actualmente es esencial para las organizaciones asumir la inseguridad como un factor fundamental, que puede limitar sus diseños a la hora de intentar lanzar un producto o servicio al mercado, es primordial que las organizaciones al menos intenten gestionar los riesgos de seguridad informática enfocados a las conexiones de redes de internet, comprendiendo que es un riesgo siempre latente el cual debe estar en constante monitoreo. (Vieites, 2015)

2.3.2.9 Seguridad de la información (ISO 27001)

La norma ISO es una herramienta de estándares con buenas prácticas que estable los requisitos para implementar, mantener y mejorar sistemas de gestión de seguridad de la información en una organización. La ISO 27001 brinda a las organizaciones base para comprender las organizaciones y su contexto, comprender sus necesidades y determinar cuáles son las expectativas de las partes interesadas con respecto al sistemas de gestión de seguridad de la información SGSI. Brinda un marco de referencia para llevar a cabo procesos como identificar, evaluar y gestionar los riesgos de seguridad de la información, y establecer medidas correctivas de seguridad pertinentes. (Baca, 2016)

2.3.2.10 Planes de cumplimiento normativo

Con el avance los de intentos de ataques o vulnerabilidades evidentes para intrusos en los SGSI, estos se han convertido en una herramienta valiosa a la hora de querer crear una empresa o poner a disposición un nuevo producto, servicio o proyecto, teniendo en cuenta un plan de cumplimiento que garantice la protección de los datos que se van a dar o se están generando dentro de los procesos de la organización. El plan de cumplimiento es eso, una garantía de cumplimiento de la normativa relativa a la privacidad y protección de datos circulantes, mismos que van a ser capturados, gestionados y explotados. Con esta herramienta se garantiza el cumplimiento de leyes, normas y regulaciones relevantes de esta forma evitar sanciones y asegurar el espacio dentro del mercado. (Sevillano, 2020)

2.4 Conclusiones del marco teórico

La auditoría informática y la gestión de la seguridad de la información tienen profundas raíces históricas con la necesidad de controlar los recursos. Con el tiempo, la creciente importancia de la información en las organizaciones y el desarrollo de la tecnología han llevado a un creciente interés en la auditoría de seguridad de la información. Lo que demuestra que este tema tiene una sólida base histórica y teórica en la gestión de la seguridad de la información.

La existencia de investigaciones y proyectos recientes relacionados con la auditoría informática y la seguridad de la información confirma la validez y relevancia de este tema. Ejemplos de investigaciones exitosas sobre la aplicación de estándares como ISO 27001 para mejorar la seguridad de la información organizacional demuestran que existen enfoques efectivos para abordar los desafíos actuales de seguridad de la información. Estos estudios respaldan la efectividad y aplicabilidad de la auditoría informática en la gestión de la seguridad de la información.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

En este capítulo, se abordan los métodos de investigación aplicados en el desarrollo de la auditoría informática, buscando enmarcar la investigación dentro de lineamientos claros que permitan proyectar sus resultados.

La aplicación de tipos y métodos de investigación diversos, siempre que estén alineados con los objetivos de la investigación en curso, proporciona una mayor claridad al momento de seleccionar y aplicar las herramientas para la recolección de datos.

3.2 Tipo de investigación

Dentro de los tipos de investigación se encuentran un sin número de herramientas, técnicas y métodos con los que es posible la obtención de información verificada que aporte a los estudios que se generen. Bajo su aplicación es posible seguir algoritmos de búsqueda y aplicación de instrumentos de recolección de datos elaborados bajo una guía reglamentada que dependerá del tipo de investigación que se esté ejecutando, posteriormente de igual manera la interpretación de datos se realiza según la investigación desarrollada. (Sambrano, 2020)

3.2.1 Investigación documental

Para comprender de manera integral un determinado tema o preocupación, la investigación documental requiere explorar múltiples fuentes publicadas, como informes, archivos personales, libros y revistas. Al examinar estos materiales con técnicas cuidadosas, los investigadores los estudian de cerca en busca de detalles valiosos y al mismo tiempo forjan conexiones para mejorar su conocimiento en un campo en particular. Es importante señalar que, a pesar de no concentrarse en el trabajo de campo o de laboratorio, la investigación documental aún requiere una recopilación, organización y análisis de datos minuciosos para generar conocimientos y contribuciones significativas a los estudios existentes. (Hernández, 2001)

La investigación documental fue esencial para fortalecer la base de este estudio de investigación, proporcionó una sólida fundamentación teórica, contexto histórico, revisión de literatura y datos relevantes que enriquecieron la calidad y profundidad de la investigación. Apoyados a este tipo de investigación se obtuvo una orientación más clara sobre cómo desarrollar el estudio escogiendo así la metodología con la cual fue ejecutado.

3.2.2 Investigación de campo

Al interactuar directamente con el sujeto de investigación, la investigación de campo permite la recopilación de información empírica y el cultivo de una comprensión profunda de un fenómeno particular en su entorno natural. Con el objetivo de obtener datos indocumentados o inadecuados, este método facilita la observación exhaustiva de un fenómeno en su hábitat objetivo, ayudando en consecuencia a la producción de nuevos conocimientos y una comprensión integral de la realidad examinada. Es importante señalar que este tipo de investigación se utiliza en estudios en los cuales se pretende analizar datos cualitativos y cuantitativos. (García, 2012)

La investigación de campo brindó enfoque que implicó recopilar datos directamente en la empresa sede de los eventos o fenómenos estudiados. Proporcionó datos empíricos, profundizando así en el contexto, validando teorías, recopilando datos cualitativos y cuantitativos, identificando factores contextuales, siendo aplicada de manera práctica, fue una herramienta fundamental para comprender y abordar la real situación de la organización auditada.

3.2.3 Investigación explicativa

La técnica de investigación explicativa propone métodos de para comprender por qué ocurren ciertos fenómenos o eventos. Su objetivo principal es identificar las causas o relaciones subyacentes que explican un resultado particular. El método se basa en la formulación de hipótesis causales y la realización de investigaciones destinadas a determinar relaciones entre variables, generalmente utilizando métodos cuantitativos y análisis estadístico. A través de la investigación interpretativa, los investigadores buscan proporcionar una comprensión más profunda y detallada de las relaciones causales entre diversas variables y eventos que

contribuyen a la generación de conocimiento logrando así la formulación de conclusiones que contrasten versiones científicas. (Bernal, 2006)

Este tipo de investigación fue elemento crucial para el desarrollo de la presente investigación, ya que se la aplicó mediante formularios sobre los controles y requisitos de cumplimiento brindados por la norma ISO 27001 de esta manera se pudo evidenciar en que parte de la organización existían falencias o posibles oportunidades mismas que fueron expuestas para un análisis exhaustivo y así determinar conclusiones basados en datos reales y actualizados.

3.3 Métodos de investigación

3.3.1 Método analítico-sintético

Este método se refiere a la desmembración mental del material que está siendo objeto de estudio, analizar cada uno de los elementos que componen a este, con esto se logra obtención de más información que se transforma en conocimientos basado en estudios prácticos acerca del objeto de estudio. Este tipo de análisis requiere de estudios multifacéticos con los que se pueda cubrir todas las áreas de estudio de lo que se investiga y comprender su estructura, con el estudio por descomposición de elementos se lograr realizar una delimitación de aquello que resulta esencial para los objetivos del estudio, de lo que no lo es, minimizar a simple lo que pueda resultar a vista general como complejo, es así que el método analítico- sintético logra así un análisis clasificado en cuanto a objetos y fenómenos que puedan aparecer durante un estudio de investigación. (León & Garrido, 2007)

Dentro del presente estudio este método se aplicó al analizar y comparar las evidencias de los cumplimientos de controles durante el proceso de auditoria cumpliendo con lo demandado por la Norma ISO 27001.

3.3.2 Método deductivo

Método para razonar acerca de comportamientos y patrones con el cual se puede ir desde lo general para así dar explicaciones particulares sobre comportamientos de los fenómenos que intervienen durante un proceso de investigación. Con este método aplicado durante un estudio

se logra la comprobación de postulados o hechos generales logrando de esta forma llegar a conclusiones más claras y concisas basadas en estudios profundos. (Bernal, 2006)

Este método fue incluido durante el estudio como herramienta que ayudó a comprender los hechos y estado actual de la organización objeto de estudio partiendo desde acontecimientos generales que se presentaban y que ya antes fueron expuestos durante la explicación de la problematización que da vida al estudio.

3.4 Fuentes de información de datos

3.4.1 Encuesta

Durante procesos de investigación de algún fenómeno, hipótesis o comprobación de alguna afirmación que requiera de respaldos científicos que le respalden, la encuesta se presenta como una herramienta mediante la cual y siendo aplicada en una determinada población se puede extraer información sistemática y confiable relacionada al contexto del estudio que se esté llevando a cabo. Con la encuesta es posible determinar posibles resultados o patrones de comportamientos recogidos de su aplicación a una muestra de la población que interviene en el objeto de estudio, la encuesta siempre resulta más factible ser aplicada a una parte de la población (muestra) y no a su totalidad ya que podría resultar en algunos casos hasta imposible. (Font, 2016)

Como parte de los procesos de obtención de datos confiable durante la ejecución del estudio se aplicó una encuesta a los servidores de la empresa objeto de estudio en la cual se consultó sobre temas puntuales referentes al contexto del estudio que se estaba llevando a cabo. Al contar con una población reducida no se consideró la toma una muestra de esta, se aplicó a su totalidad.

3.4.2 Entrevista

Es una actividad o conversatorio llevada a cabo por un entrevistador y un entrevistado, en la cual se plantean interrogantes debidamente diseñadas y encuadradas en un tema o hecho explícito de manera que las respuestas que o análisis que se den de la misma sirvan para la toma de decisiones informadas desde fuentes confiables. La entrevista puede ser estructurada,

semiestructurada o no estructurada, dependiendo de la formalidad y el grado de flexibilidad en las preguntas y respuestas. (Sánchez, 2017)

La entrevista fue aplicada como una fuente de información primaria, con la cual se logró obtener información de primera mano y confiable, los entrevistados para la obtención de información que garantice la legitimidad del presente estudio fueron la gerente de la organización objeto de estudio y la secretaria general de la misma principales administradoras de la información y por ende de los sistemas de información que se genera en la empresa.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población y muestra

3.5.1.1 Población

La población en el contexto de proyectos de investigación de campo se refiere al conjunto completo de elementos que comparten características comunes y que son objeto de estudio en un determinado tiempo y espacio. Es esencial para la obtención de datos con información real y de primera mano, ya que representa la totalidad de individuos, objetos o fenómenos que son relevantes para el tema de investigación. Es importante destacar que la población puede ser finita o infinita, dependiendo de la naturaleza del estudio. Una población finita implica que se puede enumerar y delimitar claramente, mientras que una población infinita sugiere que la totalidad de los elementos no se puede determinar con precisión. (Plata, 2019)

Para la investigación, se consideró una población que incluye a los colaboradores de la entidad sujeta a la auditoría, abarcando diversas posiciones laborales que gestionan y manipulan información relacionada con la institución. En esta población se destacan dos roles clave: la gerente general y la secretaria, quienes desempeñan funciones cruciales en el flujo de información y tienen un impacto significativo en las actividades comerciales. Además, se incluyeron 28 empleados y 16 clientes relevantes de la organización, cuya interacción y experiencia resultan esenciales para comprender el contexto completo de la auditoría. Este enfoque integral asegura una representación significativa de los distintos roles y perspectivas dentro de la entidad.

3.5.1.2 Muestra

La muestra es un conjunto selecto de elementos extraídos de una población extensa para facilitar el análisis en estudios de investigación. Esta técnica es esencial cuando la magnitud de la población dificulta la recopilación de datos de todos los elementos. Al optar por una muestra representativa, se logra una eficiente obtención de información sin comprometer la validez de los resultados. La muestra, al reflejar características clave de la población, permite realizar inferencias significativas sobre el conjunto total. Su aplicación estratégica optimiza el proceso de investigación y posibilita generalizaciones respaldadas. (Rodríguez, 2021)

Dado el tamaño relativamente pequeño de la población en estudio, no se consideró necesario aplicar un proceso de muestreo discrecional para la investigación en curso.

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

3.5.2.1 Encuesta

Encuesta: Dirigida a los empleados de Electrodomésticos Yeray

Objetivo: Identificar posibles falencias en las prácticas de seguridad de la información entre los empleados y administradores de "Yeray Electrodomésticos", evaluando la necesidad de mejoras.

1. ¿Utiliza dispositivos exclusivos proporcionados por la empresa para realizar sus tareas laborales?

   Si ☐ No ☐

2. ¿Ha recibido capacitación sobre las políticas de seguridad de la información en la empresa?

   Si ☐ No ☐

3. ¿Está al tanto de los procedimientos de seguridad establecidos para el manejo de información confidencial?

   Si ☐ No ☐

4. ¿La empresa proporciona suficientes herramientas y recursos para garantizar la seguridad de la información?

   Si ☐ No ☐

5. ¿Ha experimentado algún incidente de seguridad informática en el último año?

   Si ☐ No ☐

6. ¿Siente que las políticas de seguridad de la informática afectan negativamente su productividad laboral?

   Si ☐ No ☐ Desconozco las medidas implantadas ☐

7. ¿Está al tanto de la existencia de un protocolo de respuesta a incidentes de seguridad en la empresa?

   Si ☐ No ☐

8. ¿Ha participado en simulacros o entrenamientos relacionados con la seguridad informática en la empresa?

   Si ☐ No ☐

9. ¿Ha notado alguna actividad sospechosa en los sistemas o redes de la empresa en el último año?

   Si ☐ No ☐

10. ¿Se le proporciona regularmente información actualizada sobre las nuevas amenazas cibernéticas y cómo prevenirlas?

    Si ☐ No ☐

11. ¿Cumple con las políticas de seguridad de la información al trabajar fuera de las instalaciones de la empresa?

Si ☐ No ☐

12. ¿Tiene usted acceso a toda la información de la empresa?

Si ☐ No ☐

3.5.2.2 Entrevista

Entrevista; Dirigida para el gerente y la secretaria de Electrodomésticos Yeray.

Objetivo: Identificar posibles falencias en las prácticas de seguridad de la información entre los empleados y administradores de "Yeray Electrodomésticos", evaluando la necesidad de mejoras.

1. ¿Cómo se asegura de que los empleados utilicen los dispositivos exclusivos proporcionados por la empresa para llevar a cabo sus tareas laborales?

2. ¿Cuál es la estrategia implementada para garantizar que los empleados reciban capacitación acerca de las políticas de seguridad de la información?

3. ¿Desde su perspectiva, ¿cuál es la efectividad de los procedimientos establecidos para el manejo de información confidencial?

4. ¿Qué medidas se adoptan para proveer a los empleados de las herramientas y recursos necesarios para asegurar la confidencialidad de la información?

5. ¿Cómo aborda y gestiona cualquier incidente de seguridad informática que se presente en la empresa?

6. ¿Cuál es su evaluación sobre la percepción de los empleados acerca de cómo las políticas de seguridad informática pueden afectar su productividad laboral?

7. ¿Podría describir el protocolo vigente para responder a incidentes de seguridad en la empresa?

8. ¿Qué iniciativas se llevan a cabo para involucrar a los empleados en simulacros o entrenamientos sobre seguridad informática?

9. Desde su posición, ¿ha observado alguna actividad sospechosa en los sistemas o redes de la empresa durante el último año?

10. ¿Cómo garantiza que los empleados estén al tanto de las nuevas amenazas cibernéticas y las medidas preventivas correspondientes?

11. ¿Qué controles se implementan para asegurar que los empleados cumplan con las políticas de seguridad de la información cuando trabajan fuera de las instalaciones?

12. ¿Cómo se gestiona el acceso a la información sensible de la empresa desde su posición en la empresa?

3.5.2.3 Encuesta dirigida a clientes de la organización

Objetivo: Medir la satisfacción de los clientes en relación con la confidencialidad de la información comercial, identificando posibles áreas de mejora y oportunidades para fortalecer la seguridad de la información.

1. ¿Considera que la empresa ha mantenido la confidencialidad de la información relacionada con sus transacciones y actividades comerciales de manera satisfactoria?

Si ☐ No ☐

2. ¿Cómo calificaría la transparencia de la empresa en cuanto a la protección de la información que comparte con usted como cliente?

- Muy Satisfactorio

- Satisfactorio

- Neutral

- Insatisfactorio

- Muy Insatisfactorio

3. ¿Se siente seguro/a respecto a la gestión confidencial de la información personal que comparte con la empresa durante sus transacciones?

Si ☐ No ☐

4. ¿Ha experimentado alguna situación en la que haya percibido una falta de confidencialidad por parte de la empresa en relación con su información comercial?

Si ☐ No ☐

5. ¿Cómo evaluaría la eficacia de las medidas de seguridad implementadas por la empresa para proteger la información confidencial de sus clientes?

- Muy Efectivas

- Efectivas

- Neutrales

- Poco Efectivas

- Nada Efectivas

6. ¿Recomendaría la empresa en función de la confidencialidad que mantiene con respecto a la información de sus clientes?

- Definitivamente Sí

- Probablemente Sí

- No estoy seguro/a

- Probablemente No

- Definitivamente No

3.5.2.4 Estructura de los instrumentos de recolección de datos aplicados

El instrumento de encuesta para los servidores de la empresa consta de un banco de 12 preguntas cerradas con las opciones de Si y No con una excepción en ítems 6 con una opción adicional que ayudara a dar veracidad a otras respuestas del cuestionario. En esta se busca conocer cuál es su conocimiento en cuanto a las políticas de seguridad establecidas en la empresa para el manejo de la información y si los equipos brindan la facilidad en sus actividades.

La entrevista consta de 15 preguntas seleccionadas meticulosamente para abordar a los principales operarios de la información consolidada en la organización, en la que se exploran aspectos sobre qué tipo de políticas están implementadas en la empresa que garanticen la seguridad de la información, como se está garantizando la responsabilidad ente los empleados sobre el manejo y ejecución de los procesos internos. Esta entrevista está dirigida al gerente y secretaria general de Electrodomésticos Yeray.

