UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de una plataforma de protección de terminales para la seguridad de la información de la empresa IM SELVA SAC.

Tesis para optar el título profesional de:

INGENIERO DE SISTEMAS

CORTEZ VALVERDE, FRANCO JONAIKER

PUCALLPA - PERÚ

2024

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
COMISIÓN DE GRADOS Y TÍTULOS

ACTA DE EVALUACIÓN DE SUSTENTACIÓN DE TESIS N° 02-2025

GRADUANDO : CORTEZ VALVERDE, FRANCO JONAIKER

TEMA : ***"IMPLEMENTACION DE UNA PLATAFORMA DE PROTECCION DE TERMINALES PARA LA SEGURIDAD DE INFORMACION DE LA EMPRESA IM SELVA SAC"***

ASESOR : **Msc. OSCAR AMADO RUIZ TORRES**

CRITERIOS	PUNTAJE			
	3	2	1	0
I- PRESENTACION				
* MOTIVACION		X		
* TONO DE VOZ		X		
* CALIDAD DE MATERIAL AUDIOVISUAL		X		
II- DESARROLLO DE CONTENIDO				
* SECUENCIA		X		
* DOMINIO DE VOZ		X		
* USO ADECUADO DEL MATERIAL		X		
* VALIDEZ DE LOS HALLAZGOS		X		
III- ABSOLUCION DE PREGUNTAS				
* RESPONDE A LAS PREGUNTAS FORMULADAS POR EL JURADO		X		
IV- APORTE CIENTIFICO Y TECNOLOGICO				
* AL DESARROLLO DE LA COMUNIDAD		X		
* A LA PROFESION		X		

EVALUACION

- EXCELENCIA — 26 A 30 PUNTOS
- UNANIMIDAD — 21 A 25 PUNTOS
- MAYORIA — 16 A 20 PUNTOS
- DESAPROBADO — 15 A MENOS

CALIFICACION FINAL:
PUNTAJE : **20** / 30

CONCLUSIONES:
APROBADO POR : **MAYORIA**
DESAPROBADO POR :

JURADO EVALUADOR

Mg. ARTURO YUPANQUI VILLANUEVA
PRESIDENTE

Mg. CESAR AUGUSTO AGURTO CHERRE
MIEMBRO

Mg. EUCLIDES PANDURO PADILLA
MIEMBRO

M.SC. CLOTILDE RÍOS HIDALGO DE CERNA
SECRETARIA ACADÉMICA

PUCALLPA, 17 DE ENERO DEL 2025

2024-133

ACTA DE APROBACION DE PROYECTO DE TESIS

En la Ciudad Universitaria, a los 10 dias del mes MAYO del 2024 siendo horas 15:58:31. Los miembros del Jurado, declaran APROBADO POR UNANIMIDAD el PROYECTO DE INVESTIGACIÓN DE TESIS titulado:

IMPLEMENTACIÓN DE UNA PLATAFORMA DE PROTECCIÓN DE TERMINALES PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA IM SELVA SAC.

Presentado por el(la) Bachiller:

FRANCO JONAIKER CORTEZ VALVERDE

De la Escuela Profesional de:

INGENIERIA DE SISTEMAS

Siendo el Jurado Dictaminador, conformado por:

Presidente	: MG. ARTURO YUPANQUI VILLANUEVA
Primer Miembro	: MG. CESAR AUGUSTO AUGURTO CHERRE
Segundo Miembro	: MG. EUCLIDES PANDURO PADILLA
Asesor	: MG OSCAR AMADO RUIZ TORRES

Para dar fe de este proceso electrónico, el Vicerrectorado de Investigación de la Universidad Nacional de Ucayali - Pucallpa, mediante la Plataforma de Investigación se le asigna la presente acta y a partir de la presente fecha queda expedito para la ejecución de su PROYECTO DE INVESTIGACIÓN DE TESIS.

Pucallpa, MAYO de 2024

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE ING. DE SISTEMAS E ING. CIVIL
DECANATURA
Dr. Nilton Cesar Ayra Apac
DECANO(E)

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº V/0519-2024.

La Dirección de Producción Intelectual de la Universidad Nacional de Ucayali, hace constar por la presente, que el trabajo académico de investigación, titulado:

"**IMPLEMENTACIÓN DE UNA PLATAFORMA DE PROTECCIÓN DE TERMINALES PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA IM SELVA SAC.**"

Autor(es)	:	**CORTEZ VALVERDE, FRANCO JONAIKER**
Facultad	:	**INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL**
Escuela	:	**ING. DE SISTEMAS**
Asesor(a)	:	**M.Sc. RUIZ TORRES, OSCAR AMADO**

Presenta un **porcentaje de similitud de 5%,** verificado en el Sistema Antiplagio COMPILATIO,

De acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO, el cual indica que todo trabajo de investigación no debe superar el 10%. **En tal sentido, se declara, que el presente trabajo de investigación: Si Contiene un porcentaje aceptable de similitud,** procediéndose a emitir la presente Constancia de Originalidad de Trabajo de Investigación (COTI) a solicitud del asesor.

En señal de conformidad se firma y sella el presente documento.

Fecha: 01/10/2024

Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, Franco Jonaiker Cortez Valverde

Autor de la tesis titulada : Implementación de una plataforma de protección de terminales para la seguridad de la información de la empresa IM SELVA SAC.

Sustentada el año 2025

Asesor(a): Ruiz Torres, Oscar Amado

Facultad: Ingeniería de Sistemas e Ingeniería Civil

Escuela Profesional: Ingeniería de Sistemas

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 19 / 06 / 2025

Email: franco;97.09@gmail.com Firma: [signature]

Teléfono: 933523269 DNI: 73188527

DEDICATORIA

A mi madre, por haberme criado y educado con valores, virtudes y sobre todo a su apoyo constante que han sido mi mayor fortaleza. Este logro es tanto tuyo como mío. Gracias por ser mi guía, mi confidente, mi inspiración y mi refugio en cada paso de este camino.

AGRADECIMIENTO

A mi madre y amigos, que están a mi lado en cada momento de esta travesía. Gracias por creer en mí cuando yo dudaba, por todas las palabras de aliento y consejos llenos de comprensión. Este logro es una muestra de mi esfuerzo y dedicación que puse gracias a todos ustedes. Gracias, mamá, por ser mi pilar y mi ejemplo.

INDICE GENERAL

Pág.

DEDICATORIA.....vi

AGRADECIMIENTO vii

INDICE GENERAL.....viii

INDICE DE TABLAS xii

INDICE DE FIGURAS.....xiv

INDICE DE ANEXOS.....xv

RESUMEN xvi

ABSTRACT xvii

INTRODUCCIÓN xviii

CAPÍTULO I 19

PLANTEAMIENTO DEL PROBLEMA.....19

1.1. Descripción y fundamentación del problema.....19

1.2. Formulación del problema.....20

1.2.1 Problema general 20

1.2.2 Problemas específicos.....20

1.3. Objetivos de la investigación.....21

1.3.1 Objetivo general.....21

1.3.2 Objetivos específicos.....21

1.4. Justificación, importancia y limitaciones.....22

1.4.1 Justificación 22

1.4.2 Importancia.....23

1.4.3 Limitaciones.....23

1.5. Hipótesis.....24

1.5.1 Hipótesis general 24
1.5.2 Hipótesis específicas 24
1.6. Delimitaciones de la investigación 25
1.6.1 Delimitación espacial 25
1.6.2 Delimitación social 25
1.6.3 Delimitación temporal 25
1.6.4 Delimitación conceptual 25
1.7. Sistema de variables 26
1.7.1 Variable Plataforma de protección de terminales: 26
1.7.2 Variable Seguridad de la información: 26
1.8. Definición operacional de las variables 27
CAPÍTULO II 28
MARCO TEÓRICO 28
2.1. Antecedentes de la investigación 28
2.1.1. Antecedentes Internacionales 28
2.1.2. Antecedentes Nacionales 30
2.2 Bases teóricas 33
2.1.1. Seguridad de Terminales 33
2.3 Definición de términos básicos 41
CAPÍTULO III 43
METODOLOGÍA DE LA INVESTIGACIÓN 43
3.1. Metodología y técnicas utilizadas 43
3.1.1. Tipo de investigación 43
3.1.2. Nivel de investigación 43
3.1.3. Método de investigación 43

3.1.4. Diseño de la investigación 44
3.2 Población y muestra 44
3.2.1 Población 44
3.2.2. Muestra 44
3.3 Instrumentos de recolección de datos 45
3.4 Procedimiento de recolección de datos 45
3.5 Tratamiento de datos. 45
3.6 Grado de confiabilidad de los datos. 45
CAPÍTULO IV 46
SISTEMA DE PROTECCIÓN DE TERMINALES 46
4.1. La empresa 46
4.2. Desarrollo de fases 48
4.3. Implementar una solución para salvaguardar los activos digitales 62
CAPÍTULO V 68
RESULTADOS Y DISCUSIÓN 68
5.1. Resultados 68
5.2.1. Variable seguridad de la información 68
5.1.1 Procesamiento de datos de la dimensión iniciación 70
5.1.2 Procesamiento de datos de la dimensión planificación 72
5.1.3 Procesamiento de datos de la dimensión ejecución 74
5.1.4 Procesamiento de datos de la dimensión seguimiento 76
5.1.5 Procesamiento de datos de la dimensión cierre 78
5.2. Prueba de Hipótesis 79
5.2.1 Prueba de la hipótesis general 80
5.2.2 Prueba de la primera hipótesis especifica 83

5.2.3 Prueba de la segunda hipótesis especifica..... 85
5.2.4 Prueba de la tercera hipótesis especifica 87
5.2.5 Prueba de la cuarta hipótesis especifica 89
5.2.6 Prueba de la quinta hipótesis especifica..... 91
5.3. Discusión..... 93
CONCLUSIONES 101
RECOMENDACIONES..... 105
REFERENCIAS BIBLIOGRÁFICAS..... 107
ANEXOS..... 111

INDICE DE TABLAS

Pág.

Tabla 1: Matriz de operacionalización 27

Tabla 2: Fases SHSI……..47

Tabla 3: Actividades del SGSI 51

Tabla 4: Activo…….56

Tabla 5: Inventario de activos. 57

Tabla 6: Formato para validación de inventario de activos 57

Tabla 7: Probabilidad de ocurrencia..... 59

Tabla 8: Medición del impacto 59

Tabla 9: Calculo de nivel de riesgo 60

Tabla 10: Valoración del nivel de riesgo 60

Tabla 11: Distribución de frecuencia del pre y post test..... 68

Tabla 12: Distribución de frecuencia del pre y post test..... 70

Tabla 13: Distribución de frecuencia del pre y post test..... 72

Tabla 14: Distribución de frecuencia del pre y post test..... 74

Tabla 15: Distribución de frecuencia del pre y post test..... 76

Tabla 16: Distribución de frecuencia del pre y post test..... 78

Tabla 17:Prueba de normalidad de la hipótesis general 81

Tabla 18: Prueba de normalidad de la variable seguridad de la información 81

Tabla 19: Prueba t de Student para muestras relacionadas 82

Tabla 20:Toma de decisión de la hipótesis general 82

Tabla 21:Prueba de normalidad de la primera hipótesis especifica 83

Tabla 22: Toma de decisión de la prueba de normalidad de la dimensión iniciación. 83
Tabla 23: Prueba t de Student para muestras relacionadas 84
Tabla 24:Toma de decisión de la primera hipótesis especifica 84
Tabla 25:Prueba de normalidad de la segunda hipótesis especifica 85
Tabla 26: Toma de decisión de la prueba de normalidad de la dimensión planificación. 85
Tabla 27: Prueba t de Student para muestras relacionadas 86
Tabla 28:Toma de decisión de la segunda hipótesis especifica 86
Tabla 29:Prueba de normalidad de la tercera hipótesis especifica 87
Tabla 30: Toma de decisión de la prueba de normalidad de la dimensión ejecución. 87
Tabla 31: Prueba t de Student para muestras relacionadas 88
Tabla 32:Toma de decisión de la tercera hipótesis especifica 88
Tabla 33:Prueba de normalidad de la cuarta hipótesis especifica 89
Tabla 34: Toma de decisión de la prueba de normalidad de la dimensión seguimiento..... 89
Tabla 35: Prueba t de Student para muestras relacionadas 90
Tabla 36:Toma de decisión de la cuarta hipótesis especifica 90
Tabla 37:Prueba de normalidad de la quinta hipótesis especifica 91
Tabla 38: Toma de decisión de la prueba de normalidad de la dimensión cierre. 91
Tabla 39: Prueba t de Student para muestras relacionadas 92
Tabla 40:Toma de decisión de la quinta hipótesis especifica 92

INDICE DE FIGURAS

Pág.

Figura 1: Componentes claves de Seguridad 39

Figura 2: Esquema de red de datos 49

Figura 3: Análisis del estado actual..... 54

Figura 4: Endpoints 63

Figura 5: Equipo Firebox 64

Figura 6: Mosaico..... 65

Figura 7: Configuración de Zonas 65

Figura 8: Anadir red interna 66

Figura 9: interfaces 66

Figura 10: Barras porcentuales del pre y post test de la variable seguridad de la información..... 68

Figura 11: Barras porcentuales del pre y post test de la dimensión iniciación 70

Figura 12: Barras porcentuales del pre y post test de la dimensión planificación 72

Figura 13: Barras porcentuales del pre y post test de la dimensión ejecución 74

Figura 14: Barras porcentuales del pre y post test de la dimensión seguimiento..... 76

Figura 15: Barras porcentuales del pre y post test de la dimensión cierre 78

INDICE DE ANEXOS

Pág.

Anexo 1 Matriz de consistência..... 112

Anexo 2 Cuestionario de preguntas**,** para la recolección de datos 114

Anexo 3 Validación de los instrumentos por expertos..... 116

Anexo 4 Base de datos del pre test de la variable seguridad de la información 117

Anexo 5 Estructura de fichas para la aplicación de un Sistema de Protección de Terminales 117

RESUMEN

Toda empresa en la actualidad es consciente de que la información representa un activo clave, se le considera a ésta como un activo debido a la gran importancia que representa, pero no todas las organizaciones realizan acciones para garantizar la seguridad de los mismos, debido a ello es que muchos de estos activos se encuentran expuestos y las empresas pasan por situaciones problemáticas, por no contar como mecanismo de control. El objetivo de la presente investigación es implementar una plataforma de protección de terminales con la finalidad de mejorar la seguridad de la información tomando como guía la norma técnica peruana 27001:2014, y el involucramiento de los colaboradores involucrados en cada uno de los procesos de gestión de activos de información, con ello para poder preservar la integridad, disponibilidad de confidencialidad de los activos de información.

Palabras clave: Seguridad, activos, información, endpoint.

ABSTRACT

Every company today is aware that information represents a key asset, it is considered an asset due to the great importance it represents, but not all organizations take actions to ensure the security of these assets, due to this, many of these assets are exposed and companies go through problematic situations, due to not having a control mechanism. The objective of this research is to implement a terminal protection platform in order to improve information security using as a guide the Peruvian technical standard 27001:2014, and the involvement of the collaborators involved in each of the information asset management processes, thus being able to preserve the integrity, availability and confidentiality of information assets.

***Keywords**:* Security, assets, information, endpoint

INTRODUCCIÓN

En la actualidad debido al avance tecnológico las empresas invierten en herramientas tecnológicas para poder facilitar la gestión de sus actividades procesos de tareas, con la finalidad de que puedan transmitir la información con mayor velocidad, almacenar información para toma de decisiones; por ello, la información se ha convertido en uno de los activos más importantes los cuales deben ser gestionados de manera eficiente y segura, para evitar o minimizar las acciones que pueda atentar con la integralidad, confidencialidad y disponibilidad a través de un análisis adecuado de riegos y la aplicación de controles.

La presente investigación se encuentra organizada en capítulos los cual a continuación se describen.

- Capítulo I: Realidad problemática, Objetivos, Variables de investigación, Operacionalización, Hipótesis, importancia y limitaciones.
- Capitulo II: Marco teórico, Antecedentes, Bases teóricas y definición de términos básicos.
- Capitulo III: Metodológica de investigación, método, tipo, nivel y diseño de la investigación, población, muestra, recolección y tratamiento de datos.
- Capitulo IV: Proceso de análisis e implementación del almacén de datos.
- Capitulo V: Resultados de la investigación
- Capítulo VI: Conclusiones y Recomendaciones;
- Bibliografías y anexos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción y fundamentación del problema

Los datos y la información representan uno de los activos más valiosos para las organizaciones, gracias ello es capaz de tomar decisiones, ya sea a corto, mediano y largo plazo, permitiéndoles prosperar y competir en un mercado local, nacional e internacional.

La información es generada a partir del desarrollo de sus actividades internas en cada uno de sus procesos principales y de apoyo, Goyzueta (2023), identifica que la información también es obtenida a partir de la interacción con los clientes, socios estratégicos, proveedores, etc. y son almacenados en distintos formatos, ya sean a nivel físico como documentos impresos, formatos y de forma digital con el uso de los sistemas transaccionales, documentos, hojas de cálculo, pdfs, etc.

Ahora bien, para Estrada y Guadamud (2022), si esta información no cuenta con mecanismos de control es vulnerable a cambios maliciosos, borrado, espionaje por parte de los competidores, robo de datos a través de dispositivos electrónicos como las memorias flash, envió a través de correos electrónicos.

La empresa IM SELVA SAC, como organización que hace uso de tecnologías de la información, genera y procesa datos, los cuales se encuentran expuestos a los casos mencionados en el párrafo anterior, y esto se evidencia con argumentos de los propios trabajadores, como por ejemplo

en una ocasión hubo robo de información respecto a las importaciones que hace la empresa.

Por lo indicado, es de suma urgencia que se realice un análisis más detallado y presentar una solución a los incidentes mencionados; siendo esto en motivo y/o justificación principal de la presente investigación.

1.2. Formulación del problema

1.2.1 Problema general

¿Cómo la implementación de una Plataforma de Protección de Terminales mejora la seguridad de la información de la Empresa IM SELVA SAC?

1.2.2 Problemas específicos

- ¿Cuáles son los problemas respecto a la iniciación en los sistemas de información que corresponden a la mejora la seguridad de la información de la empresa IM SELVA SAC?
- ¿Qué características posee la planificación de las tareas y actividades para la mejora de seguridad de la información de la empresa IM SELVA SAC?
- ¿Cuáles con las actividades y tareas a implementarse para la mejora en la ejecución de la seguridad de la información de la empresa IM SELVA SAC?
- ¿De qué manera el seguimiento, control de medidas y acciones implementadas mejoran la seguridad de la información de la empresa IM SELVA SAC?

- ¿Qué características posee el cierre de la plataforma de protección de terminales para mejorar la seguridad de, la información de la empresa IM SELVA SAC?

1.3. Objetivos de la investigación

1.3.1 Objetivo general

Implementar una Plataforma de Protección de Terminales para la mejora de seguridad de la información de la empresa IM SELVA SAC.

1.3.2 Objetivos específicos

- Identificar los problemas respecto a la iniciación en los sistemas de información que corresponden para mejorar la seguridad de la información de la empresa IM SELVA SAC.
- Determinar las características que posee la planificación de la tares y actividades para mejorar de seguridad de la información de la empresa IM SELVA SAC.
- Implementar las actividades y tareas para mejorar la ejecución de la seguridad, de la información de la empresa IM SELVA SAC.
- Determinar las pautas de seguimiento, control de medidas y acciones para mejorar la seguridad de la información de la empresa IM SELVA SAC.
- Identificar las características de cierre de la plataforma de protección de terminales para mejorar la seguridad de la información de la empresa IM SELVA SAC.

1.4. Justificación, importancia y limitaciones

1.4.1 Justificación

Justificación teórica

La protección de Terminales son objetivos valiosos para los atacantes, ya que pueden proporcionar acceso a redes corporativas, datos confidenciales y recursos críticos. La protección de estos dispositivos se ha convertido en una prioridad para las organizaciones en la lucha contra las amenazas cibernéticas.

Justificación práctica

Una plataforma de protección de Terminales puede ayudar a reducir los riesgos asociados con posibles brechas de seguridad y proteger los activos digitales de una organización. Esto se logra mediante la implementación de medidas de seguridad avanzadas, como la detección y prevención de intrusiones, el control de aplicaciones y la protección contra malware y ransomware. La justificación práctica radica en la capacidad de la plataforma para proteger los datos, la propiedad intelectual y otros activos valiosos de la organización.