3.5.3 Plan de recolección de datos

Para la aplicación de estas herramientas de obtención de datos, se formuló el siguiente cronograma de activades:

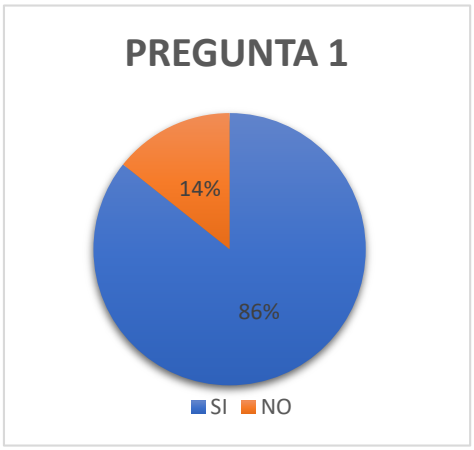
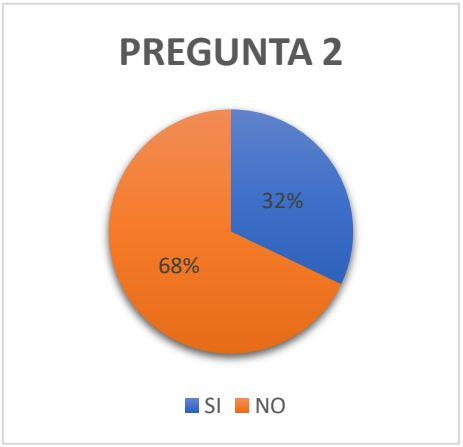
Fecha	Actividad	Personal involucrado
27/11/2023	Revisión y ajuste final de las preguntas de la encuesta y la entrevista.	Coordinador de estudio de investigación
28/11/2023	Coordinación con los participantes y confirmación de disponibilidad.	Personal administrativo y empleados de Yeray Electrodomésticos
29/11/2023	Envío de la encuesta electrónica a todos los empleados de "Yeray Electrodomésticos".	Empleados de la empresa

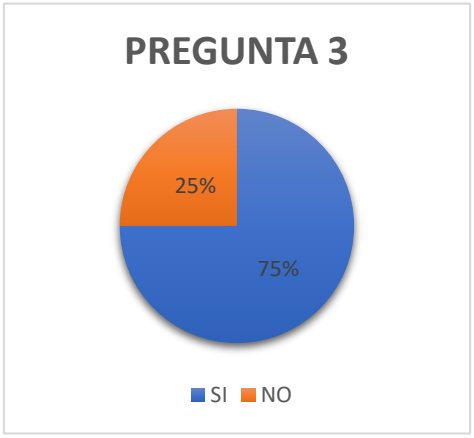
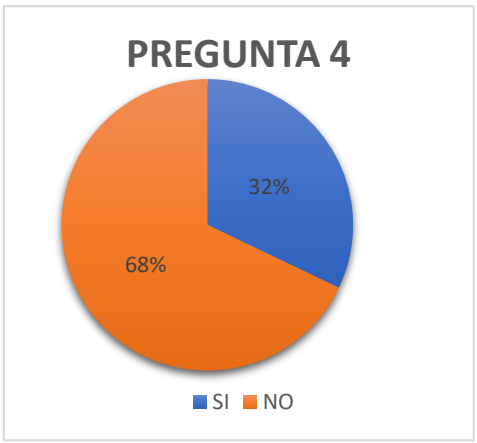
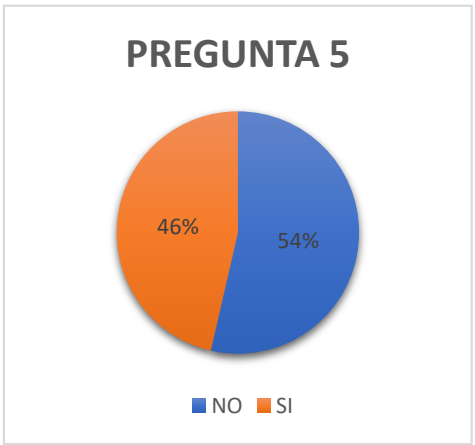
04/12/2023	Envío de recordatorios a aquellos que aún no hayan completado la encuesta.	Empleados de la empresa
05/12/2023	Programación de entrevistas con el gerente y la secretaria general	Gerente y la secretaria general de la empresa.
08/12/2023	Conducción de entrevistas con el gerente y la secretaria general	Gerente y la secretaria general de la empresa.

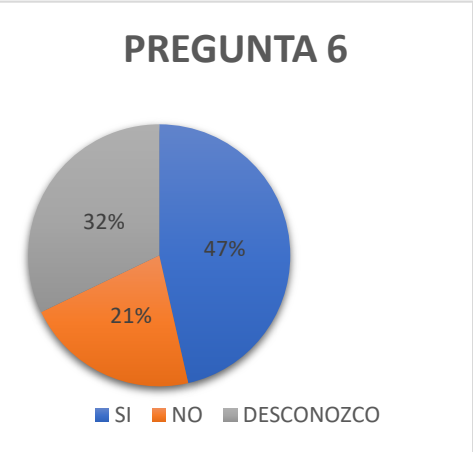
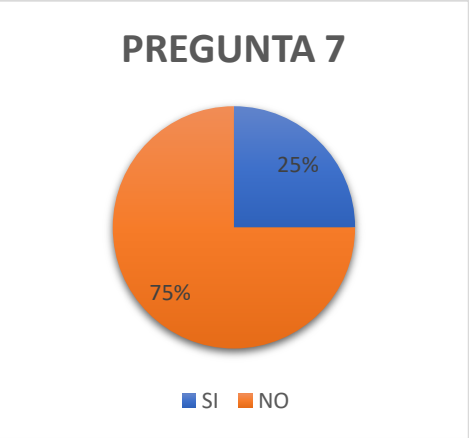
Tabla 1. Plan de recolección de datos

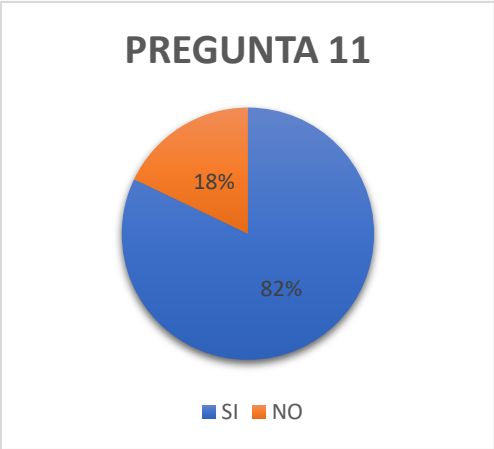
3.6 Análisis y presentación de resultados

3.6.1 Análisis de encuesta dirigida a los empleados de Electrodomésticos Yeray

Pregunta	Gráfico	Interpretación
¿Utiliza dispositivos exclusivos proporcionados por la empresa para realizar sus tareas laborales?		En el gráfico se destaca que la gran mayoría de los encuestados expresaron de manera positiva que la empresa les suministra dispositivos tecnológicos para llevar a cabo sus tareas. Solo una pequeña fracción, aproximadamente una octava parte, indicó lo contrario.
¿Ha recibido capacitación sobre las políticas de seguridad de la información en la empresa?		La mayoría de los empleados encuestados no ha recibido capacitación en políticas de seguridad, mientras que alrededor de un tercio de sus compañeros sí lo ha hecho.

¿Está al tanto de los procedimientos de seguridad establecidos para el manejo de información confidencial?		Dos tercios de los empleados indicaron estar informados, mientras que el tercio restante no tenía conocimiento de dichos procedimientos.
¿La empresa proporciona suficientes herramientas y recursos para garantizar la seguridad de la información?		La mayoría de los empleados señala que la empresa no les proporciona las herramientas necesarias para asegurar la seguridad de la información, mientras que aproximadamente un tercio sostiene lo contrario.
¿Ha experimentado algún incidente de seguridad informática en el último año?		Una proporción ligeramente superior de encuestados expresó una opinión negativa según se evidencia en el gráfico, en comparación con casi la mitad de la población que reconoce haber experimentado incidentes.

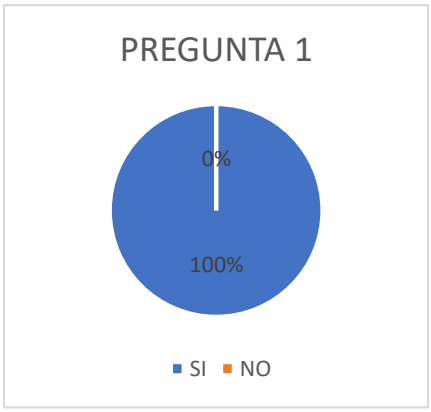
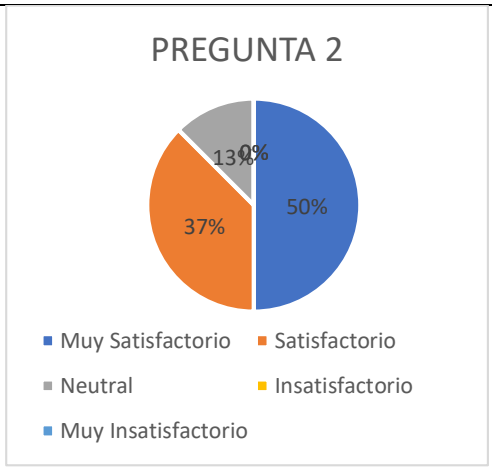
¿Siente que las políticas de seguridad informática afectan negativamente su productividad laboral?		Cerca de la mitad de los participantes afirman verse afectados, seguidos por aproximadamente un tercio de la población que indica desconocer estas directrices, y una quinta parte que asegura no experimentar ninguna afectación en sus funciones.
¿Está al tanto de la existencia de un protocolo de respuesta a incidentes de seguridad en la empresa?		La mayoría, representada por tres cuartas partes de los participantes, afirma estar informada sobre la herramienta de contingencia mencionada, en contraste con la cuarta parte restante que indica no estar al tanto de su existencia.
¿Ha participado en simulacros o entrenamientos relacionados con la seguridad informática en la empresa?		La gran mayoría de los encuestados señaló que no ha participado en eventos preventivos de incidentes de seguridad, en contraste con una minoría que afirmó haberlo hecho.

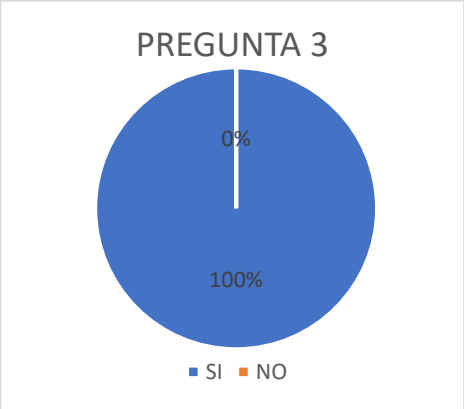
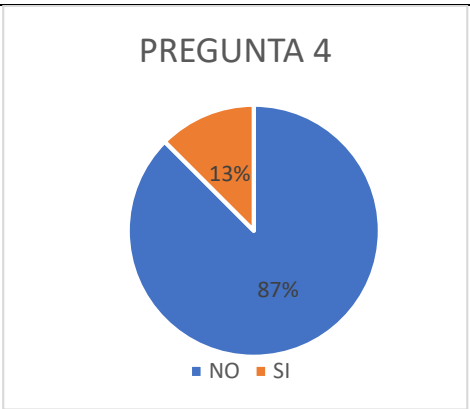
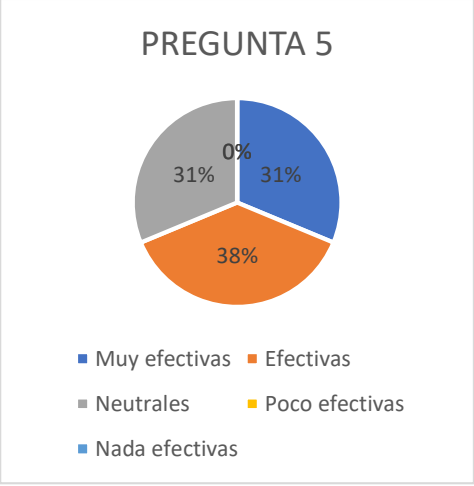
¿Ha notado alguna actividad sospechosa en los sistemas o redes de la empresa en el último año?		Más de la mitad de los empleados afirmó no haber notado nada irregular, mientras que una cantidad significativa expresó lo contrario, indicando que sí ha percibido eventos inusuales.
¿Se le proporciona regularmente información actualizada sobre las nuevas amenazas cibernéticas y cómo prevenirlas?		Más de un tercio de la población indicó no recibir información actualizada sobre el tema consultado, en contraste con una mínima porción que afirmó recibir dicha información.
¿Cumple con las políticas de seguridad de la información al trabajar fuera de las instalaciones de la empresa?		La mayoría de los encuestados afirma cumplir con las directrices establecidas para la seguridad de la información, a diferencia de una minoría que representa menos de la quinta parte encuestada y manifiesta no hacerlo.

¿Tiene usted acceso a toda la información de la empresa?		La mayoría de los encuestados indica no tener acceso a toda la información de la organización, con la excepción de uno que afirma contar con dicho privilegio.

Tabla 2. Análisis encuesta empleados

3.6.2 Análisis de encuesta aplicada a clientes de Yeray electrodomésticos

Pregunta	Gráfico	Interpretación
¿Considera que la empresa ha mantenido la confidencialidad de la información relacionada con sus transacciones y actividades comerciales de manera satisfactoria?		Todos los clientes de la consultados respondieron afirmativamente ante la pregunta, mostrando satisfacción con la forma en que se gestiona la información en las diversas transacciones.
¿Cómo calificaría la transparencia de la empresa en cuanto a la protección de la información que comparte con usted como cliente?		La mayoría de los clientes encuestados expresan satisfacción con el nivel de transparencia de la organización, mientras que una pequeña parte se mantiene en una posición neutral.

¿Se siente seguro/a respecto a la gestión confidencial de la información personal que comparte con la empresa durante sus transacciones?		Todos los clientes considerados en la encuesta expresan satisfacción con la manera en que la empresa gestiona la confidencialidad de la información en sus transacciones.
¿Ha experimentado alguna situación en la que haya percibido una falta de confidencialidad por parte de la empresa en relación con su información comercial?		Una pequeña fracción de la población encuestada menciona haber experimentado alguna inquietud en relación con la confidencialidad de sus actividades comerciales, en contraste con una amplia mayoría que afirma no haber percibido ningún incidente de inconformidad.
¿Cómo evaluaría la eficacia de las medidas de seguridad implementadas por la empresa para proteger la información confidencial de sus clientes?		Más de la mitad de los encuestados expresan un fuerte respaldo a las medidas de seguridad que protegen la información, mientras que un segmento significativo se mantiene neutral ante el tema.

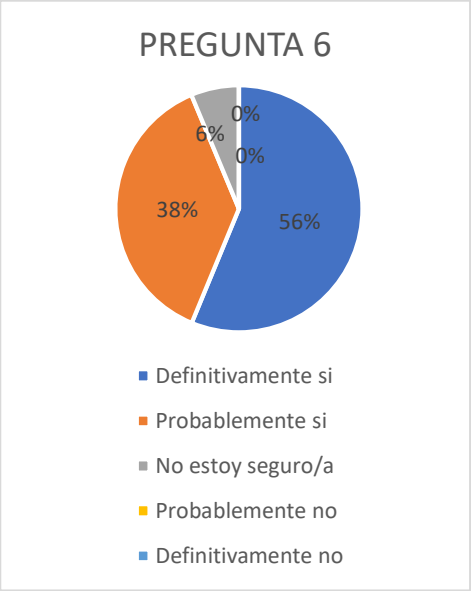
¿Recomendaría la empresa en función de la confidencialidad que mantiene con respecto a la información de sus clientes?		La mayoría de los clientes encuestados se sienten cómodos recomendando la empresa, mientras que otra parte importante estaría dispuesta a hacerlo. Un grupo reducido se muestra indeciso, todo ello en relación con la percepción del manejo de la confidencialidad en las transacciones de la empresa.

Tabla 3. Análisis encuesta clientes

3.6.3 Análisis de entrevista aplicada al gerente y secretaria de Yeray Electrodomésticos

N°	Preguntas	Respuestas	Análisis
1	¿Cómo se asegura de que los empleados utilicen los dispositivos exclusivos proporcionados por la empresa para llevar a cabo sus tareas laborales?	Las personas que trabajan en áreas administrativas poseen la computadora como dispositivo exclusivo, se lleva un control del buen uso.	Se observa que solo al personal de administración de los distintos departamentos se controla el uso de los equipos.
2	¿Cuál es la estrategia implementada para garantizar que los empleados reciban capacitación acerca de las políticas de seguridad de la información?	La persona que nos da la atención técnica capacita en los parámetros requeridos.	Se contempla que cada que se realizan ajustes técnicos, el personal es capacitado por quien realiza dicho trabajo.
3	Desde su perspectiva, ¿cuál es la efectividad de los procedimientos establecidos para el manejo de información confidencial?	Es saber con el tipo de personal con el que se labora y existe el parámetro empresarial.	Existen directrices propias de la empresa para el manejo de la información y contratación del personal.
4	¿Qué medidas se adoptan para proveer a los empleados de las herramientas y recursos necesarios para asegurar la confidencialidad de la información?	Si, mediante guías, notas de crédito se controla la facturación, los parámetros de empresa permiten limitar el acceso y asegurar los recursos que	El personal maneja instrumentos físicos para el manejo del a información que recaban según su responsabilidad dentro de la empresa no más y esta luego es concentrada en secretaria general y gerencia.

		corresponde a cada persona.	
5	¿Cómo aborda y gestiona cualquier incidente de seguridad informática que se presente en la empresa?	Se tiene un informático de confianza para realizar la gestión que se requiere.	Existe un profesional responsable que investiga el origen del incidente, gestiona y soluciona.
6	¿Cuál es su evaluación sobre la percepción de los empleados acerca de cómo las políticas de seguridad informática pueden afectar su productividad laboral?	Dependemos de lo que facturamos diariamente y si la información es filtrada para otros recursos es el empleado directamente el cuestionado no sólo la productividad se afecta, ellos tienen claro eso.	Existen sanciones a los empleados que puedan incurrir en fallas que afecten la productividad y procesos de la empresa, de esta manera se presiona de alguna forma la conciencia de los empleados a cumplir con las políticas establecidas.
7	¿Podría describir el protocolo vigente para responder a incidentes de seguridad en la empresa?	Que una persona calificada acceda a la solución	Solo un profesional capacitado es responsable de la gestión y solución de incidentes.
8	¿Qué iniciativas se llevan a cabo para involucrar a los empleados en simulacros o entrenamientos sobre seguridad informática?	No ingresamos a páginas o programas fuera de los que se utilizan para laborar. Y realizar un mantenimiento eventual.	No se mencionan actividades de buenas prácticas para la prevención de incidentes, sin embargo, destacan mantenimientos sin el personal de planta.
9	Desde su posición, ¿ha observado alguna actividad sospechosa en los sistemas o redes de la empresa durante el último año?	Hasta el momento no.	No se han registrado eventos inusuales que generen alertas de seguridad.
10	¿Cómo garantiza que los empleados estén al tanto de las nuevas amenazas cibernéticas y las medidas preventivas correspondientes?	Estamos pendientes de los avances y tratamos de ser cautelosos en el manejo de información.	Destacan delicados procesos para la gestión de información, pero no existen procedimientos claros para comunicar las posibles potenciales amenazas de seguridad al personal.
11	¿Qué controles se implementan para asegurar que los empleados cumplan con las políticas de seguridad de la información cuando trabajan fuera de las instalaciones?	La plataforma o programa sólo es accesible desde el ordenador en el puesto de trabajo.	Los empleados manejan información de manera física usando facturas o notas de venta y compra, no existen un control adecuado de que la información no sea manipulada negativamente.
12	¿Cómo se gestiona el acceso a la información sensible de la empresa desde su posición?	La información sensible la manejamos sólo dos personas, lo demás está ingresado en el sistema que es todo para una facturación.	La información crítica de la empresa solo la gestionan dos usuarios el resto del personal solo recibe información física desde secretaria.

Tabla 4. Análisis de entrevistas

3.6.4 Presentación y descripción de los resultados obtenidos

En la pregunta 1 de la encuesta a los empleados la mayoría dice recibir dispositivos tecnológicos para el desarrollo de sus actividades laborales, sin embargo, en la pregunta 1 de las entrevistas ambos administrativos consultados destacan que solo el personal de oficina cuenta con un computador proporcionado por la empresa para realizar sus labores en las mismas instalaciones.

En las preguntas 2 de la encuesta como de la entrevista tanto empleados como administrativos destacan que si se dan las respectivas capacitaciones siempre en cuando exista algún mantenimiento de equipos o sistemas por parte de un profesional contratado eventualmente.

En las preguntas 9 de la encuesta a empleados y entrevistas a directivos concuerdan en su mayoría de trabajadores y ambos superiores que se han notado eventos inusuales que generen alertas sobre la seguridad de la información, por tanto, en la pregunta 3 encuestada a los clientes la mayoría dice sentirse conforme con el manejo de su información comercial por parte de la empresa.

En la pregunta 8 de la encuesta a los empleados la mayoría dice no haber sido parte ni recibir capacitaciones sobre amenazas de seguridad. Lo que se confirma con las respuestas de los administrativos que dicen solo realizar mantenimiento eventuales equipos y sistemas, pero con personal externo.

Sobre el manejo de la información crítica de la empresa la mayoría de los empleados coincide con los administrativos en que dicha información solo es concentrada y manipulada por gerencia y secretaria general.

3.6.5 Informe final del análisis de los datos

Se evidencia una discrepancia significativa entre la percepción de los empleados y la de los clientes en relación con la seguridad de la información. Mientras los clientes muestran satisfacción general, los empleados expresan preocupaciones sobre la falta de capacitación, herramientas adecuadas y la percepción de incidentes. Esta brecha destaca la importancia de abordar las inquietudes internas para alinearlas con la imagen externa de la empresa.

La baja participación de los empleados en eventos preventivos de incidentes resalta una oportunidad perdida para fortalecer la conciencia y la preparación para la seguridad.

La gestión de información física, como facturas y notas de venta, presenta una discordancia notable, indicando una posible debilidad en los controles para prevenir manipulaciones negativas. La falta de un control adecuado sobre la información física puede representar un riesgo significativo para la integridad de los datos.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

4.2 Descripción de la propuesta

Ante la problemática expuesta, sugiero implementar una auditoría integral enfocada en la gestión de seguridad de la información, abarcando los recursos físicos vinculados a la información empresarial.

El procedimiento propuesto consistirá en un análisis detallado de los procedimientos de gestión de los recursos tecnológicos empleados en la creación y tratamiento de información. Se dará especial atención a la coherencia y precisión entre la base de datos digital y el inventario físico, explorando tanto las entradas manuales de datos como las actualizaciones automáticas del sistema. Esta fase incluirá la evaluación del estado de los equipos y el funcionamiento de los sistemas, y un escrutinio de los protocolos de seguridad vigentes para detectar posibles brechas o vulnerabilidades.

Con base en los resultados obtenidos durante esta fase diagnóstica, se elaborará un informe detallado. Este documento no solo recogerá las observaciones y hallazgos, sino que propondrá un plan estratégico de mejora. Dicho plan podría contemplar acciones como la capacitación del personal para garantizar el correcto uso y entrada de datos en los sistemas, la implementación de controles más rigurosos para reducir errores humanos y propuestas para optimizar la eficiencia y eficacia de los procesos actuales.

La finalidad de esta auditoría es doble: por un lado, busca asegurar una coherencia total entre la información registrada en la base de datos y el inventario físico, y por otro, tiene como objetivo robustecer los sistemas y protocolos de la organización. Este enfoque no solo garantiza la integridad y actualización de la información, sino que también potencia la eficiencia operativa, minimiza errores y refuerza la seguridad. De esta manera, se pretende consolidar la posición competitiva de la empresa y prevenir eventuales daños a su imagen y reputación.

4.3 Determinación de recursos

4.3.1 Humanos

Para la presente investigación se contempló la participación de empleados, clientes y personal administrativo de la empresa Yeray Electrodomésticos.

4.3.2 Tecnológicos

Recurso	Detalles	Valor U.	V. total
Computadora portátil HP	Core (TM) i7-7500U CPU 8 GB RAM 223 GB Disco duro	$820.00	$820.00
Internet	20 horas de navegación en internet	$0.45.00	$20,45
Cámara fotográfica	Cámara para la obtención de imágenes evidencia de los procesos y eventos.	$100.00	$100.00
		Total	**$940.45**

Tabla 5. Recursos tecnológicos

4.3.3 Económicos

Recurso	Detalles	Valor. U	Total
Transporte	Movilización hacia la empresa auditada.	$5.00	$50.00
Hojas papel boom	Impresiones de entrevistas e instrumentos de auditoría.	$0,05	$1.00
		Total	**$51.00**

Tabla 6. Recursos económicos

4.4 Información de la institución

4.4.1 Reseña histórica de la institución

En 2011, bajo la dirección del ingeniero Marcos Vicuña, la empresa se estableció como proveedora de servicios técnicos para electrodomésticos y aires acondicionados, principalmente de la marca Electrolux. Con el tiempo, se consolidó como uno de los principales proveedores, asegurando la durabilidad de los productos intervenidos. Ante la creciente demanda de productos de línea blanca, ServieElect, ahora conocida como Electrodomésticos y

Repuestos Yeray, expandió su enfoque, no solo proporcionando servicios sino también vendiendo productos a consumidores finales de Electrolux.

La visión empresarial condujo a la creación de Electrodomésticos y Repuestos Yeray, que actualmente se dedica a la venta y distribución de productos de línea blanca y aires acondicionados, incluyendo marcas como Mabe, Electrolux, Innova y Zitro. Ubicada en la provincia Santo domingo de los Tsáchilas, cantón Santo Domingo avenida Tsáfiqui y Augusto Gachet, la empresa no solo alberga sus oficinas administrativas sino también un showroom que exhibe no solo electrodomésticos sino también productos de entretenimiento como teléfonos celulares, amplificadores de sonido y televisores plasma.

Bajo la gerencia general de la ingeniera Ariadna Andrade y la dirección comercial y operativa del ingeniero Vicuña, la empresa se ha convertido no solo en vendedora directa a consumidores finales, sino también en proveedora de diversas tiendas en la ciudad, provincia y región. Su enfoque no se limita solo a la venta, sino que también se centra en orientar a los clientes para satisfacer sus necesidades, cuidando su bienestar económico. Con un equipo capacitado, Yeray Electrodomésticos se destaca por ofrecer un servicio integral y de calidad.

4.4.2 Misión

Brindar un excelente servicio a nuestros clientes, ofreciendo productos de alta calidad, respetando el derecho del cliente y nuestro personal. Dándonos un lugar en el mercado por nuestros precios y generando al cliente un estándar de comodidad y facilidad para su vida.

4.4.3 Visión

Proporcionar soluciones de calidad a nuestros clientes, forjar alianzas beneficiosas y promover la responsabilidad social. Aspiramos a ser reconocidos no solo por nuestros productos, sino también por el impacto positivo que generaremos en la sociedad y en la vida de quienes confíen en nosotros.

4.4.4 Organigrama institucional

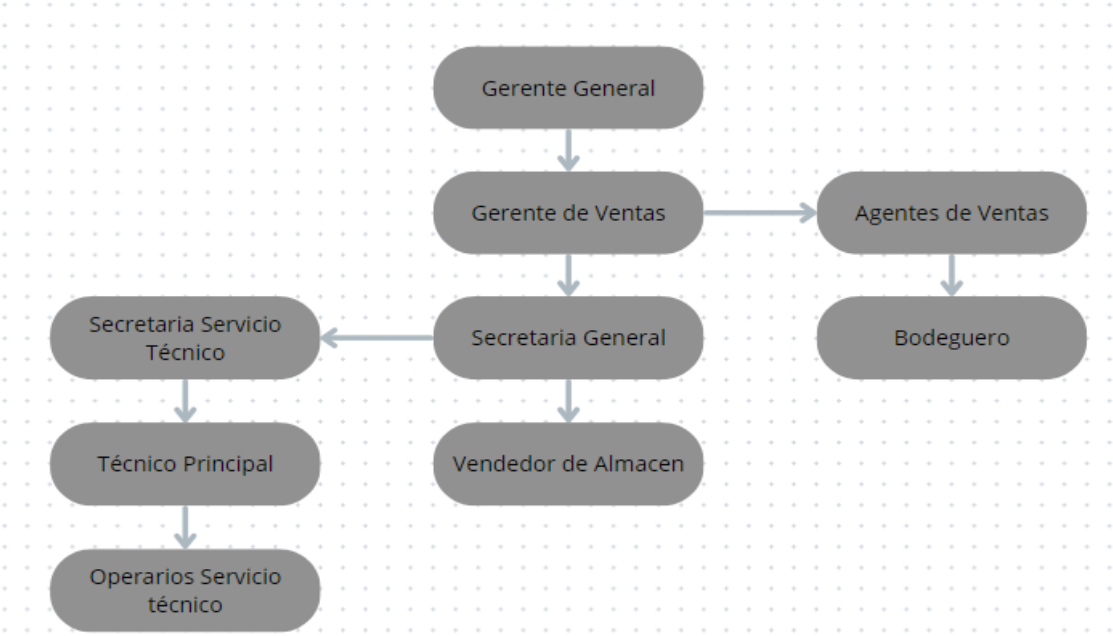


Ilustración 3. Organigrama empresarial

4.5 Etapas de acción para el desarrollo de la propuesta (auditoría)

4.5.1 Planificar

4.5.1.1 Programa de auditoría

Programa de Auditoría Informática: Gestión de seguridad de la información en Yeray Electrodomésticos		
Objetivos: • Evaluar la alineación de los controles de seguridad de la información implementados en Yeray Electrodomésticos con los requisitos establecidos por la norma ISO 27001. • Verificar el cumplimiento de las políticas y procedimientos de seguridad de la información en Yeray Electrodomésticos.		
Técnicas y procedimientos	**Referencia de papel de trabajo**	**Fecha**
Hacer un análisis sobre los lineamientos establecidos por la norma ISO 27001 fase 1.	**4.5.4**	
Diseñar instrumentos establecidos por la IS0 27001 para verificar el nivel de cumplimiento de requisitos de seguridad.	**4.5.7**	

Diseñar instrumentos de cumplimientos de controles de seguridad de la información según la ISO 27001.	**4.5.8**	
Aplicar instrumentos.	**4.5.9.1**	
Tabular datos.	**4.5.9.2**	
Analizar resultados.	**4.5.9.3**	
Informe final de auditoría.	**6.1**	
Elaborado por: David Andrade	**Revisado por:** A.S Wladimir Minaya. Mg	
Fecha:		

Tabla 7. Programa de auditoría

4.5.2 ISO 27001

La Norma UNE-ISO/IEC 27001, es otro producto de la Organización Internacional de Normalización" (en inglés, "International Organization for Standardization"). Esta dada con el fin de intervenir en el mundo de las tecnologías de la información, los sistemas de gestión de seguridad de información y las técnicas de seguridad de la información.

Esta norma se enfoca que, en establecer, gestionar, implementar, vigilar, conservar y los requisitos para la implantación y gestión de los SGSI, que se mantiene documentado según los requerimientos de exposiciones a riesgo de la organización. Esta norma puede ser aplicada a todo tipo de organización sean estas índole pública o privadas, pequeñas o multinacionales sin contemplar su actividad. Cabe mencionar que esta norma es certificable por lo tanto una organización certificada por la ISO 27001 asegura larga vida competitiva en el mercado y conserva de manera segura el mayor de los bienes actualmente que son los datos. (Fernández Sánchez, 2012)

4.5.3 Fases de la Norma ISO 27001

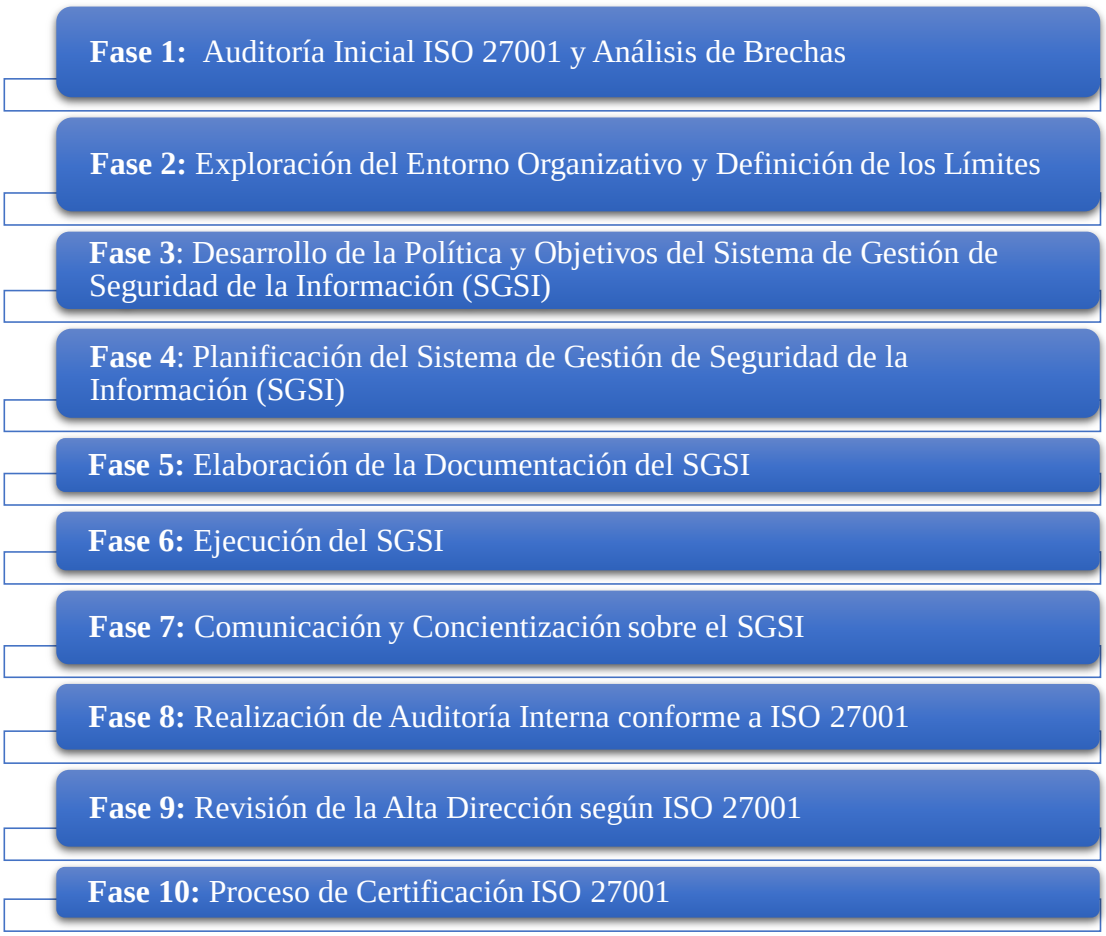


Ilustración 4. Fases ISO 27001

4.5.4 Fase 1 Auditoria Inicial ISO 27001

Dentro de la fase 1 de la norma ISO 27001, se centra en los inicios para la implementación de un Sistemas de Gestión de Seguridad de la Información (SGSI). En esta etapa se consideran cuáles serían los objetivos del SGSI, identificar los bienes críticos de la organización e identifican amenazas y vulnerabilidades asociadas a la empresa. En esta fase se debe conformar y establecer responsabilidades del equipo de trabajo destinado a la ejecución de estudios de factibilidad y e implementación del SGSI. En términos generales la fase 1 de norma ISO 27001, establece sus bases en el direccionamiento estratégico, compromiso y formar la estructura inicial que conlleve más adelante a la implementación del SGSI y que este tenga éxito en la organización. (Calder, 2013)

4.5.5 Análisis de brechas GAP

El análisis de brechas, o análisis GAP, es un método que compara el rendimiento actual de los sistemas de información o aplicaciones de una empresa con los requisitos del negocio. Busca identificar las diferencias entre el estado actual y los objetivos deseados, representando el "hueco" entre ambos. También conocido como análisis de necesidades, este enfoque ayuda a identificar deficiencias y determinar los recursos necesarios para alcanzar con éxito los objetivos, proporcionando una guía clara para cerrar esas brechas.