Justificación metodológica

La justificación metodológica implica realizar una exhaustiva revisión de la literatura científica y técnica existente sobre la protección de Terminales. Esto permitirá comprender el contexto actual, identificar

las tecnologías y enfoques más relevantes y establecer un marco de referencia teórico sólido para el estudio.

Justificación operativa

La justificación operativa radica en la capacidad de la plataforma de protección de Terminales para ser implementada y desplegada de manera eficiente en entornos operativos. Esto implica considerar aspectos como la compatibilidad con sistemas existentes, la facilidad de instalación, configuración y gestión, y la capacidad de adaptarse a las necesidades específicas de la organización.

1.4.2 Importancia

Esta investigación es de suma importancia porque con la implementación de una plataforma de protección de terminales en la empresa IM Selva SAC es fundamental para garantizar la seguridad de la información con la que cuenta, esta medida resulta crucial debido a que estará prevenido de ciberataques protegiendo los diversos dispositivos de las diferentes áreas, contra amenazas como malware, ransomware y phishing, evitando la pérdida de datos confidenciales.

1.4.3 Limitaciones

La investigación se vio condicionada por la imposibilidad del tesista de acceder a los recursos internos de la empresa, lo que obligó a desarrollar estrategias alternativas para recopilar la información pertinente. Esta situación implicó una mayor inversión de tiempo y esfuerzo en la búsqueda y análisis de fuentes externas, prolongando así el desarrollo del estudio.

1.5. Hipótesis

1.5.1 Hipótesis general

La Implementación de una Plataforma de Protección de Terminales mejora la seguridad de la información de la empresa IM SELVA SAC.

1.5.2 Hipótesis específicas

- La identificación de los problemas respecto a la iniciación en los sistemas de información mejora la seguridad de la información de la empresa IM SELVA SAC.
- Las características de la planificación de la planificación de la tares y actividades mejoran la de seguridad de la información**,** de la empresa IM SELVA SAC.
- La implementación de actividades y tareas mejoran la ejecución de seguridad de la información de la empresa IM SELVA SAC.
- Las pautas de seguimiento de seguimiento, control de medidas y acciones mejoran la seguridad de la información de la empresa IM SELVA SAC.
- Las características de cierre de la plataforma de protección de terminales identificadas mejoran la seguridad de la información de la empresa IM SELVA SAC.

1.6. Delimitaciones de la investigación

1.6.1 Delimitación espacial

Esta investigación se centra en la implementación de una plataforma de protección de terminales, para que el área de informática mantenga segura la información de la EMPRESA IM SELVA SAC.

1.6.2 Delimitación social

Esta investigación fortalece al estudiante egresado de la Escuela Profesional de Ingeniería de Sistemas de Sistemas, a encontrar a través de la investigación realizada, de solución a la problemática de la vulneración de la información, a la que constantemente las empresas con sometidas, esta solución será de gran ayuda a que la información sea bien protegida y no este corriendo riesgo de los ladrones cibernéticos.

1.6.3 Delimitación temporal

Esta investigación data del año 2024, y se desarrolló manteniendo la programación de actividades que es parte del plan de investigación, cumpliendo con los plazos establecidos por la Oficina de Grados y Títulos de la Facultad de Ingeniería de Sistemas**,** y de Ingeniería Civil.

1.6.4 Delimitación conceptual

Para el desarrollo de esta investigación se revisó los conceptos que se encuentran en las páginas web, artículos científicos, libros sobre seguridad informática, etc. Siendo estos analizados y tomando como base la forma como la empresa manejaba su sistema de seguridad informática, y así se dio solución al problema que presentaban.

1.7. Sistema de variables

1.7.1 Variable Plataforma de protección de terminales:

- Definición conceptual: Es una herramienta de protección que realiza protección en tiempo real inspeccionando y escaneando archivos tan pronto como ingresan a la red. El tipo más común de protección de terminales es una solución antivirus (AV) tradicional. Una solución antivirus incluye capacidades antimalware. Está diseñado principalmente para proteger contra ataques basados en firmas. Cuando el archivo ingresa a la red, la solución antivirus escanea los archivos para ver si la firma coincide con una amenaza maliciosa en la base de datos de inteligencia de amenazas (Cisco, 2024).
- Dimensiones: se dimensiona en cuatro procesos, 1) Evaluación, 2) Características, 3) Controles y, 4) Seguridad.

1.7.2 Variable Seguridad de la información:

- Definición conceptual: La seguridad de terminales es la práctica de proteger terminales o puntos de acceso en dispositivos de usuario final, como computadoras de escritorio, portátiles y dispositivos móviles. de perpetradores y actividades peligrosas Endpoint Security protege estos puntos finales en su red o nube de amenazas de ciberseguridad. La seguridad de los terminales ha evolucionado desde el software antivirus tradicional hasta brindar protección integral contra malware sofisticado y amenazas de día cero en evolución (Ruíz, 2022).
- Dimensiones: se enmarca en 5 factores, 1) Iniciación, 2) Planificación, 3) Ejecución, 4) Seguimiento y, 5) Cierre.

1.8. Definición operacional de las variables

Tabla 1: Matriz de operacionalización

Variable	Definición operacional	Dimensión	Indicador	Escala
Plataformas de Protección de Terminales	Las plataformas de protección de terminales se operacionalizan en cuatro dimensiones: 1) Evaluación, 2) Características, 3) Controles y, 4) Seguridad	Evaluación	• Soluciones de Protección de Terminales.	• Muy malo • Malo • Regular • Bueno • Muy bueno
		Características.	• Características de la solución de Protección de Terminales	
		Controles	• Configuraciones de controles de seguridad.	
		Seguridad	• Nivel de seguridad de los activos de TI.	
Seguridad de Información	Los sistemas de información, se fundamentan en cinco factores: 1) Iniciación, 2) Planificación, 3) Ejecución, 4) Seguimiento y, 5) Cierre.	Iniciación	• Problemas. • Roles.	• Muy malo • Malo • Regular • Bueno • Muy bueno
		Planificación	• Responsabilidades. • Control.	
		Ejecución	• Activos. • Políticas. • Riegos. • Controles	
		Seguimiento	• Indicadores	
		Cierre	• Conformidad.	

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes Internacionales

Según investigación de Guevara Tucta (2019), donde se propuso Implementar el SGSI bajo parámetros de la norma ISO/IEC 27001, para alcanzar el mejoramiento de la seguridad de la información en el Distrito 18D01 de Educación, y al finalizar se obtuvo las siguientes conclusiones: La protección física y ambiental hay procedimientos que se llevan a cabo por disposiciones de planta central y están enfocados en aspectos como ubicación y protección de los equipos pero se descuidan en gran medida apartados como el mantenimiento de equipos, los perímetros de seguridad física, los controles físicos de entrada, etc. Con esto se expone la integridad de los equipos y del personal. Relacionado a la gestión de comunicaciones y las operaciones se gestiona la misma. Gracias a las restricciones y parámetros de seguridad de sistemas institucionales, los archivos y documentos se están correctamente respaldados y documentados. El problema en la falta de seguridad de la red interna es un blanco fácil ante ataques informáticos. No se gestiona el control de accesos. Por una parte, las claves de usuarios no se modifican periódicamente y no es posible verificar.

Según investigación de Hernández Pinto (2019), con título: “Diseño de un Plan**,** Estratégico de Seguridad de Información en una empresa

del sector comercial", y al finalizar se obtuvo las siguientes conclusiones: 1. Las herramientas de tecnología evolucionan con el pasar del tiempo y aumenta también la inseguridad, convirtiéndose así en objeto de amenazas. 2. Actualmente la empresa posee la necesidad de utilizar esquemas de seguridad fuertes, que le permitan una mayor confiabilidad de la información para la toma de decisiones. 3. La falta de compresión de la Gerencia que conlleva a la falta de apoyo a la gestión de informática que limita la implantación de las medidas de seguridad, provocando que la entidad tenga una mayor exposición a los riesgos. 4. La SI es responsabilidad compartida de los niveles de la organización, que requiere del apoyo de cada uno de ellos.

Según investigación de ALVAREZ BASALDÚA (2018), con título: "SEGURIDAD EN INFORMÁTICA (AUDITORÍA DE SISTEMAS)", al finalizar se obtuvo las siguientes conclusiones: Los servicios de auditoría comprenden el estudio de sistemas para gestionar las vulnerabilidades que están presentes en los sistemas. Después de su localización, las anomalías se deben documentar, se debe informar de los resultados a cada responsable y establecer medidas proactivas, siguiendo un proceso secuencial garantizando que los sistemas mejoren la seguridad aprendiendo de los errores ocurridos en el pasado. Las auditorías permiten conocer cuál es la situación exacta de los activos de información, en cuanto a la protección, el control y las medidas de seguridad. Desarrollar trabajos de auditoría es necesario para asegurar que la seguridad de la red. El continuo cambio de las configuraciones, la aparición de nuevos parches y las mejoras en el software y la adquisición

de nuevos hardware hacen necesario, que los sistemas estén periódicamente controlados mediante auditoría. Una auditoría de sistemas, es una radiografía completa de la situación de éstos. Asegúrese de que está preparado para interconectarse. Audite sus sistemas.

2.1.2. Antecedentes Nacionales

Según investigación de Silva Guerrero (2021), con título: "Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021", se planteó el siguiente objetivo: Implementar un SGSI para mejorar la SI en una empresa MYPE – 2021, y al finalizar se obtuvo las siguientes conclusiones: Se logró establecer una estructura organizacional del sistema de gestión de seguridad de la información teniendo como guía a la NTP-ISO/IEC 27001:2014, ya que brinda los lineamientos para una adecuada implementación del SGSI. Las micro y pequeñas empresas por lo general no cuentan con un SGSI, ya que consideran que su implementación puede ser muy costosa, pero se ha visto que la implementación del SGSI está en función a los recursos y necesidades de la empresa, por ende, no es necesario invertir mucho dinero, solo lo necesario para salvaguardar los principales activos de información, así evitar consecuencias negativas para dichas empresas y que el cumplimiento estricto de las cláusulas y dominios de dicha norma permite la certificación, pero para las micro y pequeñas empresas tal vez no siempre sea necesario la certificación, pero si considerar los

lineamientos adecuados de la norma para mejorar su SI. El compromiso de la alta dirección es muy importante para el éxito de la implementación del SGSI, por medio de ellos se logra involucrar y concientizar a los jefes de áreas y a todo el personal involucrado, además permite tener un respaldo de las políticas y procedimientos implementados y debidamente difundidas y documentadas, permitiendo a los trabajadores conocer y entender el SGSI y sus tareas y actividades que realizan, es importante realizar la documentación porque nos permite estar organizados y tener lineamientos definidos.

Según investigación de HUINCHO RAMOS (2019), con título: "Sistema de gestión de, seguridad de la información para mejorar la protección informática de la Comisaria Región Huancavelica", se planteó el siguiente objetivo: Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de la protección informática de la Comisaria región Huancavelica, y al finalizar se obtuvo las siguientes conclusiones: Como conclusión final, se debe tener en cuenta que hay que recalcar que de nada sirve contar con un SGSI, que consideren todos los posibles riesgos y controles para mitigarlos o contar con toda la tecnología posible para asegurar la información si no se da una debida importancia a la seguridad de la información por parte de las autoridades dirigentes de la organización y no sé cumplen las políticas y procedimientos establecidos por parte del personal de la comisaria de la PNP de la región de Huancavelica. Los usuarios potenciales de la comisaria PNP de la región de Huancavelica y de una manera general de nuestra institución, deberán ser capaces de superar el problema

cultural, de sobreponerse al temor natural y apreciar el horizonte de utilidades, aplicaciones, así como del ahorro de tiempo y dinero, que nos ofrecen la seguridad de la información, lo cual será posible a partir de una adecuada implementación y capacitación.

Según investigación de Vergara Quiroz (2017), con título "Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal", se planteó el siguiente objetivo: Determinar la relación entre la seguridad de información y la calidad de servicio en la Universidad Nacional Federico Villarreal, al finalizar se llegó a las siguientes conclusiones: Se ha determinado que existe una relación directa y significativa de nivel alto, entre la integridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016, obteniendo como resultado Rho de Spearman = 0.773** y un p-valor =0.000<0.05, en tal sentido se comprueba la hipótesis alterna y se rechaza la hipótesis nula. Se ha determinado que existe una relación directa y significativa de nivel moderado, entre la disponibilidad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016, obteniendo como resultado Rho de Spearman = 0.609** y un p-valor =0.000<0.05, en tal sentido se comprueba la hipótesis alterna y se rechaza la hipótesis nula.

2.2 Bases teóricas

2.1.1. Seguridad de Terminales

Definición

La seguridad de terminales es definida por Ruíz (2022), como la práctica de proteger terminales o puntos de acceso en dispositivos de usuario final, como computadoras de escritorio, portátiles y dispositivos móviles. de perpetradores y actividades peligrosas Endpoint Security protege estos puntos finales en su red o nube de amenazas de ciberseguridad. La seguridad de los terminales ha evolucionado desde el software antivirus tradicional hasta brindar protección integral contra malware sofisticado y amenazas de día cero en evolución.

Resalta Alay (2024), que organizaciones de todos los tamaños enfrentan riesgos provenientes de estados-nación, atacantes y organizaciones criminales. y amenazas internas maliciosas y no intencionadas. La seguridad de los terminales a menudo se considera la primera línea de la ciberseguridad. y es uno de los primeros lugares donde las organizaciones buscan proteger sus redes corporativas

A medida que el número y la sofisticación de las amenazas a la ciberseguridad siguen aumentando. La demanda de soluciones avanzadas de seguridad para terminales también está aumentando. Los sistemas de protección de terminales actuales están diseñados para detectar, analizar, bloquear y controlar rápidamente los ataques en curso. Para ello, necesitan trabajar juntos y con otras tecnologías de seguridad. Permitir que los administradores comprendan las amenazas

avanzadas para acelerar los tiempos de respuesta de detección y remediación (Gómez y Mero, 2023).

Importancia de la Seguridad de Terminales.

De acuerdo con Aarness (2024). Una estrategia de seguridad de endpoints es fundamental. Esto se debe a que cada punto final remoto puede ser un punto de partida para un ataque. Y con el rápido cambio hacia el trabajo remoto, el número de terminales no hará más que aumentar. Según un artículo de Forbes de 2023, el 12,7% de los empleados estadounidenses trabajan de forma remota y el 28,2% tienen acuerdos de trabajo híbridos. Aunque la mayoría de los empleados están actualmente en la oficina, se espera que el número de trabajadores remotos crezca a 32,6 millones para 2025, lo que representa el 22% de la fuerza laboral estadounidense. El riesgo que representan los puntos finales y los datos confidenciales es un desafío que no desaparecerá.

El entorno del destino cambia constantemente. Y las empresas de todos los tamaños son objetivos atractivos para los ciberataques. Esto es sentido común. Incluso en las pequeñas empresas Según el Informe de impacto empresarial de 2023 del ITRC, el 73% de los propietarios de pequeñas y medianas empresas (PYMES) informan que experimentaron un ciberataque en 2022 o 2023, según el Informe sobre delitos cibernéticos del FBI. En 2022 se recibió un total de 800.944 quejas. Para 2022, las pérdidas reportadas superarán los 10.300 millones de dólares. Los ataques de ingeniería social van en aumento y CrowdStrike rastrea

a más de 200 adversarios, según el Informe de amenazas globales de CrowdStrike 2023.

Según el Informe de costos de vulneración de datos de 2023 de IBM, el costo promedio de una vulneración de datos es de 4,45 millones de dólares, un 15 % más que en los últimos tres años. Un estudio encuentra que el mayor impacto financiero de una filtración de datos es que la "pérdida de negocios" representa casi el 40% del costo promedio de una filtración de datos.

Prevenir ataques a terminales es un desafío. Porque los puntos finales se encuentran en la intersección de humanos y máquinas. Las empresas se esfuerzan por mantener la seguridad del sistema sin interferir con las actividades legítimas de los empleados. Aunque las soluciones técnicas son muy efectivas, se pueden reducir las posibilidades de que los empleados queden expuestos a ataques de ingeniería social. Pero no se puede evitar por completo.

Características de los Sistemas de Protección de Terminales.

De acuerdo a lo expresado por Checkpoint (2024), Una solución de protección de terminales debe proporcionar protección integral para terminales y redes empresariales. Algunas de las características básicas de una solución de seguridad para terminales incluyen:

a. Antimalware: su solución de protección de terminales debe detectar y prevenir infecciones, gusanos y otro malware.

b. Análisis de comportamiento: Ransomware y otras formas de malware Tiene un comportamiento único que permite la detección sin necesidad de firma. Al examinar estos comportamientos, las soluciones de protección de endpoints pueden detectar y responder a ataques de día cero.
c. Cumplimiento: a medida que crecen el trabajo remoto y BYOD, la capacidad de hacer cumplir las políticas de seguridad de una organización se ha vuelto más importante. La solución de punto final debe evaluar los dispositivos y solo permitir conexiones a la red corporativa si cumplen con la política corporativa.
d. Cifrado de datos: el cifrado es la forma más eficaz de proteger los datos del acceso no autorizado y posibles fugas. Las soluciones de seguridad de endpoints deben incluir cifrado de disco completo (FDE) y admitir cifrado de medios extraíbles.
e. Controles de aplicaciones y firewall: la segmentación de la red es fundamental para gestionar el riesgo de acceso y la seguridad de la red. Las capacidades de control de aplicaciones y firewall permiten la segmentación de la red y el bloqueo del tráfico según políticas de seguridad y reglas específicas de la aplicación.
f. Inspección de zona de pruebas: los puntos finales pueden infectarse mediante métodos como phishing y exploits. Las soluciones de seguridad de endpoints deben aislar e inspeccionar archivos en un entorno sandbox para identificar y evitar que contenido malicioso llegue a los endpoints.

g. Acceso remoto seguro: el acceso remoto seguro es importante para los empleados que trabajan de forma remota o en modo híbrido. Las soluciones de seguridad de terminales deben incluir clientes de red privada virtual (VPN) u otras soluciones de acceso remoto seguro.
h. Filtrado de URL: los enlaces maliciosos son una técnica común utilizada en ataques de phishing. Y el uso inadecuado de la web en dispositivos corporativos puede reducir la productividad y poner en riesgo a la empresa. El filtrado de URL ayuda a proteger contra estas amenazas al bloquear sitios web maliciosos e inapropiados.

Componentes del software de seguridad para terminales.

Según Fortinet (2024). Un firewall es una solución de seguridad de red que monitorea el tráfico entrante y saliente. y decidir si permitir o denegar el acceso. La seguridad de los terminales ayuda a proteger los datos en el dispositivo. Esto permite a las empresas monitorear la actividad y el estado de todos los dispositivos de sus empleados en todo momento.

Tradicionalmente, los firewalls han sido adecuados para empresas donde todos los empleados trabajan en el mismo edificio e inician sesión en la misma red. Sin embargo, a medida que más personas trabajan de forma remota o desde casa, los firewalls ya no son suficientes. Esto se debe a que la transmisión de datos ya no pasa por una red central. Esto hace que el dispositivo sea vulnerable a ataques (López, et al., 2023).

También depende de la organización que protege la red o el punto final. La seguridad de la red ayuda a las organizaciones a protegerse

contra posibles amenazas de seguridad a nivel de red bloqueando los puertos abiertos. limite la transmisión de datos y utilice servicios de prevención y detección de intrusos. La seguridad de endpoints ayuda a las organizaciones a proteger los dispositivos conectados a la red. Al convertir los puntos finales en el nuevo perímetro de la red, las organizaciones pueden protegerse y detectar actividades sospechosas sin importar dónde se encuentren los empleados.