Esta evaluación se rige por dos objetivos fundamentales que son:

- Definir el punto de partida para poner en práctica la norma y valorar la inversión necesaria, al mismo tiempo que contar con una herramienta confiable para desarrollar un plan de implementación de ISO 27001.
- Sostener una herramienta para evaluar el nivel de integración de la norma a lo largo del proceso de implementación y medir el progreso del proyecto.

4.5.6 Requisitos evaluados

Ítems	Control	Detalles
4	Organización y su contexto	Evaluar el entorno operativo, identificar factores internos y externos que afecten la seguridad de la información, y analizar la misión, visión, valores y objetivos, así como las partes interesadas, para establecer eficientemente el alcance del Sistema de Gestión de Seguridad de la Información (SGSI).
5	Liderazgo	Capacidad de la alta dirección para proporcionar dirección y compromiso con el Sistema de Gestión de Seguridad de la Información. Se evalúa la claridad de políticas, asignación de responsabilidades y el fomento de una cultura de seguridad
6	Planificación	Implica la definición sistemática de objetivos, procesos y recursos necesarios para establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).
7	Soporte	Este elemento aborda la importancia de contar con el respaldo y la participación de la alta dirección, así como la asignación adecuada de recursos humanos, financieros y tecnológicos para garantizar el éxito y la efectividad del SGSI.

8	Operación	Se llevan a cabo las actividades diarias relacionadas con la seguridad de la información, incluyendo la gestión de accesos, la monitorización de eventos, la respuesta a incidentes, y la operación continua de los controles de seguridad.
9	Evaluación de desempeño	Determinar en qué medida se están cumpliendo los objetivos, metas y controles establecidos para la seguridad de la información. Incluye la revisión de indicadores clave de rendimiento (KPI) y la comparación de los resultados con las expectativas y requisitos predefinidos.
10	Mejora	revisar regularmente controles y procesos de seguridad, identificar oportunidades de mejora, actualizar políticas y procedimientos, realizar auditorías internas, y aplicar acciones correctivas y preventivas para fortalecer el SGSI de manera constante.

Tabla 8. Requisitos evaluados

4.5.7 Instrumento para evaluación de requisitos

Para la verificación del nivel de madurez de seguridad de la información presente en la empresa objeto de auditoría, toma en cuenta el cuestionario de cumplimiento de requisitos dado por la ISO 27001 que se detalla a continuación.

EQUISITO	CONTROL	PREGUNTA	NIVEL CUMPLIMIENTO	OBSERVACIONES
La ganización su contexto	Entendiendo la organización	¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?		
		¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de laInformación?		
		¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos parala seguridad de la Información?		
	Expectativas de las partes interesadas	¿Se han identificado las partes interesadas?		
		¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?		
		¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos,requisitos legales y requisitos contractuales?		
	Alcance del SGSI	¿se ha especificado el alcance del SGSI y se conserva información documentada?		
Liderazgo	Liderazgo y compromiso	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?		
		¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?		
		¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?		
	Política de la Seguridad de la Información	¿Se ha definido una Política de la Seguridad de la Información?		
		¿Se ha establecido un marco que permita el establecimiento de objetivos?		
		¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda laempresa?		
		¿Se mantiene información documentada de la política del SGSI y de sus objetivos?		
	Roles y Responsabilidades	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?		
		¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?		
anificación	Tratamiento de Riesgos y Oportunidades	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas enrelación con la Seguridad de la Información?		
		¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?		
		¿Se ha definido un proceso de tratamiento de riesgos?		
		¿Se mantiene información documentada de los puntos anteriores?		
	Planificación para consecución de objetivos	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivosdel negocio?		
		¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de laorganización teniendo en cuenta las funciones principales dentro de la Organización?		
		¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación		
	Recursos	¿Se identifican y asignan los recursos necesarios para el SGSI?		
	Competencia	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúantareas que puedan afectar a la seguridad?		

Tabla 9. Instrumento de requisitos evaluados

4.5.8 Instrumentos para evaluación de cumplimiento de controles

Los controles de seguridad son reglamentos que se enmarcan en conservar la seguridad de la información en las organizaciones, considerando todos los aspectos que la componen. Para evaluar su cumplimiento la ISO 27001, pone a consideración el siguiente cuestionario:

NUMERAL	CLAUSULA	ANEXO	REQUISITO	CUMPLE SI/NO	OBSERVACIONES
A5	Políticas de Seguridad de la Información	A5.1	¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?		
			¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?		
A6	Organización de la Seguridad de la Información	A6.1	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la empresa?		
			¿Se han dividido las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?		
			¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?		
			¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?		
			¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?		
	Dispositivos Móviles y Teletrabajo	A6.2	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?		
A7	Seguridad en los Recursos Humanos	A7.1	¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Verificar Titulación- Referencias		
			¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?		
		A7.2	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?		
			¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?		
			¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?		
		A7.3	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?		

Tabla 10. Instrumento cumplimiento de controles

4.5.9 Hacer

4.5.9.1 Aplicación

Tras la elaboración de los instrumentos necesarios para llevar a cabo la auditoría informática, los cuales se basaron en la guía proporcionada por la norma ISO 27001, se procedió a realizar una visita formal a la empresa YERAY ELECTRODOMESTICOS, sujeto de estudio. Durante esta visita, se coordinó una reunión con el representante de la empresa para abordar las preguntas contenidas en los cuestionarios.

La entrevista para la recopilación de datos, destinada a respaldar los objetivos de estudio, fue planificada para llevarse a cabo inicialmente en la oficina de quien gerencia la empresa. El propósito de esta fase era responder al cuestionario que evalúa el nivel de madurez en la gestión de seguridad. Sin embargo, el cuestionario de cumplimiento de controles se

respondió durante un recorrido por las instalaciones de la organización, con el objetivo de otorgar autenticidad a las respuestas obtenidas.

Esta estrategia fue implementada con el fin de obtener resultados objetivos que respalden el estudio en cuestión y que, en caso necesario, sirvan como base para formular recomendaciones de mejora.

Ilustración 5. Entrevista de evaluación de controles

4.5.9.1.1 Registro de información en el instrumento 1 nivel de cumplimiento de requisitos según la norma ISO 27001

Para documentar la información recopilada durante la ejecución de la auditoría inicial destinada a evaluar el nivel de madurez en la gestión de seguridad de la información en la organización, se empleó una hoja de Microsoft Excel. En dicha hoja, mediante el uso de fórmulas, se destacaron los diversos parámetros establecidos en los rangos de evaluación, como se ilustra en detalle a continuación:

REQUISITOS		PREGUNTA	CUMPLIMIENT	Promedio	Estado GAP	Brecha	ESTADO DE MADUREZ
4 La Organización y su Contexto	4.1 Entendiendo la Org	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	1	0,86	17%	83%	No cumple
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	1				
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	1				
	4.2 Expectativas de las	1.- ¿Se han identificado las partes interesadas?	2				
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	0				
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	0				
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	1				
5 Liderazgo	5.1 Liderazgo y compr	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	2	2,11	42%	58%	CUMPLE PARCIALMENTE
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	1				
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	1				
	5.2 Política de la Segur	1.- ¿Se ha definido una Política de la Seguridad de la Información?	3				
		2.- ¿Se ha establecido un marco que permita el establecimiento de objetivos?	4				
		3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	3				
		4.- ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	3				
	5.3 Roles y Responsab	1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	1				
		2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	1				

Ilustración 6. Tabulación información auditoría inicial

En la evaluación del cumplimiento de los requisitos establecidos en los controles de acuerdo con la norma ISO 27001, se implementó una escala de calificación que abarca desde 0 hasta 5. Esta escala se utilizó para asignar la puntuación correspondiente, reflejando así el grado de cumplimiento. Los detalles de esta calificación se encuentran detallados en la siguiente tabla:

Número del Nivel	Estado de cumplimiento	Detalles
0	Inexistente	No reconoce la importancia de establecer el control.
1	Ad-hoc	Se reconoce la necesidad del control peor, su aplicación es parcial a ciertas áreas.
2	Ejecutado	Cuentan con algunos controles definidos, pero no existe documentación de estos.
3	Definido	Se han establecido oportunamente los controles y se cumplen a cabalidad manteniendo la documentación de sus logros.
4	Medible	Existen los controles y su cumplimiento esta supervisado a interno de la organización.
5	Optimizado	Se gestiona a interno de la organización el cumplimiento de los requisitos establecidos en los controles, para los que se proponen metas de constantes mejoras.

Tabla 11. Escala de evaluación cumplimiento de requisitos.

Después de evaluar el nivel de cumplimiento de los requisitos con los valores detallados anteriormente, se procede a tabular y promediar estos datos. Esto da como resultado una cifra

porcentual que se clasifica en tres rangos definidos, los cuales describen el grado de cumplimiento de los requisitos dentro de la organización auditada.

Rangos % de nivel de cumplimiento	Descripción del estado
Menor a 1.65%	No cumple
De 1.66% a 3.25%	Cumple parcialmente
Mayor a 3.26%	Cumple los requisitos de la norma

Tabla 12. Rangos de estado del cumplimiento

4.5.9.1.2 Registro de información en el instrumento evaluador del cumplimiento de controles según la norma ISO 27001

En el proceso de registro de la información recopilada en la empresa sujeta a auditoría, se implementaron las evaluaciones proporcionadas por la norma ISO 27001. Estas evaluaciones fueron adaptadas de manera cuidadosa y pertinente a las particularidades de las actividades comerciales realizadas en la organización. Este enfoque permitió alinear de manera efectiva los estándares de la norma con los procesos específicos y las necesidades operativas de la empresa, garantizando así una evaluación integral del cumplimiento de los requisitos de seguridad de la información en el contexto de sus operaciones comerciales.

Numeral	Clausula		Requisito	CUMPLE
A5	Políticas de Seguridad de la Información	A5.1 Dirección de gestión para la seguridad de la información	1.- ¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?	1
			2.- ¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	0
A6	Organización de la Seguridad de la Información	A6.1	1.- ¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	1
			2.- ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	1
			3.- ¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	1
			4.- ¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	1
			5.- ¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?	0
		A6.2. Dispositivos y teletrabajo	1.- ¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?	0

Ilustración 7. Tabulación de datos auditoría

4.5.9.2 TABULACIÓN DE DATOS

Tras la consolidación de la información en las matrices de evaluación para verificar tanto el nivel de madurez como el cumplimiento de controles, se llevó a cabo un paso crucial mediante la tabulación de estos datos en hojas de cálculo en Microsoft Excel. El uso de hojas de cálculo en Excel resultó fundamental, ya que las fórmulas implementadas permitieron realizar cálculos automáticos, ofreciendo así una visión objetiva y exacta del estado de la empresa en cuanto al cumplimiento de la norma para la gestión de la información. Este enfoque no solo agilizó el proceso de análisis, sino que también proporcionó una plataforma robusta para la generación de gráficos representativos.

Con esta herramienta, se lograron obtener gráficos visuales que presentaban de manera clara y comprensible las cifras relacionadas con el cumplimiento de los controles establecidos por la norma ISO 27001. Estos gráficos no solo facilitaron la interpretación de los resultados, sino que también sirvieron como valiosos recursos para el análisis posterior y la toma de decisiones informadas en el ámbito de la seguridad de la información.

REQUISITOS		PREGUNTA	CUMPLIMIENTO	Promedio	Estado GAP	Brecha	ESTADO DE MADUREZ
4 La Organización y su Contexto	4.1 Entendiendo la Organiz	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	1	0,86	17%	83%	No cumple
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	1				
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	1				
	4.2 Expectativas de las par	1.- ¿Se han identificado las partes interesadas?	2				
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	0				
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	0				
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	1				
5 Liderazgo	5.1 Liderazgo y compromis	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	2	2,11	42%	58%	CUMPLE PARCIALMENTE
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	1				
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	1				
	5.2 Política de la Seguridad	1.- ¿Se ha definido una Política de la Seguridad de la Información?	3				
		2.- ¿Se ha establecido un marco que permita el establecimiento de objetivos?	4				
		3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	3				
		4.- ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	3				
	5.3 Roles y Responsabilida	1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	1				
		2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	1				

Ilustración 8. Matriz de tabulación de datos

4.5.9.3 ANALISIS DE RESULTADOS

4.5.9.3.1 Resultados generales instrumento para evaluar el nivel de madurez por el cumplimiento de requisitos

La norma ISO 27001 proporciona un marco normativo que orienta la implementación, gestión y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). En consonancia con estas directrices, se llevó a cabo una auditoría informática en la empresa Yeray

Electrodomésticos. Durante la evaluación para medir el nivel de madurez en el cumplimiento de los requisitos establecidos por la norma, se identificaron los resultados detallados en la tabla adjunta, donde se destacó una brecha significativa de incumplimiento de los requisitos, generando una situación de alerta en términos de seguridad de la información.

REQUISITO DE ISO 27001	Cumple la Norma	BRECHA
4. Organización y Contexto	17%	83%
5. Liderazgo	42%	58%
6. Planificación	40%	60%
7. Soporte	29%	71%
8. Operación	35%	65%
9. Evaluación y desempeño	49%	51%
10. Mejora	47%	53%
Promedio Requisitos	**37%**	**63%**

Tabla 13. Resumen resultados nivel de madurez

4.5.9.3.2 Resumen resultados instrumento de evaluación sobre cumplimiento de controles y anexos

Una vez sacado un general de los resultados sobre el cumplimiento de los controles establecidos por la norma ISO 27001 para una buena gestión de seguridad de la información, se obtiene los siguientes valores detallados en siguiente tabla; (***véase Tabla 13).***

En estos resultados se logra comprobar el problema con el cual se plateo el desarrollo de la presente auditoria en Yeray Electrodomésticos, ya que se evidencian controles con la totalidad de incumplimiento entre ellos uno altamente preocupante que involucra actividades para la continuidad del negocio en caso de incidentes de seguridad de la información. Dejando a notar un incumplimiento alto de los controles de seguridad de la información, evidenciando así vulnerabilidades con mayores probabilidades de materializarse dentro de la organización afectando sus actividades.

CLAUSULAS	%Cumplimiento	% no Cumple
A5 Políticas de Información	50%	50%
A6 Organización de Seguridad de la Información	67%	33%
A7 seguridad de los recursos humanos	71%	29%
A8 gestión de activos	50%	50%
A9 Control de acceso	43%	57%
A10 Criptografía	0%	100%
A11 Seguridad Física y del entono	42%	68%
A12 seguridad en las operaciones	50%	50%
A13 Seguridad en las comunicaciones	14%	86%
A14 Adquisición, desarrollo y mantenimiento de sistemas de información	20%	80%
A15 Relación con proveedores	40%	60%
A16 Gestión de incidentes de seguridad de la información	71%	29%
A17 Gestión de la Continuidad del Negocio	0%	100%
A18 Cumplimiento	0%	100%
PROMEDIO	***38%***	***62%***

Tabla 14. Resumen cumplimiento de controles.

CAPÍTULO V

5 INTRODUCCIÓN

El informe de auditoría representa el compendio formal resultante de un exhaustivo proceso de evaluación realizado en el seno de una organización. Su propósito es comunicar a las partes interesadas los hallazgos derivados de este estudio y proponer planes de acción para abordar y corregir las deficiencias identificadas, así como para fortalecer los controles existentes.

Durante este capítulo se resalta los puntos críticos de vulnerabilidad, también se identifican los puntos fuertes que podrían ser replicados o mejorados en otras áreas de la organización. De esta manera se proporciona una visión panorámica de la salud y la robustez del sistema de gestión de la seguridad de la información de la organización, destacando tanto sus logros como sus áreas de oportunidad.

5.1 EVALUACIÓ DE RESULTADOS

5.2 Informe final de auditoría

5.2.1 Dirigido a

Ing. Ariadna Angelica Andrade Farias

Gerente general de Electrodomésticos y Repuestos Yeray.

5.2.2 Motivo

Cumplir con los requisitos necesarios para concluir el trabajo de investigación en la modalidad de Proyecto Integrador, previo a la obtención del título de Ingeniero en Tecnologías de la Información.

5.2.3 Objetivo

- Evaluar la alineación de los controles de seguridad de la información implementados en Yeray Electrodomésticos con los requisitos establecidos por la norma ISO 27001.

- Verificar el cumplimiento de las políticas y procedimientos de seguridad de la información en Yeray Electrodomésticos.

5.2.4 Alcance

Para dar ejecución al presente estudio de auditoría sobre la gestión de seguridad de la información se aplicaron las técnicas y procedimientos detalladas a continuación:

Hacer un análisis sobre los lineamientos establecidos por la norma ISO 27001 fase 1.

- Diseñar instrumentos establecidos por la IS0 27001 para verificar el nivel de cumplimiento de requisitos de seguridad.
- Diseñar instrumentos de cumplimientos de controles de seguridad de la información según la ISO 27001.
- Aplicar instrumentos.
- Tabular datos.
- Analizar resultados.
- Informe final de auditoría.