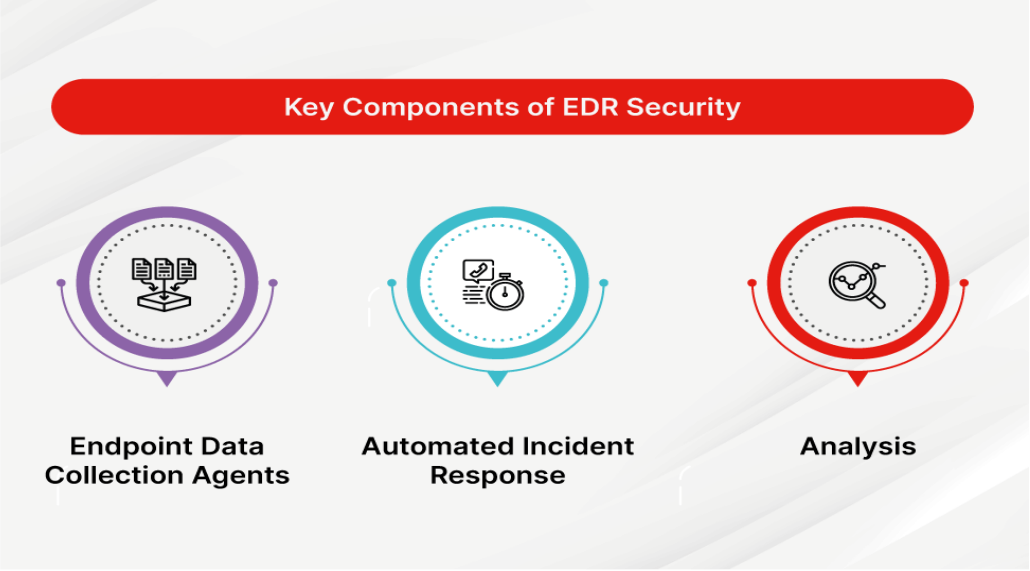
La selección de la solución de seguridad adecuada depende de la situación única y los requisitos de seguridad de cada organización:

a. Número de empleados: las pequeñas empresas pueden encontrar que los productos que requieren dispositivos administrados por separado funcionan bien. Pero cuando crezca, puede resultar más difícil para los equipos de seguridad y TI administrar dispositivos individuales de esta manera. Como resultado, obtienen importantes eficiencias al implementar soluciones de seguridad que centralizan el control de los terminales (Pinzón, et al., 2021).
b. Ubicación de los empleados: las empresas con empleados que trabajan desde una ubicación central pueden no tener problemas para administrar el acceso a los terminales. Pero aquellos con una fuerza laboral diversa, ya sea que trabajen desde casa en una oficina remota o estén viajando, debe haber una solución de seguridad de terminales que proteja los terminales donde y cuando los empleados intenten conectarse a sus redes y recursos (Pinzón, et al., 2021).

c. Propiedad de dispositivos: el aumento de BYOD ha desdibujado los límites de la propiedad de dispositivos. Los empleados utilizan cada vez más sus propios dispositivos para iniciar y cerrar sesión en las redes empresariales. Y es necesario hacerlo de forma segura. Las soluciones de seguridad para terminales permiten a las empresas proteger a los empleados cada vez que inician sesión en la red y monitorear el acceso en todo momento (Pinzón, et al., 2021).

d. Sensibilidad de los datos: las empresas que gestionan propiedad intelectual de alto valor o datos confidenciales pueden encontrar que el software antivirus no es adecuado para proteger sus datos. Porque sólo se puede proteger de virus. Para protegerse de eventos de pérdida de datos que plantean importantes riesgos financieros y de reputación. Estas organizaciones necesitan implementar soluciones de seguridad de terminales. Esto ayuda a proteger la información más importante. Cumplimiento y aprobación de la inspección (Pinzón, et al., 2021).

Figura 1: Componentes claves de Seguridad



Fuente: (Fortinet, 2024)

Tipos de protección de terminales

En concordancia con lo expresado por Cisco (2024). Los atacantes se mantienen al día con las últimas tendencias de seguridad para lanzar ataques más sigilosos. Hace que las herramientas antivirus tradicionales queden obsoletas La seguridad de endpoints combina la protección preventiva de una solución EPP con las capacidades de detección y auditoría de un EDR.

a. Plataforma de protección de terminales (EPP). Una solución EPP es una herramienta de protección que realiza protección en tiempo real inspeccionando y escaneando archivos tan pronto como ingresan a la red. El tipo más común de protección de terminales es una solución antivirus (AV) tradicional. Una solución antivirus incluye capacidades antimalware. Está diseñado principalmente para proteger contra ataques basados en firmas. Cuando el archivo ingresa a la red, la solución antivirus escanea los archivos para ver si la firma coincide con una amenaza maliciosa en la base de datos de inteligencia de amenazas (Cisco, 2024).
b. Detección y resolución de terminales (EDR). Una solución EDR es más que un simple mecanismo de detección de un momento determinado. En cambio, monitorea continuamente todos los archivos y aplicaciones que ingresan al dispositivo. Esto significa que las soluciones EDR pueden proporcionar visibilidad y análisis más detallados para las investigaciones de amenazas. Las soluciones EDR también pueden detectar amenazas más allá de los ataques

basados en firmas. Utilice una solución EDR para detectar malware. Eso no incluye archivos, ransomware, varios tipos de ataques y más (Gómez y Mero, 2023).

c. Detección y respuesta extendidas (XDR). EDR mejora la detección de malware en lugar de las capacidades antivirus, mientras que XDR amplía el alcance de EDR para incluir soluciones de seguridad más activas. XDR ofrece una funcionalidad más amplia. EDR utiliza la última tecnología para brindar visibilidad. mejor y recopilar y vincular información sobre amenazas al mismo tiempo que utiliza análisis y automatización para ayudar a detectar ciberataques actuales y futuros (Gómez y Mero, 2023).

2.3 Definición de términos básicos

a. Implementación: Según Lutkevich (2024). La implementación es la ejecución o práctica de un plan, un método o cualquier diseño, idea, modelo, especificación, estándar o política**,** para hacer algo. Como tal, la implementación es la acción que debe seguir a cualquier pensamiento preliminar para que algo realmente suceda.

b. Plataforma: Según Rouse (2020). Una plataforma es un grupo de tecnologías que se utilizan como base sobre la cual se desarrollan otras aplicaciones, procesos o tecnologías.

c. Protección: Según Careemergencytoolkit (2024). Esto significa que los programas y el personal de CARE deben trabajar para respetar y defender la vida y la dignidad de las personas incorporando principios

de protección en la programación de ayuda y tomando acciones protectoras siempre que sea posible.

d. Terminales: Según Itconnect (2016). Un terminal es un dispositivo de hardware de comunicación electrónica que maneja la entrada y visualización de datos.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Metodología y técnicas utilizadas

3.1.1. Tipo de investigación

El tipo de investigación será Aplicada, Según Murillo (2008) es también se le llama investigación práctica o empírica porque presenta el uso y aplicación de conocimientos previamente adquiridos.

3.1.2. Nivel de investigación

La presente investigación es de un nivel Explicativo, según Ibarra (2011), su objetivo principal es explicar qué ha sucedido o está sucediendo en un fenómeno. ¿Y cuáles son las condiciones necesarias para su manifestación? ¿O cuál es la relación entre dos o más variables de investigación?

3.1.3. Método de investigación

El método de investigación es Deductivo-Inductivo. De acuerdo con Gladys (2006). Deductivo: Este es un proceso de pensamiento que comienza con una afirmación general. y utilizar las reglas de la lógica para llegar a un mensaje específico e Inductivo: La conclusión de una inferencia es verdadera sólo si la razón subyacente es verdadera.

3.1.4. Diseño de la investigación

Este diseño es consistente con un modelo experimental del tipo pre experimental que incluye una prueba previa y posterior para determinar relaciones causales entre las variables independientes y dependientes.

Se representar de la siguiente manera:

$$\mathbf{M}: \boldsymbol{O_1 - X - O_2}$$

Dónde:

M: La muestra.

O_1: Pre test.

X: Manipulación de la variable independiente.

O_2: Post test

3.2 Población y muestra

3.2.1 Población

Esta comprendido de todo el personal de TI quienes tienen como función principal salvaguardar la información de la organización, estos empleados hacen un total de 11, que lo conformar 01 Jefe, 02 Administradores de Servidores, 02 Administradores de Sistemas, 04 Asistentes de TI y 02 de soporte.

3.2.2. Muestra

Porque el número total de usuarios no es grande, es conveniente hacer uso del método no probabilístico. Por lo tanto, se optó por un muestreo por conveniencia y la muestra es el total de la población, siendo este un número total de 11 empleados.

3.3 Instrumentos de recolección de datos

Como herramienta de investigación se hará uso de la encuesta que viene a ser el proceso de búsqueda de información a través de un cuestionario elaborado previamente. El cuestionario debe contener preguntas específicas de la información que se desea obtener.

3.4 Procedimiento de recolección de datos

Según Simplilearn (2023). El proceso de recopilar y analizar información precisa de diversas fuentes. Encontrar respuestas a preguntas de investigación, tendencias, probabilidades, etc. Evaluar posibles resultados. Se llama recopilar información. el conocimiento es poder La información es conocimiento Y los datos son información en forma digital. Al menos según la definición de TI.

3.5 Tratamiento de datos.

Según Sharma (2023). El análisis de datos cuantitativos es el proceso de analizar e interpretar datos numéricos. Utilice cálculos matemáticos y pruebas estadísticas para identificar patrones, tendencias y relaciones entre variables que le ayudarán a comprender sus datos.

3.6 Grado de confiabilidad de los datos.

Se aplicará el alfa de Cronbach que es una forma de medir la coherencia interna de una encuesta o cuestionario. El alfa de Cronbach oscila entre 0 y 1, y los valores más altos indican que la encuesta o el cuestionario son más fiables.

CAPÍTULO IV

SISTEMA DE PROTECCIÓN DE TERMINALES

4.1. La empresa

IM Selva, como empresa que invierte en activos de tecnología de información entre las que destacan:

a. La implementación de hardware (computadoras, personales, impresoras, laptop, servidores) y programas (software) para la agilización de las actividades rutinarias y de gestión (Sistemas Operativos, aplicativos, etc),
b. Obtiene una ventaja o celeridad de procesos; pero al mismo tiempo el control de estos activos, debido a su variedad, sin el control adecuando, coloca a la organización en condiciones vulnerables y de riesgo;
c. Fue necesario realizar la presente investigación, con la finalidad de minimizar los riesgos y garantizar la fuga o robo de información, con la aplicación de controles y la implementación de una solución.

Tomando como referencia a la investigación de Silva Guerrero (2021), la metodología para la implementación de la solución toma como base las fases del SGSI divido en 05 fase que a continuación se describen brevemente:

Tabla 2: Fases del SGSI

Fases	Etapas/ Actividad
Iniciación	- Identificación de problemas principales. - Elaborar acta de constitución del proyecto.
Planificación	- Definir el alcance - Estructurar el cronograma de actividades - Establecer roles y responsabilidades - Control de documentación. - Análisis del estado actual de la empresa tomando como base el SGSI. - Elaborar análisis de costo - beneficio. - Elaborar políticas de seguridad de la información.
Ejecución del proyecto	- Activos de información. - Gestión de riegos y oportunidades. - Análisis y valoración de riesgos - Tratamiento de riesgos y selección de controles. - Elaborar el programa de capacitaciones.
Seguimiento y control.	- Resultados y análisis de indicadores. - Auditoría interna.
Cierre	- Elaborar el acta de cierre del proyecto

4.2. Desarrollo de fases

a. Fase: Iniciación

- **Identificación de problemas**

  A continuación, se mencionan los principales problemas referente a los sistemas de información, esto es producto de recopilación de información a través de entrevistas con el personal:

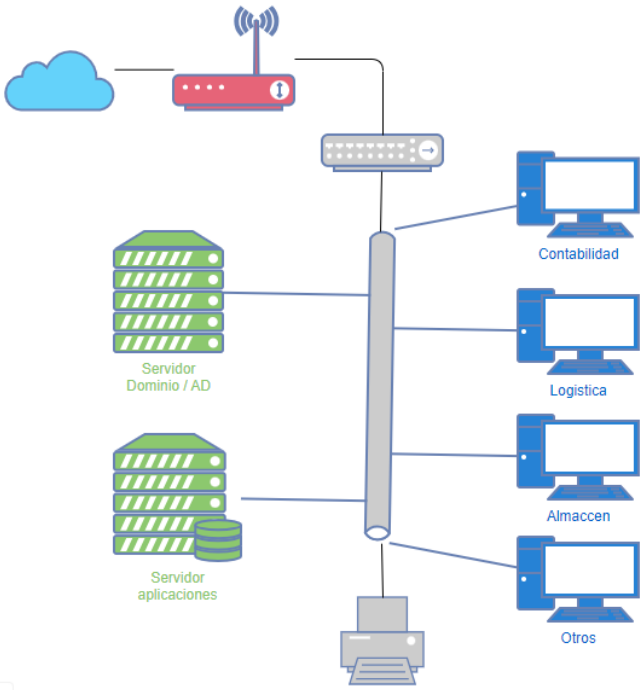
- **Descripción del problema**

  Como resultado de indagaciones se logró determinar que el área de Tecnología de la información presenta problemas respecto a los sistemas de información; por esta razón, que a partir de dicha área se iniciaría la implementación del SGSI. Seguido se detalla los problemas encontrados:

  - Diseño inadecuado de infraestructura de TI.
  - Información no actualizada.
  - Manipulación inadecuada de información.
  - Sistemas informáticos expuestos e infectados por programas maliciosos.
  - Poca organización documentaria.
  - Procedimientos desconocidos.
  - Carencia de seguridad de TI.
  - Perdida y/o robo de información a través del uso de TI.

Esquema general de la red de datos

Figura 2: Esquema de red de datos



- **Elaboración del Acta de constitución del proyecto**

  Este documento, define el inicio del proyecto y es aprobado por la alta dirección, y es donde se define los objetivos y se determina el alcance.

b. Fase 2: Planificación

En esta etapa se planifica, definen las actividades y tareas para la implementación del SGSI, el mismo que cuenta con las siguientes actividades:

- **Definición del Alcance del SGSI**

  Se debe definir el alcance, con el fin de estimar todos los recursos, el costo y el tiempo de la implementación.

- **Alcance**

  El alcance puede resultado de reuniones con el personal de la empresa, principalmente con las jefaturas, y se aprobó implementar el proyecto,

con el fin de reducir los problemas, buscar el involucramiento de los encargados y con ello la facilidad del proceso de implementación.

A continuación, se muestra de forma general el esquema del documento de alcance (Anexo 05).

- **Estructura del Cronograma de actividades**

  Vienen a ser una serie de actividades y /o tareas fundamentales para el desarrollo del proyecto de SGSI.

- **Tareas - actividades del SGSI**

  A continuación, se detallar las actividades

Tabla 3: Actividades del SGSI

Gestión del proyecto		
Iniciación	Identificación d problemas	Descripción del problema
	Elaboración del acta de constitución	Acta de constitución
Planificación.	Definición del alcance	Alcance del SGSI
	Estructura de cronograma	Cronograma
	Establecer roles y responsabilidades	Roles y responsabilidades
Ejecución	Control documentario	Ficha de control
	Análisis actual	Ficha Informe de análisis
	Elaboración del análisis	Informe
	Elaboración de políticas	Política
	Activos de información	Identificación Inventario
	Gestión de riesgo	Manual
	Tratamiento de riesgo	Tratamiento
	Capacitaciones	Materiales evaluación
Seguimiento	Resultado de análisis	Resultado Ficha
	Auditoria	Informe
Cierre	Elaboración del Acta	

- **Roles y responsabilidades**
  - Jefe de TI

    El jefe desde es el responsable de la ejecución del proyecto y de la implementación del SGSI de lo que respecta a la para estratégica y operativa, están bien quien toma las decisiones respecto al SGSI.
  - Asistente TI

    Es el colaborador y efectuar o realizar la parte operativa de la implementación del SGSI.
  - Otros jefes

    Está conformado por el personal que apoyan en el planteamiento estratégico del SGSI el ayudado a que éste sea más objetivo.
  - Consultor SGSI

    Es el encargado de brindar las pautas para la correcta implementación del SGSI, las cuales deben estar estrechamente relacionadas con las normas técnicas.
- **Controles de la documentación**

  La documentación respecto a la implementación del SGI es de suma importancia, debido al accidente estos se encuentran detallado los procedimientos de forma correcta, el mantenimiento de los acuerdos establecidos, es importante también llevar un control de estos con la finalidad de que su contenido será preciso, exacto y no ambiguo.

  Esta documentación debe estar almacenado de manera física y firmada por los responsables directos, debe ser reformado un almacén almacenado en lugares específicos y también debe y puede ser

almacenados en formato digital para luego ser compartido con el personal idóneo.

Los procesos de modificación y actualización de la documentación también deben ser aprobados por el comité directos debe ser grave impresos de forma física y nuevamente volver a ser digitalizado llena de control de las versiones.

- Ficha de control documental

  A continuación, se mostrarán un fragmento de la estructura de la ficha de control documentado implementado (Anexo 05).

c. Fase 3: Ejecución del proyecto

En esta fase se ejecutan e implementan las actividades y tareas planificadas respetando el cronograma, entre las que tenemos: la implementación de políticas, la gestión de riesgos, elaboración de controles, políticas y procedimientos, etc.

- **Estado actual de la empresa**
  - Fecha de entrevista

    Es un documento que nos ayudará a recabar información del estado actual de la organización tomando como referencia al SI, para lograr esto, es necesario realizar reuniones con la finalidad de obtener información a través del uso de preguntas, el uso de fichas, los cuales han sido respondidos por el personal clave de las tareas de la empresa.

    A continuación, se presentará de forma General el formato de fecha de entrevista (Anexo 05).

- Informe de análisis de situación actual.

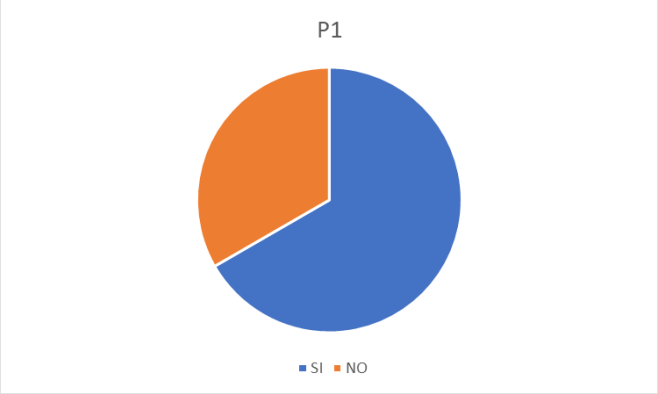
  Del presente documento se ha elaborado tomando como base la información obtenida de las fichas de entrevista, se elaboró un informe de las principales faltas de SI que se encuentran dentro de la organización. Asimismo, para entender los riesgos a los que se exponen.

  A continuación, se presenta un fragmento del análisis del estado actual:

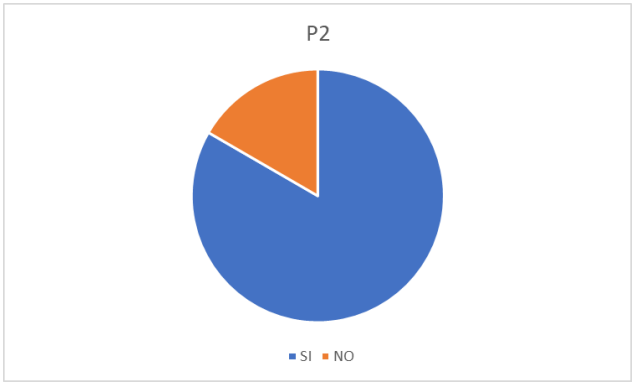
Figura 3: Análisis del estado actual

	RESPUESTAS																		
Nro	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
E1	SI	SI	SI	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
E2	SI	SI	SI	SI	NO	NO	SI	NO	SI	SI	SI	SI	NO	SI	NO	SI	SI	SI	SI
E3	NO	SI	SI	NO	SI	SI	NO	SI	NO	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
E4	SI	NO	SI	SI	SI	SI	NO	NO	SI	NO	NO	NO	SI	SI	NO	NO	NO	NO	NO
E5	NO	SI	SI	NO	SI	NO	NO	SI	NO	SI	NO	SI	NO	NO	NO	SI	SI	SI	SI
E6	SI	SI	SI	NO	NO	SI	NO	NO	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI

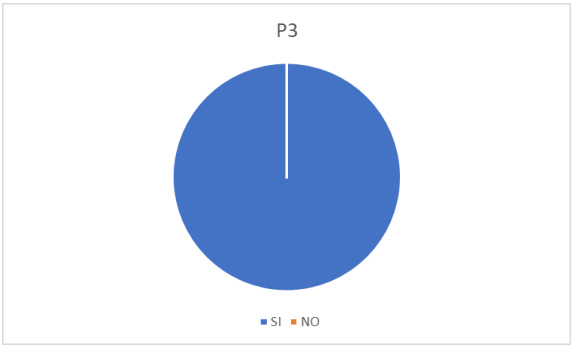
1. ¿Usted considera que es importante identificar y conocer los activos de información que maneja su área?



2. ¿Ud. considera que se ha logrado identificar cuáles son los activos críticos de información el posee su área?



3. ¿Cree usted que los activos de información obtenido poseen controles de garantizar la seguridad de los mismos?