5.2.5 Personal involucrado

Personal	Rol
Ing. Ariadna Andrade Farías	Gerente general (entrevista)
Lic. Jésica Cedeño	Secretaria (entrevista)
Colaboradores/empleados	Encuestados
David Andrade	Auditor

Tabla 15. Personal involucrado

5.2.6 Hallazgos

5.2.6.1 Nivel de madurez por el cumplimiento de los requisitos de la ISO 27001

Tras revisar los resultados obtenidos de la evaluación del estado de cumplimiento de los requisitos para determinar el nivel de madurez de seguridad de la información, se observa que la empresa conocida como Yeray Electrodomésticos presenta una brecha de seguridad significativa que supera las dos terceras partes de incumplimiento de los requisitos establecidos por la norma ISO 27001. Este hallazgo se refleja en el gráfico estadístico que se muestra a continuación.

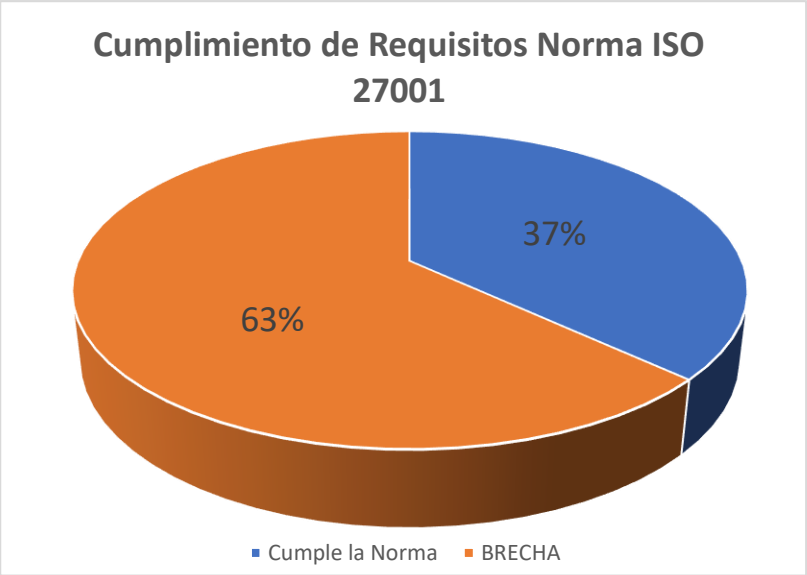
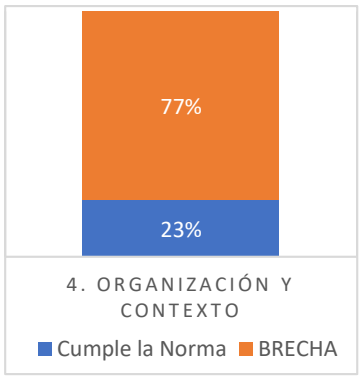


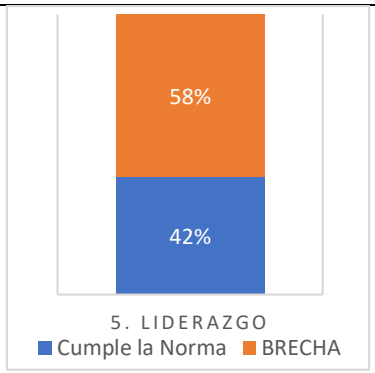
Ilustración 9. Resultados cumplimiento de requisitos

5.2.6.1.1 Análisis de cumplimiento de requisitos

Gráfico de resultados	Análisis
	En cuanto al cumplimiento de los requisitos que involucra parámetros en la razón de ser de la empresa contemplados en la organización y contexto se evidencia una amplia brecha de incumplimiento, los motivos que se encuentran en una baja calificación se detallan a continuación.

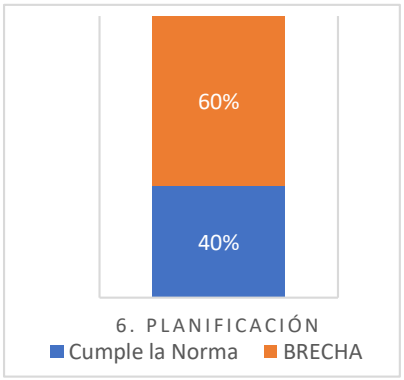
Motivos:

- No existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas.
- No cuentan con un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales.
- No están identificadas las cuestiones internas y externas relacionadas con la Seguridad de la Información.
- No se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información.
- No se ha determinado el alcance del SGS y se conserva información documentada.

Gráfico de resultados	Análisis
	En el contexto del liderazgo se observa que en la empresa objeto de auditoría existe un cumplimiento parcial de los requisitos establecidos. Sin embargo, entre los requisitos que cumple ninguno obtuvo la calificación perfecta de la tabla de valores considerados para la evaluación.

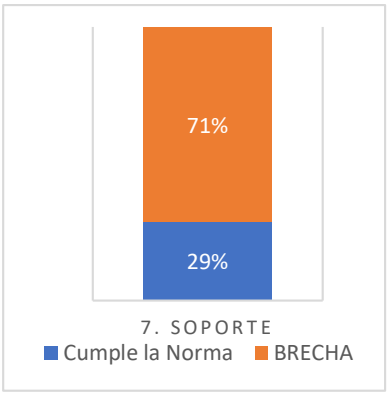
Motivos:

- La dirección no provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI.
- La dirección no revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI.
- No se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información.
- No se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información.

Gráfico de resultados	Análisis
	Los requisitos evaluados en el contexto de la planificación para un desarrollo adecuado y seguro en la organización revelan un estado de cumplimiento parcial como resultado, aún existen áreas que requieren atención y mejoras para garantizar un nivel óptimo de seguridad.

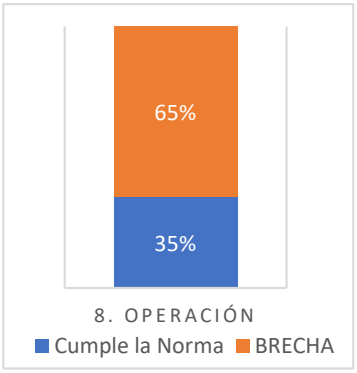
Motivos:

- No hay definido un proceso de tratamiento de riesgos.
- El plan para abordar riesgos y oportunidades no considera las expectativas de las partes interesadas en relación con la Seguridad de la Información.
- No se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos
- No se mantiene información documentada.

Gráfico de resultados	Análisis
	Al evaluar los ítems relacionados con las actividades de buenas prácticas de soporte, se observa un incumplimiento en los resultados obtenidos. Aunque este incumplimiento no es total, el nivel de madurez alcanzado se considera insuficiente según los rangos de evaluación establecidos para la respectiva calificación.

Motivos:

- No se identifican ni asignan los recursos necesarios para el SGSI.
- No se evalúa la competencia en materias de Seguridad de la Información.
- Información desactualizada sobre la competencia del personal.
- El personal no está involucrado ni es consciente de su papel en la Seguridad de la Información.
- No hay conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información.
- No se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno.
- No cuentan con proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información.
- No se controlan en su totalidad los documentos de origen externo.

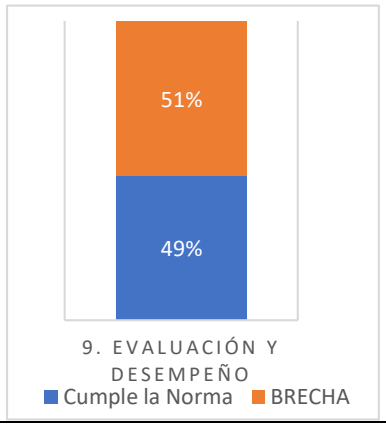
Gráfico de resultados	Análisis
	En el estado de cumplimiento de los requisitos para una operación efectiva, la empresa Yeray se encuentra en un nivel de cumplimiento parcializado. No obstante, la brecha identificada supera las dos terceras partes, lo que genera una alerta significativa debido al grado de discrepancia revelado.

Motivos:

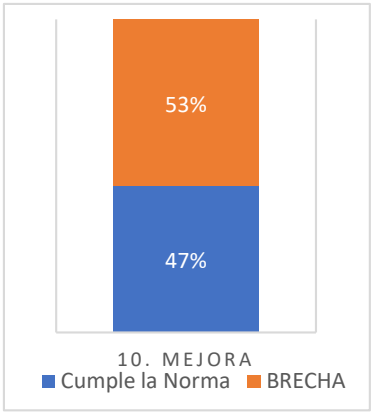
- No están documentados los procesos de seguridad de la Información para controlar que se realizan según lo planificado.
- No existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad.
- No establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados.

<table>
<tr><td colspan="2">

- No se identifican ni controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información.
- No se identifican todos los controles necesarios para mitigar el riesgo y justificar su aplicación.

</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>En los requisitos de evaluación y desempeño, el nivel de cumplimiento se califica como parcial, aunque con cierto optimismo al acercarse a la mitad de la totalidad óptima. Sin embargo, se observa un cumplimiento mínimo en todos los requisitos evaluados.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">

- No se ha establecido un proceso documentado para evaluar los resultados de las mediciones, ni se toman en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información.
- No se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información, ni se tienen en cuenta los controles para la seguridad de la información.
- No se consideran acciones correctivas ni propuestas de cambio en los informes de auditoría.

</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>El estado de cumplimiento de los requisitos de mejora se sitúa en un nivel parcial según la escala de calificación, donde solo se cumplen de manera relativa algunos de los ítems considerados.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">

- No existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora.
- No hay una diferenciación dentro de las acciones correctivas entre acciones correctivas sobre la no conformidad y sobre las causas de esta.

</td></tr>
</table>

Tabla 16. Análisis de resultados, nivel de cumplimiento de la norma

5.2.6.2 Cumplimiento de controles establecidos por la ISO 27001

La empresa Yeray Electrodomésticos muestra un incumplimiento considerable en los controles de seguridad de la información, de acuerdo con los requisitos establecidos por la norma ISO 27001. Se observa que más de la mitad de los controles evaluados no están siendo cumplidos. Además, se identifican controles específicos en los que no se está aplicando ningún tipo de medida, lo que subraya una deficiencia significativa en el establecimiento de medidas de seguridad adecuadas.

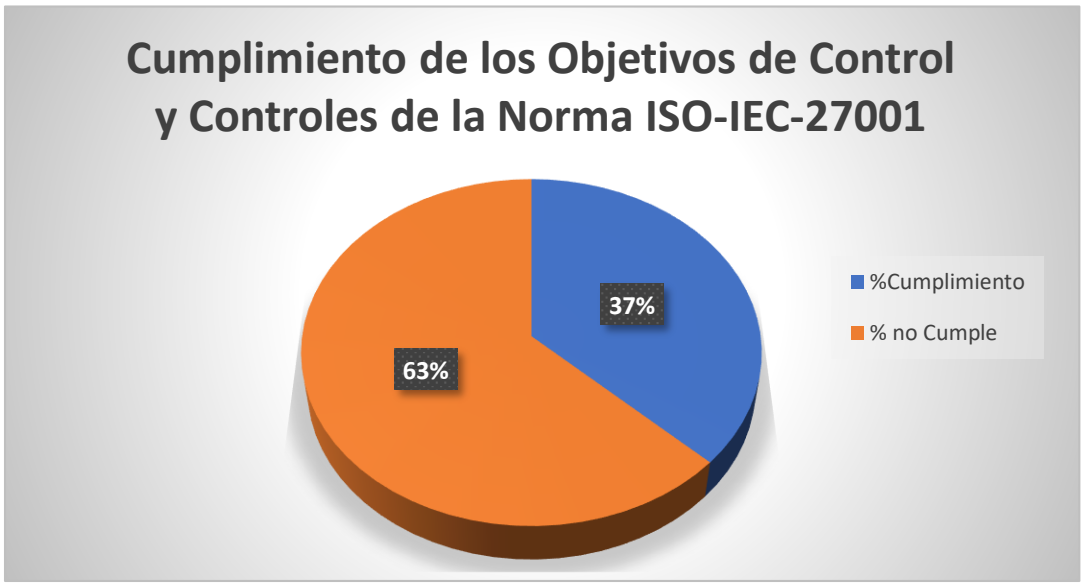
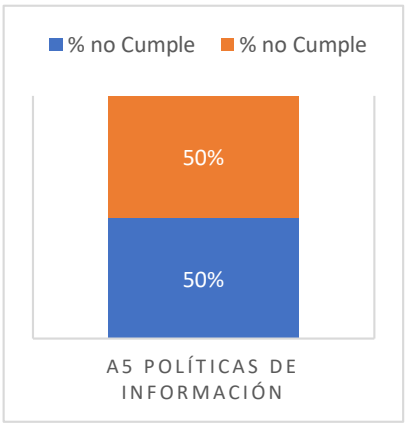
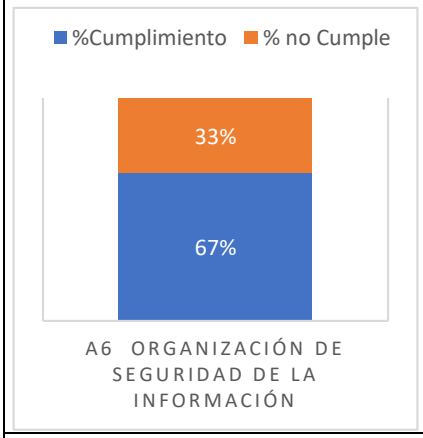
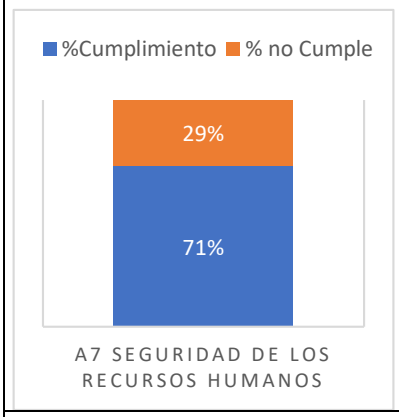
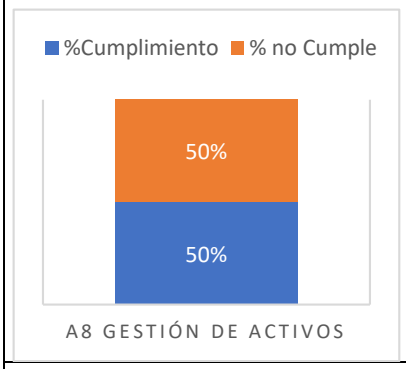
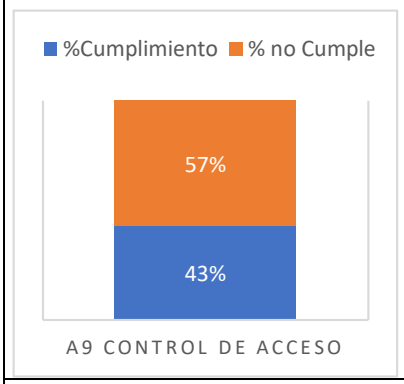


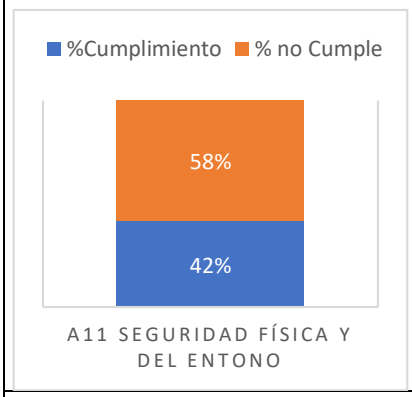
Ilustración 10.Resultados total controles evaluados.

5.2.6.2.1 Análisis cumplimiento de controles

Gráfico de resultados	Análisis
	En el anexo que evalúa las cláusulas relacionadas con el cumplimiento de controles para la seguridad de la información, se observa que la empresa auditada cumple en un nivel intermedio.