- **Análisis costo beneficios**

  En esta fase se buscará demostrar la relación entre el costo de la implementación y el beneficio que se alcanzaría, o el objetivo de determinar si es necesario ejecutar el proyecto o no, para lograr esto se ha tomado en cuenta proceso reales que han tenido lugar en la organización, así como algunas estimaciones de carácter técnico que ha sido sugeridas por responsables de las actividades de tecnología.

  Mediante el presente documento se pretende saber si es pertinente efectuar la implementación para el proceso de tecnología de información, a continuación, se detallan las características de la evaluación costo beneficio (Anexo 05).

- **Políticas de seguridad**

  Las políticas de seguridad se elaboran tomados cuenta los objetivos unas estrategias organizacionales, con la finalidad de proporcionar procedimientos de control para alcanzar los objetivos planteados, es necesario que la empresa invierta en recursos, los cuales van a mejorar la labores que desempeñan los colaboradores como parte del compromiso y el entendimiento de las políticas.

  Estas políticas deben ser elaborado y aprobado por los altos directivos de tal forma de ser cuente con el respaldo que requerido para su cumplimiento. Para la elaboración de las políticas se tomó en cuenta los dominios de control de traslados en la norma técnica peruana 27001.

  A continuación, se presenta un fragmento General respecto al documento política de seguridad de la información (Anexo 05).

- **Activo de información**

  Son todos los elementos que contienen información que cuentan con un Valor para la empresa, esto debe ser protegido y para eso es necesario identificarlos, para luego realizar una valoración de cada uno.

  Para la identificación de los activos, se aplicó el siguiente formato de tabla:

Tabla 4: Activo

Id activo	Categoría	Sub categoría	Nombre del activo	Descripción del activo	Proceso al que pertenece	Tipo	Ubicación	El propietario

- Id Activo: identificador único del activo
- Categoría: puede ser primario o de soporte:
- Subcategoría: puede ser local, del servicio, de información, documento, hardware, red, software, personal o auxiliares.

- Descripción: se detallada la finalidad o importancia del activo.
- Proceso que pertenece: se resista cuales el proceso que contienen ha dicho activo.
- Tipo: pudiendo ser tecnológico o no tecnológico.
- Ubicación: se precisa lugar donde se encuentra el archivo
- Propietario: es el personal o entidad que posee que controla el activo.

- **Inventario de activos.**

  Para el correcto control este importante evitar la duplicidad de la ambigüedad de la descripción de los activos, este inventario permite registrar únicamente aquellos activos más importantes del proceso den TI, asimismo nos permitirá calcular, estimar el Valor de cada uno de ellos; por lo cual, es importante considerar qué consecuencias podrían generar daño o pérdida cuando algún incidente afecta al activo, para una correcta moderación ser uso de una escala cualitativa:

Tabla 5: Inventario de activos.

Valor	**Descripción**
De 1 a 3	Valor bajo de color será el verde
De 4 a 6	Valor medio de color amarillo
De 7 A más	Valor alto de color rojo

A continuación, se muestra el formato de tabla utilizado para el inventario y valoración de activos:

Tabla 6: Formato para validación de inventario de activos

	Datos del activo			Afecta				Valoración
No	Id activo	Nombre	Propietario/ responsable	C	I	D	Total	

- No: número de activo
- Confidencialidad(C): se precisa la clasificación pudiendo ser 0 para “no afecta”, 1 para “uso público”, 2 para “uso interno” y 7 para “confidencial”.
- Integridad: puede ser 0 para “no afecta”, 1 para “baja”, 2 para “normal” y 7 para “sensible”
- Disponibilidad: para ser 0 para “no afecta”, 1 para “baja”, 2 para “media” y 7 para “Alta”.
- Total: viene a ser la suma de los campos CID

Valoración del activo: pudiendo ser:

- De 1 a 3 Valor bajo de color será el verde
- De 4 a 6 Valor medio de color amarillo
- De 7 A más Valor alto de color rojo

- **Gestión de riesgo.**

  Este trabajo es la más importante, debido al fin y ésta se puede identificar aquellos riesgos de carácter interno o externo para que los activos de información se encuentran expuestos.

  A continuación, se muestra en forma General, un manual de gestión de riesgos y oportunidades aplicado en la empresa (Anexo 05).

- **Análisis y valoración de riesgo**

  De esta etapa permite la gestión de los riesgos que moverlos a un nivel aceptable con la finalidad de que no tengan efectos negativos cuando estos sucedan. El análisis identificar a los peligros sobre los activos y permitirá estimada el grado de exposición de los mismos el caso de la materialización de una o varias amenazas.

Las amenazas vienen a ser aquellos elementos o incidentes que puede surgir y acelera de forma natural, humana o artificial que aprovecha una o varias vulnerabilidades es de un activo, estas amenazas pueden ser de origen interno, externó un o accidentales e intencionales.

Las vulnerabilidades representan las debilidades de los activos y que de materializarse se convierten en una amenaza.

La probabilidad de ocurrencia se detallada a continuación:

Tabla 7: Probabilidad de ocurrencia

Tipo	**Descripción**
1 casi nunca	Una vez cada 2 años
2 poco probable	Ocurre cada año
3 probable	Ocurren cada 6 meses
4 muy probable	Puede ocurrir al mes
5 frecuente	Cada semana

La medición del impacto se detalla continuación:

Tabla 8: Medición del impacto

Tipo	**Descripción**
2 insignificante	El impacto de forma ligera
4 menor	Impactante y el funcionamiento del proceso
6 moderado	Impacta de forma considerable
8 mayor	Impacta fuertemente
10 desastroso	Impacta de forma crítica

Cálculo del nivel de riesgo

Tabla 9: Calculo de nivel de riesgo

	Riesgo = Probabilidad*Impacto					
Probabilidad	5	10	20	30	40	50
	4	8	16	24	32	40
	3	6	12	18	24	30
	2	4	8	12	16	20
	1	2	4	6	8	10
		2	**4**	**6**	**8**	**10**
				Impacto		

Donde:

Tabla 10: Valoración del nivel de riesgo

1	Aceptable	Se acepta el riesgo y se asume	Desde 2 a 4
2	Tolerable	El riesgo se asume que se trata de reducirlo. Su aprehensión es inmediata y se debe monitorear de forma permanente	Desde 6 a 12
3	Intolerable	Se debe realizar acciones para reducir, eliminar o transferir el riesgo. Su atención es inmediata con monitoreo permanente.	Desde 16 a 24
4	Extremo	Es intolerable, y su tratamiento lo debe efectuar la alta dirección	Desde 30 a 50

A continuación, se muestra de manera General el informe de riesgo de los activos de información (Anexo 05).

- **Tratamiento de riesgo**

  La finalidad de la gestión de riesgos es convertirlos a éstos en niveles aceptables, para ello se ha determinado 4 estrategias de tratamiento de los cuales son:

- Asumir: se decidió asumir el riesgo, debido a que se encuentra en el nivel aceptable.
- Reducir: Esto se puede lograr mediante la implementación de controles. Los controles tienen por finalidad minimizar la posibilidad de los riesgos.
- Transferir: Esta acción es aplicable cuando se piensa pasar el riesgo la otra entidad o compartirlo, para ello se tiene que realizar una evaluación del Valor del activo y el coste de los controles.
- Eliminar: se realizan acciones con la finalidad de eliminar el riesgo o tal vez la eliminación del activo.

A continuación, se muestra de forma General el establecimiento de controles (Anexo 05).

- **Capacitación.**

  Para realizarlas capacitaciones que debe primero coordinar con todas las áreas, se debe definir las fechas, los materiales, se debe elaborar un manual de la gestión de riesgos, se debe realizar evaluaciones para obtener los resultados de la capacitación.

d. Fase 4: Seguimiento y control

Se de implementar un grupo de medidas y acciones para poder evaluar la ejecución de las actividades del proyecto que se definió en la planificación.

- **Resultado y análisis de indicadores**

  En esta etapa fue necesario realizar entrevistas y aplicar el cuestionario sobre los empleados y de esta manera determinar los resultados con el fin de averiguar el grado de mejora o respecto al conocimiento.

- **Auditoría interna**

  Para poder corroborar que se ha cumplido hoy grado de cumplimiento de las políticas y procedimientos establecidos es necesario en la alta dirección realice acciones para que se produzca una auditoría interna, la auditoría pretende que se cumplan todos los lineamientos establecidos en el SGSI.

e. Fase 5: Cierre

- **Acta**

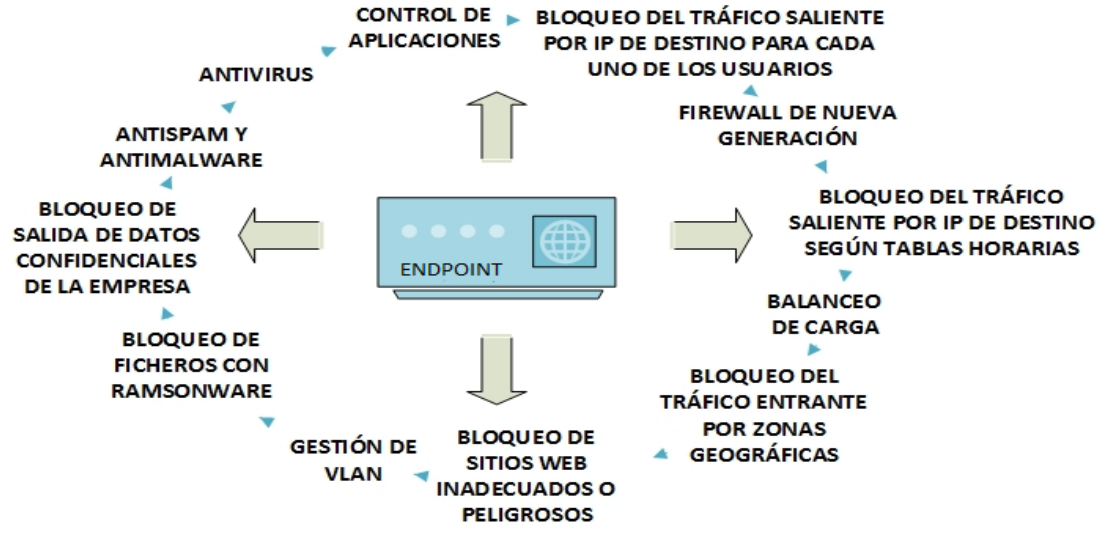
  Al finalizar la implementación del proyecto, que se realizará una reunión con todo el personal y voluntad de para elaborar el acta de cierre del mismo este documento debe ser firmado por las partes interesadas, con la finalidad de dar su aprobación y el visto bueno de la implementación.