<table>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>El estudio de evaluación del cumplimiento de controles en el Anexo 6 de la ISO 27001 revela un grado de cumplimiento significativo que excede dos tercios del nivel requerido para la verificación.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización.
• No se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>En la verificación del cumplimiento de los controles relacionados con la seguridad de los colaboradores de la compañía, se observa un nivel de cumplimiento aceptable. Sin embargo, el índice negativo también refleja porcentajes que deben ser considerados seriamente.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato.
• No se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
</table>

<table>
<tr><td> 
</td><td>Se identifica un cumplimiento parcial de la mitad de los ítems considerados al evaluar los controles establecidos y su cumplimiento para una gestión efectiva de activos.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No se ha realizado un inventario de activos que den soporte al negocio y de información.
• No se ha identificado al responsable de cada activo en cuanto a su seguridad.
• No existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>Se evidencia un incumplimiento significativo de los controles evaluados dentro del Anexo A9, conforme a la norma ISO 27001, aplicada en Yeray Electrodomésticos.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo según las necesidades de cada actividad o puesto de trabajo.
• No se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados.
• No se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla, etc.
• No se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
</table>

<table>
<tr><td>
</td><td>Se detecta un incumplimiento total por parte de la empresa auditada en lo que respecta al anexo de controles de seguridad relacionados con la criptografía.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No existe una política para el establecimiento o uso de controles criptográficos.
• No hay un control del ciclo de vida de las claves criptográficas.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>Se identifica un nivel significativo de incumplimiento en los controles evaluados relacionados con la seguridad física y los entornos de la compañía, que excede la mitad de los ítems considerados según la normativa y la naturaleza de la actividad.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No se establecen perímetros de seguridad física donde sea necesario con barreras de acceso.
• Los equipos no están protegidos contra fallos de suministro de energía.
• No se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas, etc., en áreas accesibles al personal externo.
• No se planifican ni realizan tareas de mantenimiento sobre los equipos.
• No se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados.
• No se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo.
• No se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
</table>

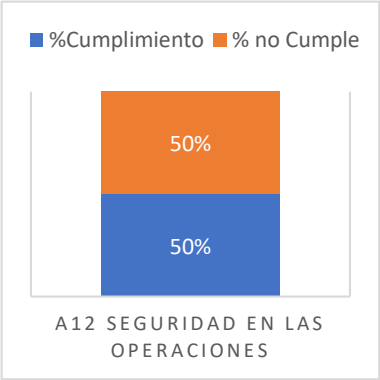
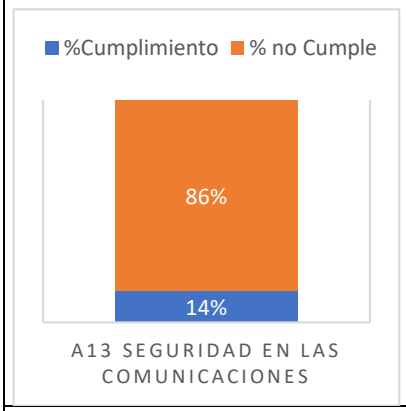
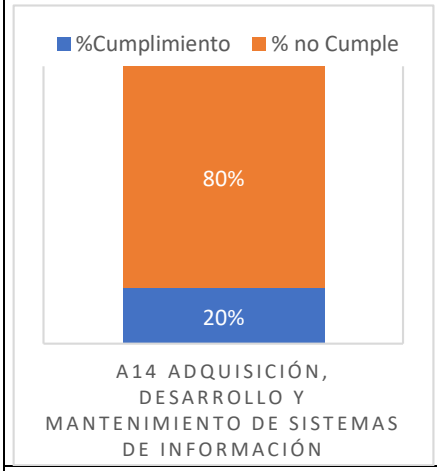
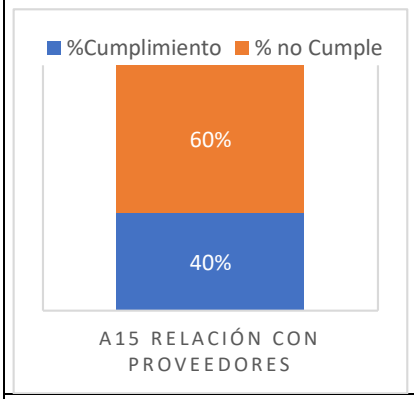
<table>
<tr><td> 
</td><td>La empresa evaluada demostró un cumplimiento considerable en los controles establecidos en el Anexo 12 sobre seguridad en las operaciones. Sin embargo, su índice global de cumplimiento se encuentra en una situación similar.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos.
• No existen sistemas de detección para Software malicioso o malware.
• No se realiza un registro de eventos, incluyendo intentos de acceso fallidos/exitosos, desconexiones del sistema, alertas de fallos, etc.
• Las instalaciones de nuevas aplicaciones SW o modificaciones no son verificadas en entornos de prueba y no existen protocolos de seguridad para su instalación.
• No se establecen métodos de control para vulnerabilidades técnicas como "hacking ético", etc.
• No existen mecanismos de auditorías de medidas de seguridad de los sistemas.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>En el anexo correspondiente a los controles de seguridad y comunicación, se evidencia un alto índice de incumplimiento en contraste con un escaso cumplimiento de estos controles de seguridad.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No se gestiona la protección de los sistemas en el entorno de red mediante controles de red y de elementos conectados.
• No se establecen condiciones de seguridad en los servicios de red, ya sean propios o subcontratados.
• No existe separación o segregación de redes considerando condiciones de seguridad y clasificación de activos.
• No se establecen políticas ni procedimientos para proteger la información en los intercambios.
• No se establecen normas o criterios de seguridad en la mensajería electrónica.
• No se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades.</td></tr>
</table>

Gráfico de resultados	Análisis
	Dentro de la evaluación del anexo dedicado a verificar el cumplimiento de controles para la adquisición de sistemas y mantenimiento, se ha identificado un incumplimiento que excede la segunda de las dos terceras partes de esta sección.

Motivos:

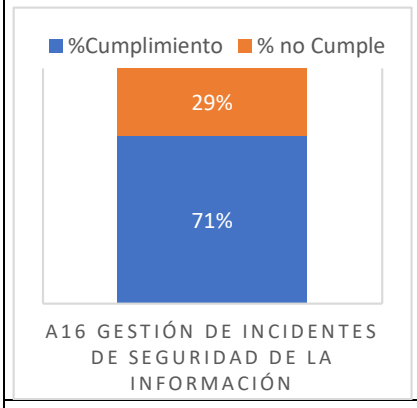
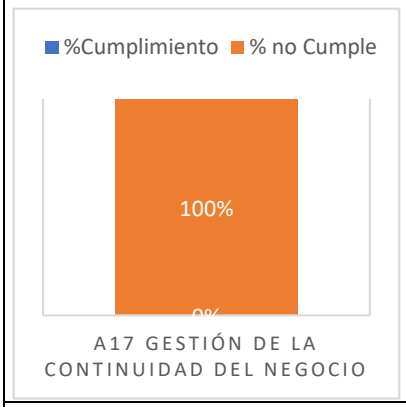
- No se definen ni documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información.
- No se gestiona el control de cambios en relación con el impacto que puedan tener en los sistemas.
- No se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información.
- No se establecen procedimientos de revisión después de efectuar cambios o actualizaciones.

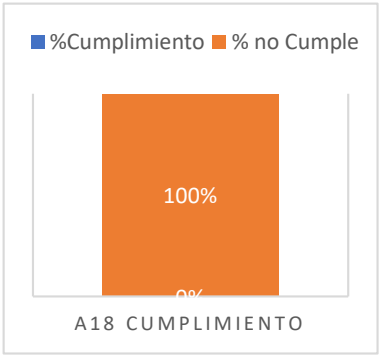
Gráfico de resultados	Análisis
	En el anexo A15, que aborda la evaluación de la seguridad de la información en las relaciones con los proveedores, se ha detectado un incumplimiento significativo que supera la mayoría de los criterios evaluados.

Motivos:

- No existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa.
- No se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos.
- No se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro.

Gráfico de resultados	Análisis

<table>
<tr><td> 
</td><td>El anexo A16 relativo a Yeray Electrodomésticos indica un cumplimiento mayoritario, aunque revela un nivel de incumplimiento que roza aproximadamente el tercio de la totalidad evaluada.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• La información proporcionada por los eventos en la Seguridad de la información no es tratada para tomar medidas preventivas.
• No existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
<tr><td> 
</td><td>El anexo 17 muestra un incumplimiento en la totalidad de los controles evaluados, lo que indica una situación preocupante en términos de la efectividad de los procesos relacionados con la seguridad y el cumplimiento de las políticas establecidas.</td></tr>
<tr><td colspan="2">Motivos:</td></tr>
<tr><td colspan="2">• No se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información.
• No se han implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio.
• No se han verificado ni probado las acciones previstas en el plan de Continuidad del Negocio.
• No se ha evaluado la necesidad de redundar los activos críticos de la Información.</td></tr>
<tr><td>Gráfico de resultados</td><td>Análisis</td></tr>
</table>

	En el anexo 18 se ha constatado un incumplimiento en todos los controles evaluados. Esto indica la necesidad de examinar detenidamente las causas y tomar medidas correctivas adecuadas.
Motivos:	
• No se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento. • No se revisan los controles de la Seguridad de la Información por personal independiente. • No se realiza una revisión periódica del cumplimiento de las políticas y controles de la Seguridad de la información. • No se llevan a cabo evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información.	

5.2.7 Opinión

5.2.7.1 Estado del cumplimiento de los requisitos establecidos por ISO 27001 para la seguridad de la información en Yeray Electrodomésticos

Tras la evaluación para medir el cumplimiento de los requisitos de la norma ISO 27001 en relación con las prácticas de gestión de seguridad, se identificó una brecha significativa del 63%. Ninguno de los siete parámetros evaluados alcanzó un cumplimiento del 50%. Este hallazgo revela un déficit preocupante en la seguridad de la empresa auditada, lo que aumenta el riesgo de vulnerabilidades que podrían resultar en perjuicios tanto para la compañía como para la información que maneja. Es fundamental abordar estas deficiencias de manera urgente para mitigar los riesgos potenciales y fortalecer la seguridad de la organización.

5.2.7.2 Cumplimiento de controles de seguridad establecidos por la ISO 27001 para una buena gestión de seguridad de la información en Yeray Electrodomésticos

De los trece anexos evaluados, segmentados en cláusulas que verifican el cumplimiento de los controles de seguridad para el manejo del Sistema de Gestión de Seguridad de la Información (SGSI), se observa que Yeray exhibe un incumplimiento del 100% en tres de los

anexos, abarcando todos los controles evaluados. En términos generales, la empresa presenta un nivel de cumplimiento del 37%, lo que indica una seguridad mínima establecida en la organización frente a un incumplimiento del 63% en los controles. Estos resultados señalan una preocupante vulnerabilidad en materia de seguridad informática que podría impactar negativamente en las operaciones económicas de la compañía si se materializa. Es crucial abordar estas deficiencias de manera urgente para garantizar la integridad de los activos de información de la empresa.

5.2.8 Conclusiones y recomendaciones de auditoría

5.2.8.1 Conclusiones

Se concluyó que Yeray Electrodomésticos tiene un nivel de cumplimiento de requisitos de la norma ISO 27001 calificado como BAJO. Esta evaluación se basó en el hecho de que todos los parámetros evaluados estaban por encima del nivel medio de incumplimiento, lo que indicaba deficiencias significativas en la implementación de los controles de seguridad.

5.2.8.2 Recomendaciones

Dada la situación evidenciada en el proceso de auditoría en Yeray, se recomienda la adopción del siguiente MANUAL DE POLÍTICAS DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE SEGURIDAD. ***(Véase Anexo D)*** Este manual tiene como objetivo mejorar la redacción y proporcionar directrices claras y efectivas para fortalecer la seguridad informática en la organización.

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Se identificó una discrepancia significativa entre el conocimiento del personal operativo y las percepciones de los administradores en relación con la seguridad de la información. La empresa enfrenta un claro conflicto en términos de comunicación y gestión de eventos relacionados con la seguridad de la información.

Existe un amplio conjunto de material bibliográfico actualizado que abarca información teórica y práctica relevante en diversas formas. Este material ha desempeñado un papel crucial como soporte teórico tanto para las variables dependientes como para las independientes en el contexto de esta investigación.

La empresa Yeray Electrodomésticos exhibe un nivel de cumplimiento mínimo en cuanto a requisitos y controles que mediamente contribuyen a una gestión adecuada de la seguridad de la información. En contraste, se detectaron niveles de incumplimiento que exceden el umbral establecido por la norma ISO 27001, lo que señala la presencia de brechas de seguridad clasificadas como de alta calificación, incluyendo los anexos de controles de seguridad.

Se pone a disposición de la organización sujeto de estudio un Manual de Políticas de Buenas Prácticas con el fin de mejorar los procesos internos relacionados con la gestión de seguridad de la información.

6.2 Recomendaciones

Después de completar el proceso de auditoría, se sugiere a la Ing. Ariadna Andrade, en su calidad de Gerente General de Yeray Electrodomésticos, adoptar el Manual de Políticas de Seguridad y compartirlo con todos los implicados en los procesos internos de la organización.

Es imperativo implementar medidas correctivas para abordar las deficiencias identificadas durante la auditoría, las cuales podrían estar causando interrupciones en las actividades de la empresa a corto plazo.

Se recomienda la capacitación del personal en el manejo adecuado de la información, especialmente aquella que contiene datos sensibles de clientes, productos y de la propia empresa.

Se insta a los representantes académicos de la extensión universitaria a proporcionar más oportunidades e información a las futuras generaciones de estudiantes, con el objetivo de sensibilizar sobre la importancia actual de la información para las organizaciones y las consecuencias potencialmente catastróficas de su vulnerabilidad frente a incidentes de seguridad.

7 REFERENCIAS BIBLIOGRÁFICAS

- Angel Palacios, V. B. (2018). Auditoría de seguridad informática a la Dirección Distrital 02D03 Chimbo-San Miguel-Educación, aplicando COBIT 5

- Arantes, S. C. (2023). Auditoría de seguridad informática. Ediciones de la U.

- Baca, G. U. (2016). Introducción a la seguridad informática. Grupo Editorial Patria.

- Bernal, C. A. (2006). Metodología de la investigación. Pearson Educación.

- Calder, A. (2013). ISO/IEC 27001:2013 - A Pocket Guide. IT Governance Publishing.

- Castro, M. I. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Área de Innovación y Desarrollo, S.L.

- Chicano Tejada, E. (2023). Gestión de incidentes de seguridad informática (2a ed.). IC Editorial.

- Chicano, E. T. (2015). Gestión de incidentes de seguridad informática. IC Editorial.

- Comamala, J. P. (2015). Auditoría. Editorial RA-MA.

- Cuenca, M. G. (2015). Modelo de gestión de seguridad de la información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001. Universidad Nacional de Loja UNL.

- Díaz, G. (2004). Seguridad en las comunicaciones y en la información. UNED - Universidad Nacional de Educación a Distancia.

- Fernández Sánchez, C. M. (2012). Modelo para el gobierno de las TIC basado en las normas ISO. AENOR - Asociación Española de Normalización y Certificación.

- Font, F. J. (2016). Las encuestas de opinión. Editorial CSIC - Consejo Superior de Investigaciones Científicas.

- García, E. L. (2012). Técnicas de investigación de campo y documental: basado en competencias. Grupo Editorial Éxodo.

- Gil, M. A., & Orueta, G. D. (2014). Procesos y herramientas para la seguridad de redes. UNED.

- Hernández, F. (2001). Investigación documental y comunicación científica. Universidad Abierta para Adultos (UAPA).

- León, I. H., & Garrido, J. T. (2007). Paradigmas y métodos de investigación en tiempos de cambios. CEC, S.A.

- Luca, M. A. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. IDICT, 21(2).

- Menéndez Arantes, S. C. (2022). Auditoría de seguridad informática: curso práctico. RA-MA Editorial.

- Plata, L. D. (2019). Cómo hacer un perfil proyecto de investigación científica. Palibrio.

- Pomaquero, R. L. (2022). Auditoría informática aplicando la norma ISO 27001 para optimizar la seguridad de la información en el Departamento de TICs del Centro de Investigación y Desarrollo FAE. Universidad Técnica de Ambato.

- Instituto Mexicano de Contadores Públicos. (2020). Guías de auditoría. Instituto Mexicano de Contadores Públicos.

- Rivas, G. A. (1988). Auditoría informática. Díaz de Santos.

- Rodríguez, P. I.-M.-N. (2021). Aportes para la implementación de la investigación en ciencias sociales. Editorial de la Universidad Pedagógica y Tecnológica de Colombia - UPTC.

- Sambrano, J. (2020). Métodos de investigación. Alpha Editorial.

- Sánchez Ch., W. (2021). Teoría de la auditoría. Grupo Editorial Nueva Legislación SAS.

- Sánchez, F. E.-G. (2017). La entrevista en las organizaciones (3a ed.). El Manual Moderno.

- Sevillano, F.-B. (2020). Dirección de seguridad y gestión del ciberriesgo. RA-MA Editorial.

- Tejada, E. C. (2023). Auditoría de seguridad informática. IFCT0109. IC Editorial.

- Torres, C. A. (2006). Metodología de la investigación para administración, economía, humanidades y ciencias sociales (2a ed.). Pearson Educación.

- Vieites, G. Á. (2015). Gestión de incidentes de seguridad informática. RA-MA Editorial.

ANEXOS

Anexo A. Reporte anti-plagio Urkund

CERTIFICADO DE ANÁLISIS
magister

David Anddrade Final compilatio

4% Textos sospechosos

4% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos

Nombre del documento: David Anddrade Final compilatio.docx
ID del documento: b1adfe3c25bf3361082858114480 8e100d8e9c8e
Tamaño del documento original: 7,02 MB

Depositante: RENELMO MINAYA MACIAS
Fecha de depósito: 27/7/2024
Tipo de carga: interface
fecha de fin de análisis: 27/7/2024

Número de palabras: 26.632
Número de caracteres: 179.919

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repository.unipiloto.edu.co** https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2643/Trabajo de grado.pdf?sequ... 67 fuentes similares	< 1%		Palabras idénticas: < 1% (231 palabras)
2	**openaccess.uoc.edu** https://openaccess.uoc.edu/bitstream/10609/132987/18/matiglacarcelTFM0621anexo2.pdf 57 fuentes similares	< 1%		Palabras idénticas: < 1% (184 palabras)
3	**www.e-certchile.cl** https://www.e-certchile.cl/ecert/site/docs/20200319/20200319104455/... po 01 politica general_... 65 fuentes similares	< 1%		Palabras idénticas: < 1% (155 palabras)
4	**ribuni.uni.edu.ni** http://ribuni.uni.edu.ni/3051/1/95597.pdf 24 fuentes similares	< 1%		Palabras idénticas: < 1% (126 palabras)
5	**Documento de otro usuario** #5d0367 El documento proviene de otro grupo 72 fuentes similares	< 1%		Palabras idénticas: < 1% (103 palabras)

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ EXTENSIÓN EN EL CARMEN
Uleam
COMISIÓN ACADÉMICA
EL CARMEN - MANABÍ

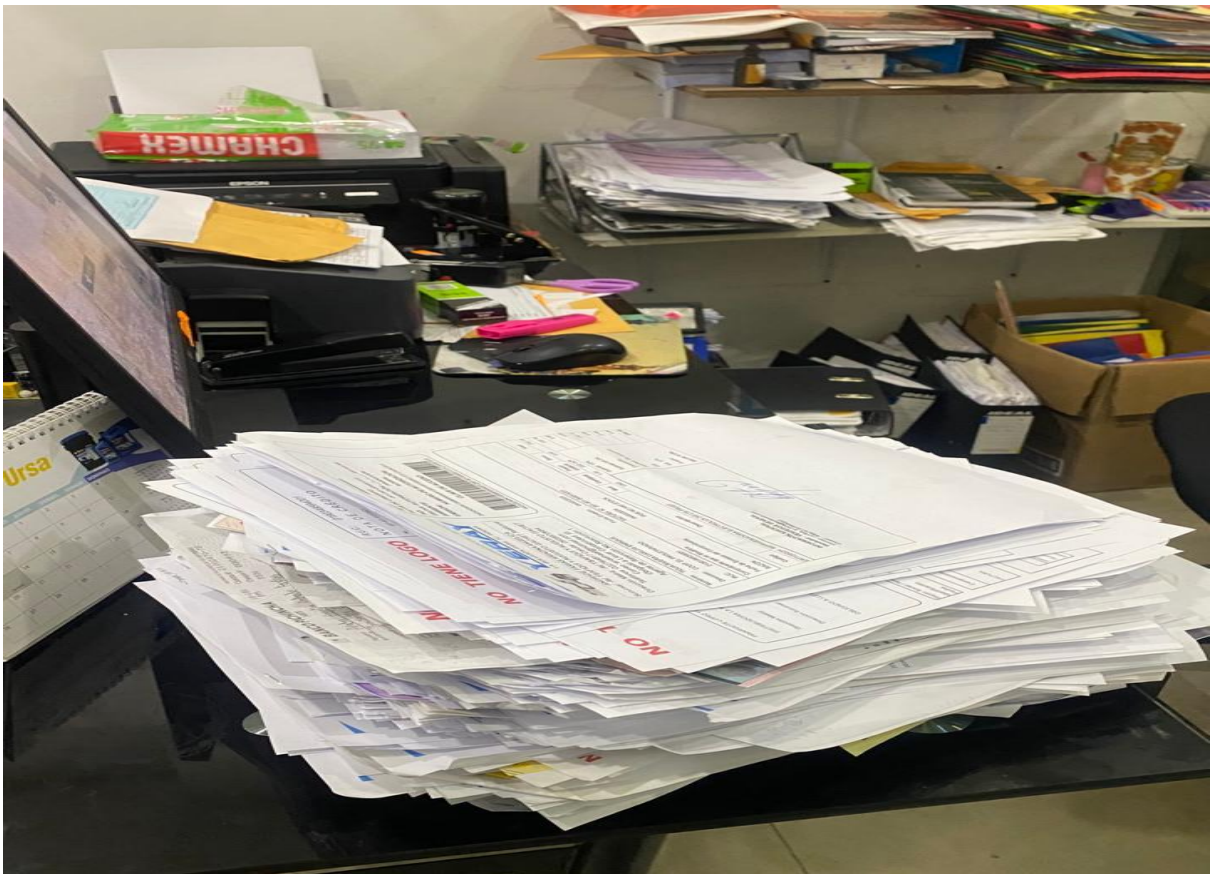
Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repositorio.espe.edu.ec** https://repositorio.espe.edu.ec/bitstream/21000/4279/3/T-ESPE-032634-A.pdf	< 1%		Palabras idénticas: < 1% (31 palabras)
2	**repositorio.utn.edu.ec** https://repositorio.utn.edu.ec/bitstream/123456789/15944/2/PG 1823 TRABAJO DE GRADO.pdf	< 1%		Palabras idénticas: < 1% (34 palabras)
3	**www.sunat.gob.pe** https://www.sunat.gob.pe/legislacion/superin/2023/ANEXO-SGSI-MA-03-000148-2023.pdf	< 1%		Palabras idénticas: < 1% (31 palabras)
4	**Documento de otro usuario** #c0a3fd El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (30 palabras)
5	**mmujica.files.wordpress.com** https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf	< 1%		Palabras idénticas: < 1% (28 palabras)

Fuentes ignoradas Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**David Anddrade Final compilatio.docx | David Anddrade Final compilatio** #c00b54 El documento proviene de mi biblioteca de referencias	100%		Palabras idénticas: 100% (26.632 palabras)
2	**normaiso27001.es | Implementar ISO 27001 paso a paso - 1 como hacer un Analisi...** https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/	8%		Palabras idénticas: 8% (2321 palabras)
3	**repositorio.pucesa.edu.ec** https://repositorio.pucesa.edu.ec/bitstream/123456789/3711/1/77995.pdf	6%		Palabras idénticas: 6% (1727 palabras)
4	**normaiso27001.es** https://normaiso27001.es/wp-content/uploads/2019/02/Test_cumplimiento_ISO_27001.pdf	5%		Palabras idénticas: 5% (1389 palabras)
5	**normaiso27001.es** https://normaiso27001.es/wp-content/uploads/2019/02/Test_cumplimiento_anexoA.pdf	5%		Palabras idénticas: 5% (1285 palabras)
6	**www.studocu.com | Desarrollo de proyecto(David A) CAP. III 13 - PORTADA UNIVE...** https://www.studocu.com/ec/document/universidad-laica-eloy-alfaro-de-manabi/taller-de-materiale...	2%		Palabras idénticas: 2% (502 palabras)

Anexo B. Fotografías



Imágenes tomadas en la oficina principal de la c la empresa auditada, evidencia parte del manejo de la información.

Anexo C. Aplicación de entrevistas

Ilustración 111. Entrevista a gerente Compañía

Ilustración 12. Entrevista secretaria general compañía

Anexo D. Manual de Políticas de buenas prácticas para la Gestión de Seguridad

Introducción

El Manual de Políticas de Buenas Prácticas en la Gestión de Seguridad de la Información en Yeray Electrodomésticos surge como resultado de una auditoría informática basada en la norma ISO 27001. La auditoría reveló que existen áreas de mejora significativas en los controles de seguridad de la empresa, lo que pone en riesgo la confidencialidad e integridad de los datos de la organización y de sus clientes.

El propósito principal de este Manual es proporcionar un marco de referencia claro y práctico para mejorar los procesos internos de seguridad de la información. Basado en las recomendaciones de la norma ISO 27001 y las mejores prácticas de la industria, este documento establece políticas y procedimientos diseñados para mitigar los riesgos identificados durante la auditoría. Se espera que la implementación de las medidas propuestas fortalezca la seguridad de la información de Yeray Electrodomésticos y proteja sus activos de posibles amenazas y vulnerabilidades.

Objetivo

Implementar un conjunto de políticas y procedimientos de seguridad de la información en Yeray Electrodomésticos, con el fin de fortalecer la protección de los activos de información de la empresa y garantizar la confidencialidad, integridad y disponibilidad de los datos sensibles ante posibles amenazas cibernéticas.

Alcance

Las directrices dadas en el presente Manual de Políticas en Yeray Electrodomésticos abarcan la definición e implementación de medidas de seguridad de la información en toda la organización. Esto incluye la creación de políticas y procedimientos relacionados con el manejo de datos sensibles, el acceso a la información, la gestión de contraseñas, la protección contra malware y ciberataques, así como la seguridad física y lógica de los sistemas de información.

Además, comprende la capacitación del personal en materia de seguridad de la información y la promoción de una cultura de seguridad dentro de la empresa. Este manual se aplicará a todos los empleados, contratistas y terceros que manejen información confidencial o sensible en Yeray Electrodomésticos.

Definición de términos

Acciones correctivas: Medidas tomadas para corregir y prevenir la repetición de no conformidades o problemas identificados en un sistema o proceso.

Acciones preventivas: Medidas proactivas tomadas para prevenir la ocurrencia de problemas, no conformidades o riesgos potenciales.

Auditoría de sistemas: Evaluación independiente de los sistemas informáticos y sus controles de seguridad.

Auditoría interna: Evaluación periódica de los controles internos y procesos de una organización.

Conciencia de seguridad: Conocimiento y comprensión de los riesgos y medidas de seguridad por parte de los empleados.

Controles de acceso: Medidas para regular y restringir el acceso a sistemas y datos.

Cortafuegos (Firewalls): Sistema de seguridad que controla el tráfico de red y previene accesos no autorizados.

Cifrado de información: Proceso de convertir datos en un código secreto para protegerlos de accesos no autorizados.

Cumplimiento de normativas: Adherencia a las leyes y regulaciones aplicables en materia de seguridad de la información.

Criptografía: Técnica de cifrado y descifrado de datos para garantizar su confidencialidad e integridad.

Evaluación: Proceso de análisis y valoración de la efectividad, eficiencia y cumplimiento de determinados aspectos o actividades dentro de una organización.

Evaluación de controles: Revisión y análisis de los controles de seguridad implementados para asegurar su eficacia.

Evaluación de riesgos: Identificación y análisis de posibles amenazas y vulnerabilidades en un sistema.

Eventos de seguridad: Sucesos que indican posibles amenazas o violaciones a la seguridad de la información.

Gestión de cambios: Proceso para controlar y gestionar cambios en sistemas y procesos de una organización.

Gestión de configuración: Control y seguimiento de los cambios realizados en la configuración de sistemas y software.

Gestión de contraseñas: Implementación de políticas y procedimientos para asegurar contraseñas seguras y su gestión adecuada.

Gestión de eventos: Proceso de monitorear y analizar eventos que ocurren en un sistema de información para detectar posibles incidentes de seguridad.

Gestión de incidentes: Proceso para detectar, responder y resolver incidentes de seguridad de manera efectiva.

Gestión de la seguridad: Proceso de planificar, implementar y mantener medidas para proteger la información.

Gestión de la seguridad de la información (SGSI): Marco estructurado de políticas, procedimientos y prácticas establecidos para dirigir y controlar una organización y lograr sus objetivos en materia de seguridad de la información.

Gestión de riesgos: Proceso de identificación, evaluación y gestión de los riesgos para minimizar su impacto y probabilidad de ocurrencia en una organización.

Gestión de sistemas: Proceso de administración y mantenimiento de los sistemas de información de una organización.

Gestión de vulnerabilidades: Proceso de identificación y gestión de debilidades en la seguridad de un sistema.

Malware: Software malicioso diseñado para dañar o infiltrarse en sistemas informáticos.

Métricas: Indicadores cuantitativos o cualitativos utilizados para medir y evaluar el desempeño, resultados o características de un proceso, sistema o actividad.

Mitigación: Acción de reducir la gravedad, intensidad o riesgo de un problema o situación.

Monitoreo continuo: Acción de observar y controlar de manera constante y regular el desempeño de un proceso, sistema o actividad.

No conformidad: Situación en la que un producto, servicio o proceso no cumple con los requisitos especificados.

Oportunidades de mejora: Situaciones identificadas que pueden ser objeto de acciones para mejorar la eficiencia, eficacia o calidad de un proceso, producto o servicio.

Planificación de la seguridad: Desarrollo de estrategias y planes para garantizar la seguridad de la información.

Plan de respuesta a incidentes: Documento que establece los procedimientos a seguir en caso de que ocurra un incidente de seguridad.

Política de buenas prácticas: Conjunto de reglas y directrices para promover comportamientos y acciones apropiadas en una organización.

Política de protección de datos: Conjunto de reglas y procedimientos para proteger la información personal.

Política de seguridad: Declaración formal que establece los principios, objetivos y responsabilidades en materia de seguridad de la información dentro de una organización.

Proceso de documentación: Actividad de registro y elaboración de documentos que describen los procesos, procedimientos y políticas de una organización.

Proceso de monitorización: Actividad continua de seguimiento y análisis de eventos y actividades para detectar posibles amenazas.

Proceso de tratamiento de riesgos: Actividad para identificar, evaluar y mitigar riesgos en un sistema de información.

Proceso documentado: Serie de pasos o actividades claramente definidos y registrados en documentos escritos que guían la realización de una tarea o actividad específica.

Protocolos de seguridad: Conjunto de reglas y estándares para garantizar la seguridad de las comunicaciones y transacciones.

Revisión periódica: Evaluación sistemática y regular de un proceso, sistema o actividad en intervalos de tiempo definidos para garantizar su eficacia y adecuación.

Segregación de funciones: Separación de responsabilidades dentro de una organización para evitar conflictos de interés y fraudes.

Seguridad física: Medidas para proteger los recursos físicos de una organización, como edificios y equipos.

Software malicioso: Programa diseñado para dañar o infiltrarse en sistemas informáticos.

Vulnerabilidad: Debilidad o fallo en un sistema o proceso que podría ser explotado por amenazas para comprometer la seguridad.

POLÍTICAS DE SEGURIDAD PARA ELEVAR EL NIVEL DE MADUREZ EN CUANTO AL CUMPLIMIENTO DE LOS REQUISITOS ESTABLECIDOS POR LA ISO 27001 ORIENTADO A CRITERIOS ESPECÍFICOS

POLÍTICAS PARA LA ORGANIZACIÓN Y SU CONTEXTO

Directrices:

a. Listado de Requisitos de Seguridad de las Partes Interesadas: Identificar y documentar los requisitos de seguridad de la información de todas las partes interesadas relevantes para la organización.
b. Listado de Requisitos Legales y Contractuales de Seguridad de la Información: Establecer un catálogo completo de los reglamentos, leyes y requisitos contractuales relacionados con la seguridad de la información que la organización debe cumplir.
c. Identificación de Cuestiones Internas y Externas de Seguridad: Implementar un proceso para identificar y evaluar cuestiones internas y externas que puedan afectar la seguridad de la información, como cambios en el entorno operativo y nuevas amenazas.
d. Identificación de Amenazas y Riesgos Asociados: Realizar un análisis de riesgos detallado para identificar cómo las partes internas y externas pueden representar amenazas o riesgos para la seguridad de la información.
e. Determinación del Alcance del Sistema de Gestión de Seguridad: Definir claramente el alcance del Sistema de Gestión de Seguridad de la Información, incluyendo los límites del SGSI y la documentación necesaria para respaldarlo.

POLÍTICAS PARA EL LIDERAZGO

Provisión de Recursos Materiales y Humanos:

a. Asignar un presupuesto adecuado para la seguridad de la información.
b. Contratar personal capacitado en seguridad de la información si es necesario.
c. Adquirir herramientas y tecnologías de seguridad adecuadas.

Revisión Directa de la Eficacia del SGSI:

a. Establecer revisiones periódicas programadas del SGSI por parte de la dirección.
b. Definir indicadores clave de rendimiento (KPI) para evaluar la eficacia del SGSI.
c. Designar a un equipo responsable de realizar auditorías internas regulares del SGSI.

Asignación de Responsabilidades y Autoridades:

a. Definir claramente los roles y responsabilidades del responsable de seguridad de la información y otros actores clave.
b. Documentar las responsabilidades y autoridades en un organigrama de seguridad de la información.
c. Establecer canales claros de comunicación y reporte para las actividades relacionadas con la seguridad de la información.

Comunicación Efectiva de Responsabilidades y Autoridades:

a. Desarrollar y distribuir un manual de políticas de seguridad de la información que detalle las responsabilidades y autoridades.
b. Realizar sesiones de capacitación periódicas para todos los empleados sobre las políticas y procedimientos de seguridad de la información.
c. Integrar la seguridad de la información en la cultura organizacional mediante campañas de concientización y reconocimiento del cumplimiento de las políticas de seguridad.

POLÍTICAS PARA UN BUEN LIDERAZGO

Implementar un Proceso de Tratamiento de Riesgos:

a. Se recomienda establecer un proceso formal y documentado para el tratamiento de riesgos en relación con la seguridad de la información. Esto incluiría la identificación, evaluación, tratamiento y monitoreo continuo de los riesgos.

Considerar Expectativas de las Partes Interesadas:

a. Es importante incorporar las expectativas de las partes interesadas relacionadas con la seguridad de la información en el plan para abordar riesgos y oportunidades. Se recomienda establecer canales de comunicación para recopilar y considerar estas expectativas durante el proceso de gestión de riesgos.

Adoptar un Método Estructurado para Identificar y Analizar Riesgos:

a. Se sugiere implementar un método estructurado y documentado para identificar y analizar los riesgos de seguridad de la información. Esto podría incluir el uso de técnicas reconocidas de evaluación de riesgos, como análisis cualitativos y cuantitativos, y establecer criterios claros para la aceptación o mitigación de los riesgos identificados.

Establecer un Sistema de Gestión Documental:

a. Recomendamos implementar un sistema de gestión documental para mantener información detallada sobre los riesgos identificados, las medidas de mitigación y los resultados de las evaluaciones de riesgos. Esto garantizará la disponibilidad y accesibilidad de la información relevante para la toma de decisiones y el seguimiento continuo de los riesgos de seguridad de la información.

POLÍTICAS PARA LA PLANIFICACIÓN

Establecimiento de un Proceso de Tratamiento de Riesgos:

a. Desarrollar un procedimiento sencillo y práctico que detalle cómo identificar, evaluar y abordar los riesgos de seguridad de la información de manera regular.

b. Designar un responsable encargado de coordinar y ejecutar el proceso de tratamiento de riesgos, utilizando herramientas accesibles y fácilmente comprensibles.

Consideración de las Expectativas de las Partes Interesadas:

a. Realizar reuniones periódicas con representantes de las partes interesadas para recopilar sus expectativas y necesidades en relación con la seguridad de la información.
b. Integrar las expectativas identificadas en el plan de gestión de riesgos de forma clara y práctica, asegurando que sean comprensibles para todos los involucrados.

Adopción de un Método Estructurado de Evaluación de Riesgos:

a. Utilizar plantillas o herramientas simples para identificar y analizar los riesgos de seguridad de la información, como listas de verificación o matrices de riesgos.
b. Capacitar al personal en la aplicación de un enfoque básico de evaluación de riesgos, centrándose en la identificación de amenazas comunes y posibles impactos en la seguridad de la información.

Mantenimiento de Información Documentada:

a. Implementar un sistema de archivos electrónico o físico que facilite el almacenamiento y la recuperación de la información relacionada con la gestión de riesgos.
b. Establecer un procedimiento claro para documentar las acciones tomadas para abordar los riesgos de seguridad de la información, garantizando la trazabilidad y transparencia en el proceso.

POLÍTICAS PARA BRINDAR UN BUEN SOPORTE

Directrices:

a. Asignar un responsable para la gestión de recursos del SGSI y garantizar la identificación y asignación adecuada de los recursos necesarios.
b. Realizar evaluaciones regulares de la competencia del personal en seguridad de la información y proporcionar formación según sea necesario.

c. Mantener registros actualizados sobre la competencia del personal en seguridad de la información.
d. Fomentar la participación del personal en iniciativas de seguridad de la información y comunicar claramente sus roles y responsabilidades.
e. Impartir programas de sensibilización sobre los riesgos de no seguir las políticas de seguridad de la información.
f. Establecer canales efectivos de comunicación para difundir la política de seguridad de la información y las responsabilidades asociadas.
g. Implementar un sistema de reporte confidencial para informar sobre deficiencias en seguridad de la información.
h. Establecer procedimientos para el control integral de documentos de origen externo relevantes para el SGSI.

POLÍTICAS PARRA MEJORAR LAS OPERACIONES

Directrices:

a. Documentar todos los procesos de seguridad de la información para garantizar su ejecución según lo planificado y su actualización constante.
b. Realizar una evaluación exhaustiva de los riesgos en seguridad de la información antes de implementar cualquier cambio en el Sistema de Gestión o procesos relacionados.
c. Establecer medidas y planes específicos para mitigar los riesgos en seguridad de la información que puedan surgir como resultado de cambios realizados en el sistema de gestión o procesos de seguridad.
d. Identificar y controlar los procesos externalizados relacionados con la seguridad de la información para gestionar adecuadamente los riesgos asociados.
e. Identificar de manera exhaustiva los controles necesarios para mitigar los riesgos en seguridad de la información, justificando su aplicación en función de la evaluación de riesgos realizada.

POLÍTICAS PARA MEJORAR LOS PROCESOS DE EVALUACIÓN DE DESEMPEÑO

Evaluar resultados:

a. Implementar un procedimiento formal que especifique cómo se realizarán las evaluaciones de los resultados de las mediciones en seguridad de la información.
b. Involucrar a los responsables de los procesos y de la seguridad de la información en este proceso de evaluación para garantizar una revisión integral.

Monitoreo continuo:

a. Desarrollar un plan de monitoreo periódico de los aspectos clave de la seguridad de la información, estableciendo indicadores y métricas relevantes.
b. Hay que asegurar que se implementen controles efectivos para la seguridad de la información y que se monitoreen de manera regular para detectar y mitigar posibles riesgos.

Acciones correctivas:

a. Establecer un mecanismo para identificar y documentar las acciones correctivas sugeridas durante las auditorías de seguridad de la información.
b. Incluir en los informes de auditoría un apartado específico para registrar las propuestas de cambio que puedan mejorar la seguridad de la información y la eficacia del sistema de gestión.
c. Designar responsables para implementar estas acciones correctivas y propuestas de cambio, asegurando su seguimiento y cumplimiento.

POLÍTICAS PARA MEJORAR LOS PROCESOS DE MEJORA

Directrices:

a. Implementar un procedimiento formal para identificar y registrar oportunidades de mejora en el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando su revisión periódica y su integración en el ciclo de mejora continua.
b. Establecer una política que distinga claramente entre las acciones correctivas dirigidas a abordar la no conformidad y aquellas orientadas a tratar las causas subyacentes, garantizando una gestión eficaz de los problemas identificados en el SGSI.

POLÍTICAS PARA MEJORAR Y ELEVAR EL CUMPLIMIENTOS DE LOS CONTROLES DE SEGURIDAD ESTABLECIDOS POR LA NORMA ISO 27001.

POLÍTICAS PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN

Directrices:

a. Establecer un proceso planificado y verificable para revisar las políticas de Seguridad de la Información.
b. Designar responsables, desarrollar criterios claros para la revisión, implementar un sistema de seguimiento.
c. Realizar revisiones periódicas, verificar la efectividad de las revisiones y documentar los resultados para garantizar la mejora continua del proceso.

POLÍTICAS DE MEJORAS EN LA ORGANIZACIÓN Y SEGURIDAD DE LA INFORMACIÓN

Establecer Políticas de Seguridad de la Información para Proyectos:

a. Abordar la seguridad de la información en la gestión de proyectos, incluyendo roles y responsabilidades, controles de acceso, manejo de información confidencial y evaluación de riesgos.
b. Incorporar requisitos de seguridad en todos los procesos de gestión de proyectos, desde la planificación hasta la ejecución, asegurando evaluaciones de riesgos y controles adecuados.
c. Proporcionar capacitación sobre los riesgos y medidas de seguridad relevantes para el personal involucrado en proyectos.

Implementar Controles de Seguridad en Dispositivos Móviles:

a. Encriptación de datos, contraseñas seguras y restricciones de acceso.
b. Establecer procedimientos para la gestión de dispositivos móviles, definir procedimientos para la gestión y monitoreo de dispositivos móviles, como inventarios y auditorías periódicas.

c. Realizar campañas de concienciación para educar al personal sobre los riesgos y fomentar el cumplimiento de las políticas de seguridad.

POLÍTICAS DE MEJORAS EN LA SEGURIDAD EN CASO DE REMOCIÓN O RENOVACIÓN DE PERSONAL

Directrices:

a. Desarrollar un proceso documentado que asegure la protección de la información al cambiar de empleado, puesto de trabajo o al finalizar un contrato.
b. Incluir la transferencia o revocación de accesos, la entrega de activos de información y la revisión de responsabilidades.
c. Incorporar disposiciones específicas relacionadas con la seguridad de la información en los contratos de trabajo.
d. Estas cláusulas deben abordar la confidencialidad, el manejo de información sensible, las responsabilidades del empleado y las consecuencias por incumplimiento.

POLÍTICAS DE SEGURIDAD PARA LA GESTIÓN DE ACTIVOS

Directrices:

a. Establecer un proceso para identificar y catalogar todos los activos relacionados con el negocio y la información que respaldan. Esto incluye equipos, sistemas, datos, software y cualquier otro recurso relevante.
b. Asignar responsables específicos para cada activo en términos de su seguridad.
c. Los responsables deben ser identificados claramente y tener la autoridad y los recursos necesarios para proteger el activo de manera efectiva.
d. Desarrollar un procedimiento documentado para la devolución de activos prestados a terceros o al finalizar un puesto de trabajo o contrato.

POLÍTICAS DE SEGURIDAD PARA EL CONTROL DE ACCESO A LA INFORMACIÓN

Directrices:

a. Definir los controles de acceso a la información, considerando el principio de acceso selectivo según las necesidades específicas de cada actividad o puesto de trabajo.
b. Establecer accesos restringidos a recursos y necesidades de red según perfiles definidos.
c. Implementar procesos de inicio de sesión seguro que incluyan limitaciones en los intentos de acceso, control de la información en pantalla y otras medidas de seguridad.
d. Implementar controles rigurosos para la capacitación y perfil de las personas con permisos de administración, especialmente aquellos con perfiles bajos de seguridad.

POLÍTICAS DE SEGURIDAD PARA EL CONTROL DEL ENTORNO FÍSICO

Directrices:

a. Definir y delimitar áreas específicas dentro de la organización donde sea necesario implementar barreras de acceso físico para proteger los activos y la información sensible.
b. Implementar medidas de protección, como sistemas de respaldo de energía (UPS), para garantizar la continuidad operativa y la protección de los equipos ante posibles cortes de suministro eléctrico.
c. Establecer medidas de seguridad, como filtros de privacidad en pantallas y restricciones de acceso físico, en áreas de oficinas accesibles al personal externo para proteger la información sensible.
d. Desarrollar un plan de mantenimiento regular para los equipos, que incluya actividades programadas para garantizar su buen funcionamiento y seguridad.
e. Definir procedimientos claros para proteger o eliminar la información almacenada en equipos que han quedado obsoletos o van a ser reutilizados, evitando la exposición no deseada de datos sensibles.
f. Establecer directrices y normas para proteger la información en los equipos cuando los usuarios abandonan temporal o definitivamente su puesto de trabajo, incluyendo el bloqueo de sesión y el cifrado de datos.

POLÍTICAS DE MEJORAS PARA MANTENER LA SEGURIDAD EN LAS OPERACIONES

Directrices:

a. Establecer un procedimiento documentado para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos organizativos.
b. Implementar sistemas de detección de software malicioso o malware en todos los dispositivos y redes de la organización.
c. Mantener un registro detallado de eventos de seguridad, incluyendo intentos de acceso fallidos/exitosos, desconexiones del sistema y alertas de fallos.
d. Establecer un protocolo de verificación en entornos de prueba para nuevas aplicaciones de software o modificaciones antes de su implementación en entornos de producción.
e. Desarrollar métodos de control para identificar y mitigar vulnerabilidades técnicas, como realizar pruebas de penetración o "hacking ético".
f. Realizar auditorías periódicas de las medidas de seguridad implementadas en los sistemas de información para garantizar su efectividad y adecuación.

POLÍTICAS DE MEJORAS PARA MANTENER LA SEGURIDAD EN LAS COMUNICACIONES

Directrices:

a. Implementar controles de red y de elementos conectados para proteger los sistemas en el entorno de red, como firewalls y sistemas de detección de intrusos.
b. Definir condiciones de seguridad para los servicios de red, internos y subcontratados, abordando temas como el cifrado de datos y la autenticación de usuarios.
c. Separar las redes según criterios de seguridad y clasificación de activos para garantizar la protección de la información.
d. Establecer procedimientos de protección de la información durante los intercambios, incluyendo el cifrado de datos y la autenticación de extremo a extremo.
e. Establecer normas claras de seguridad para el uso de la mensajería electrónica, abordando aspectos como la autenticación de correos y la protección contra el phishing.

f. Implementar acuerdos de confidencialidad previos a los intercambios de información con otras entidades para garantizar la confidencialidad de los datos compartidos.

POLÍTICAS DE MEJORAS PARA MANTENER LA SEGURIDAD EN LAS ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Directrices:

a. Definir y documentar los requisitos de Seguridad de la Información para los nuevos sistemas, incluyendo aspectos como la confidencialidad, integridad y disponibilidad de los datos.
b. Gestionar el control de cambios, evaluando el impacto que puedan tener en los sistemas y asegurando que se implementen medidas de seguridad adecuadas.
c. Establecer requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información, incluyendo autenticación robusta y cifrado de datos.
d. Implementar procedimientos de revisión posteriores a los cambios o actualizaciones, para verificar la efectividad de las medidas de seguridad implementadas y corregir posibles fallos.

POLÍTICAS DE MEJORAS PARA MANTENER LA SEGURIDAD LAS TRANSACCIONESCON PROVEEDORES

Directrices:

a. Establecer una política de Seguridad de la Información para proveedores que accedan a activos de la empresa, definiendo claramente los requisitos de seguridad que deben cumplir y los procedimientos para su supervisión.
b. Implementar controles para monitorear los posibles impactos en la seguridad ante cambios en los servicios proporcionados por proveedores externos, asegurando que se realicen evaluaciones periódicas y se tomen medidas correctivas según sea necesario.
c. Fijar requisitos específicos para extender la seguridad de la información a toda la cadena de suministro, incluyendo la definición de estándares mínimos de seguridad que deben

cumplir todos los proveedores y la realización de auditorías regulares para verificar el cumplimiento.

POLÍTICAS DE MEJORAS PARA DAR MEJOR GESTIÓN A LOS INCIDENTES DE SEGURIDAD OCURRIDOS

Directrices:

a. Implementar un proceso de análisis de la información proporcionada por los eventos en la Seguridad de la Información, con el fin de identificar posibles amenazas y tomar medidas preventivas de manera oportuna.
b. Establecer un procedimiento para recopilar evidencias sobre los incidentes en la seguridad de la Información, incluyendo la documentación detallada de los eventos, las acciones tomadas y los resultados obtenidos para su posterior análisis y mejora continua.

POLÍTICAS DE MEJORAS PARA ASEGURAR LA CONTINUIDAD DEL NEGOCIO

Directrices:

a. Elaborar un plan de continuidad del negocio que incluya medidas específicas para hacer frente a incidentes de Seguridad de la Información, garantizando la disponibilidad y la integridad de los datos críticos.
b. Implementar las medidas de recuperación definidas en el plan de Continuidad del Negocio para restablecer las operaciones de manera eficiente y minimizar el impacto de los incidentes en la Seguridad de la Información.
c. Verificar y probar regularmente las acciones contempladas en el plan de Continuidad del Negocio para asegurar su efectividad y realizar ajustes según sea necesario.
d. Evaluar la necesidad de redundancia en los activos críticos de la Información para garantizar su disponibilidad y mitigar los riesgos asociados a posibles fallos o interrupciones.

POLÍTICAS DE MEJORAS PARA DAR CUMPLIMIENTO A LAS DIRECTRICES DE SEGURIDAD

Identificar y cumplir legislaciones de protección de datos personales

a. Establecer un proceso para identificar y mantenerse actualizado sobre las leyes y regulaciones relevantes de protección de datos.
b. Designar un responsable o equipo encargado de monitorear y garantizar el cumplimiento de estas leyes.
c. Implementar políticas y procedimientos para asegurar que se respeten los derechos de privacidad de los individuos en todas las actividades de procesamiento de datos.

Revisar controles de seguridad con personal independiente

a. Contratar a expertos externos o auditorías independientes para revisar regularmente los controles de seguridad.
b. Garantizar que los auditores externos tengan la experiencia y conocimientos necesarios en seguridad de la información.
c. Analizar y actuar sobre las recomendaciones proporcionadas por los auditores independientes para mejorar la efectividad de los controles de seguridad.

Revisar periódicamente el cumplimiento de políticas y controles de seguridad

a. Establecer un programa de revisión periódica de políticas y controles de seguridad internos.
b. Designar a un equipo interno o responsable encargado de llevar a cabo estas revisiones.
c. Documentar los hallazgos de las revisiones y tomar medidas correctivas para abordar cualquier incumplimiento o deficiencia identificada.

Evaluar regularmente el funcionamiento de medidas técnicas de protección

a. Implementar herramientas y sistemas de monitoreo continuo para evaluar la efectividad de las medidas técnicas de protección.
b. Establecer métricas y criterios claros para medir el rendimiento de las medidas técnicas de seguridad.
c. Realizar evaluaciones de vulnerabilidad y pruebas de penetración de forma regular para identificar y abordar posibles debilidades en la seguridad de la información.

GLOSARIO

Amenazas: Son posibles eventos o circunstancias que pueden causar daño a los activos de información.

Auditoría: Proceso sistemático de evaluación y verificación de los controles de seguridad y prácticas establecidas en una organización.

Auditor: Persona encargada de llevar a cabo una auditoría, evaluando y verificando los controles de seguridad de una organización.

Brecha Gap: Es la diferencia entre el estado actual de seguridad de la información de una organización y el estado deseado o requerido.

Ciclos Deming: Proceso de mejora continua que incluye planificar, hacer, verificar y actuar, utilizado para mejorar la eficacia y la calidad de los procesos.

Ciberataques: Acciones deliberadas llevadas a cabo para comprometer la seguridad de sistemas informáticos, redes o datos.

Ciberseguridad: Conjunto de medidas y prácticas destinadas a proteger los sistemas informáticos, redes y datos contra ataques cibernéticos.

Cifrado de Información: Proceso de convertir la información en un código secreto para protegerla contra accesos no autorizados.

Cobit 5.0: Marco de referencia para el gobierno y la gestión de tecnologías de la información en las organizaciones.

Controles: Medidas implementadas para mitigar riesgos y proteger los activos de información de una organización.

Datos: Representación simbólica de hechos, conceptos o instrucciones en forma adecuada para la comunicación, interpretación o procesamiento por parte de personas o sistemas.

Equipos: Dispositivos electrónicos utilizados para procesar, almacenar o transmitir información.

Firmware: Software almacenado en hardware que controla cómo opera ese hardware.

Firewall: Dispositivo de seguridad que controla y regula el tráfico de red entre redes separadas.

Gestión de Seguridad: Conjunto de actividades orientadas a proteger la información sensible de una organización.

Hardware: Componentes físicos de un sistema informático, como computadoras, impresoras, dispositivos de red, etc.

Hallazgos: Resultados identificados durante una auditoría que pueden requerir acción correctiva.

Incidentes de Seguridad: Eventos que pueden comprometer la confidencialidad, integridad o disponibilidad de los activos de información.

Información Digital: Datos en formato electrónico que pueden ser procesados, almacenados o transmitidos por sistemas informáticos.

Internet: Red global de computadoras interconectadas que permite el intercambio de información.

Inventario: Lista detallada de todos los activos de información y recursos de tecnología de la información de una organización.

ISO: Organización Internacional de Normalización, que establece estándares internacionales en diversas industrias.

Magerit: Metodología de análisis y gestión de riesgos de seguridad de la información utilizada en España.

Malware: Software malicioso diseñado para dañar, alterar o robar información de sistemas informáticos.

Matriz: Estructura organizada de datos dispuestos en filas y columnas.

Microsoft Excel: Aplicación de hoja de cálculo desarrollada por Microsoft.

Pegasus: Programa de espionaje informático desarrollado por una empresa de ciber inteligencia israelí.

Políticas de Seguridad: Directrices y procedimientos establecidos para proteger la información y los sistemas de una organización.

Programa de Auditoría: Plan detallado para llevar a cabo una auditoría, incluyendo los objetivos, alcance y actividades planificadas.

Redes: Interconexión de dispositivos informáticos y de comunicación que permite la transmisión de datos.

Requisitos ISO 27001: Conjunto de criterios y estándares establecidos por la norma ISO 27001 para un Sistema de Gestión de Seguridad de la Información (SGSI).

Riesgo: Probabilidad de que una amenaza se materialice y cause daño a los activos de información de una organización.

SGSI: Sistema de Gestión de Seguridad de la Información, marco de trabajo para gestionar y proteger la información de una organización.

Sistema Operativo: Software que controla la operación de hardware y permite a los usuarios interactuar con una computadora.

Software: Conjunto de programas, instrucciones y datos que controlan el funcionamiento de un sistema informático.

TICS: Tecnologías de la Información y la Comunicación, conjunto de tecnologías utilizadas para procesar, almacenar y transmitir información.

Vulnerabilidades: Debilidades o fallos en los sistemas, redes o aplicaciones que podrían ser explotados por amenazas para comprometer la seguridad.

Zitro: Plataforma de análisis de ciber inteligencia y detección de amenazas.