4.3. Implementar una solución para salvaguardar los activos digitales

Como se pudo observar en la evaluación de riesgos uno de los puntos más críticos es la fuga o pérdidas de información, esto se puede dar a través de la sustracción de archivos y datos de las computadoras los cuales pueden ser confiados en dispositivos externos o enviados a través del correo electrónico; en tal sentido, como parte de los controles implementados en el proyecto, se detallan los criterios y características de la implementación de un equipo informático cuya finalidad es gestionar la salida de información momento sin permiso.

- **Amenazas Internas a tratar**
  - Protección contra virus y otro tipo de amenazas, debido al uso de pen-driver
  - Las contraseñas de acceso a los recursos compartidos débiles o divulgadas.
  - Carecía de política respecto a permisos de acceso a recursos compartidos
  - Carece de procedimientos para copias de seguridad
  - Almacenamiento de información interpretar locales.
- **Amenazas externas a tratar**
  - Inadecuada configuración de firewall que no bloquear accesos
  - Aplicaciones maliciosas.
  - Carencia de control antivirus y otros
  - Carece de control sobre tipos de datos que salen de la organización
- **Equipo endpoint**

Figura 4: Endpoints



- **Características Técnicas**
  - Proteger contra exploits, sitios web maliciosos.
  - Controlar las aplicaciones de acceso a internet
  - Detectar ataques y amenazas nuevos
  - Velocidad en manejo de paquetes hasta 3 Gbps, análisis de 4.5 millones por segundo, concurrencia de 2 millones, sesiones de hasta 77000 TCP/UDP
  - Contar con 02 puertos WAN Gbit Ethernet
  - Contar con 16 puertos LAN Gbit Ethernet
  - Contar con 02 puertos SFP Gbit Ethernet
- **Equipo Firebox M200 watchguard**

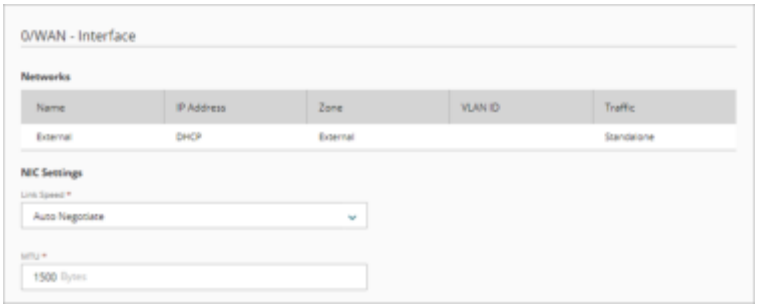
Figura 5: Equipo Firebox



- **Configuración**

  Ajuste de la NIC
  - Configurar>Dispositivo
  - Seleccionar “Firebox administrador en la nube”
  - Seleccione “Configurar dispotiviso”
  - Selecciones pestaña “redes”
  - En la pestaña interfaces “, seleccione mosaico

Figura 6: Mosaico

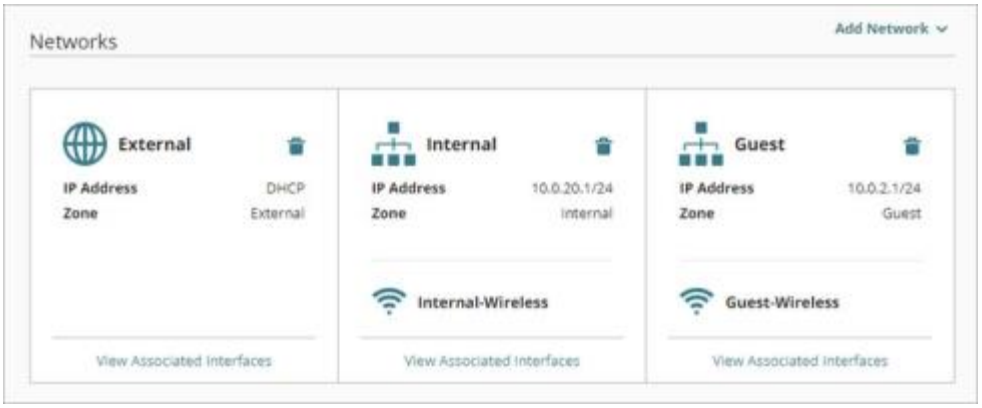


- En la lista “Velocidad de enlace”, seleccionar la velocidad.
- En MTU, defina el tamaño del paquete máximo (1500 bytes)
- Guardar

Configurar Zonas de red

Ver detalle en el panel de control de la configuración de redes.

Figura 7: Configuración de Zonas



- Externa: Red como en este caso es internet.
- Interna: Es la red local de la organización.
- Invitado: No aplicado.

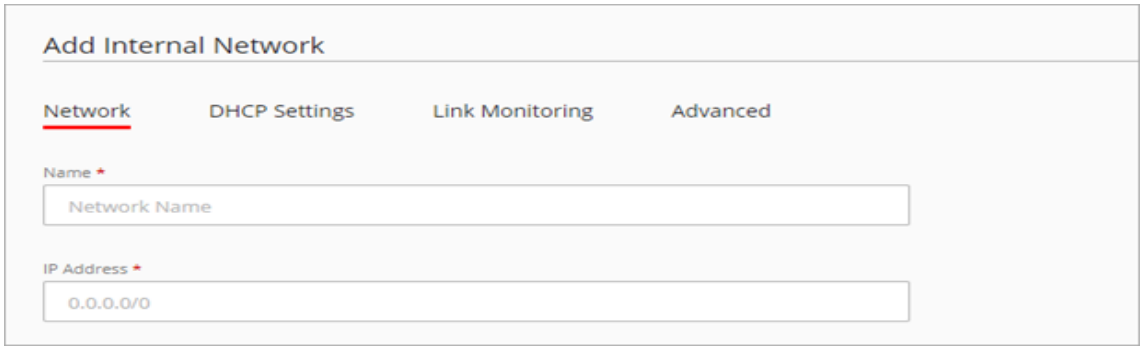
Configurar red interna.

Zona de red es interna, las políticas de firewall saliente se aplican al tráfico de la red.

Agregar red:

- Configurar>dispositivo
- En la pestaña de redes, seleccione mosaico
- Agregar red
- De la lista seleccione el tipo

Figura 8: Anadir red interna



Configurar interfaces:

Se debe asociar a una red a continuación se muestran las disponibles:

Figura 9: interfaces



Seleccionar el tipo 3 asociada con esta red.

Configurar plantillas.

Proporcionan una forma de administración de las configuraciones compartidos, permite configurar políticas y servicios.

A continuación, se listas los ajustes realizados:

- Políticas de firewall
- Excepciones

- Filtrado de contenido
- Bloque de red
- Copia de información.

CAPÍTULO V
RESULTADOS Y DISCUSIÓN

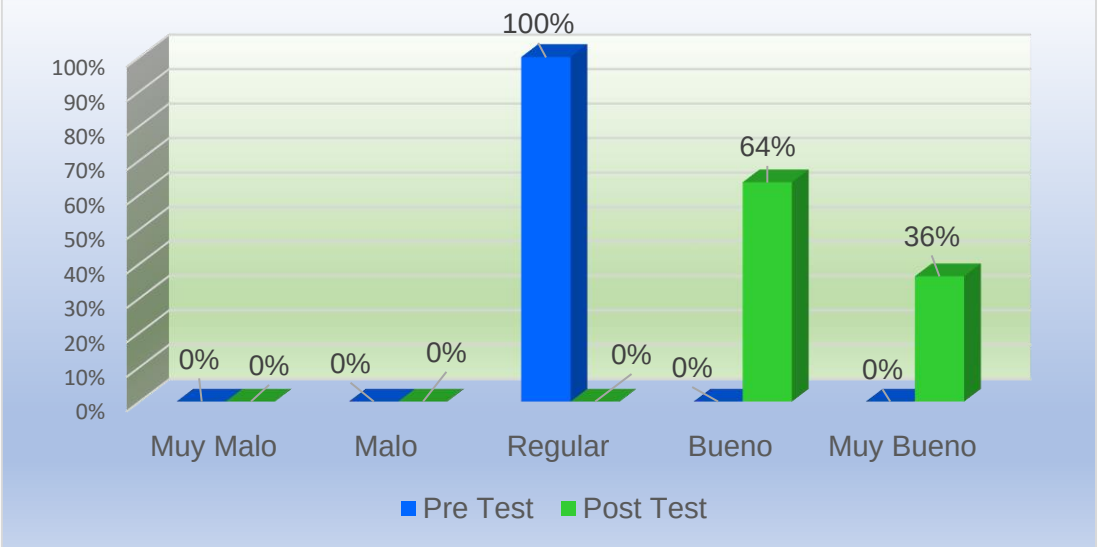
5.1. Resultados variable seguridad de la información

Tabla 11: Distribución de frecuencia del pre y post test

Seguridad de la Información	Pre Test		Post Test	
	Frecuencia	Porcentajes	Frecuencias	Porcentajes
Muy Malo	0	0%	0	0%
Malo	0	0%	0	0%
Regular	11	100%	0	0%
Bueno	0	0%	7	64%
Muy Bueno	0	0%	4	36%
Total	11	100%	11	100%

Fuente: Anexo 4 y 5

Figura 10: Barras porcentuales del pre y post test



Fuente: tabla 11

En base a la tabla 11 y figura 10, la implementación de la plataforma de protección de terminales en la empresa IM SELVA SAC ha demostrado una mejora significativa en la seguridad de la información, según los resultados obtenidos en el pre test y post test. Inicialmente, el 100% de las evaluaciones se clasificaron como "Regular", lo que indica una seguridad de la información

insuficiente. Sin embargo, tras la implementación de la plataforma, se observó una notable mejora: el 64% de las evaluaciones se clasificaron como "Bueno" y el 36% como "Muy Bueno". No se registraron evaluaciones en las categorías de "Muy Malo" o "Malo" en ninguno de los dos tests, lo que refuerza la efectividad de la plataforma implementada. Estos resultados evidencian que la plataforma de protección de terminales ha mejorado considerablemente la seguridad de la información en la empresa, cumpliendo así con el objetivo planteado en esta investigación.

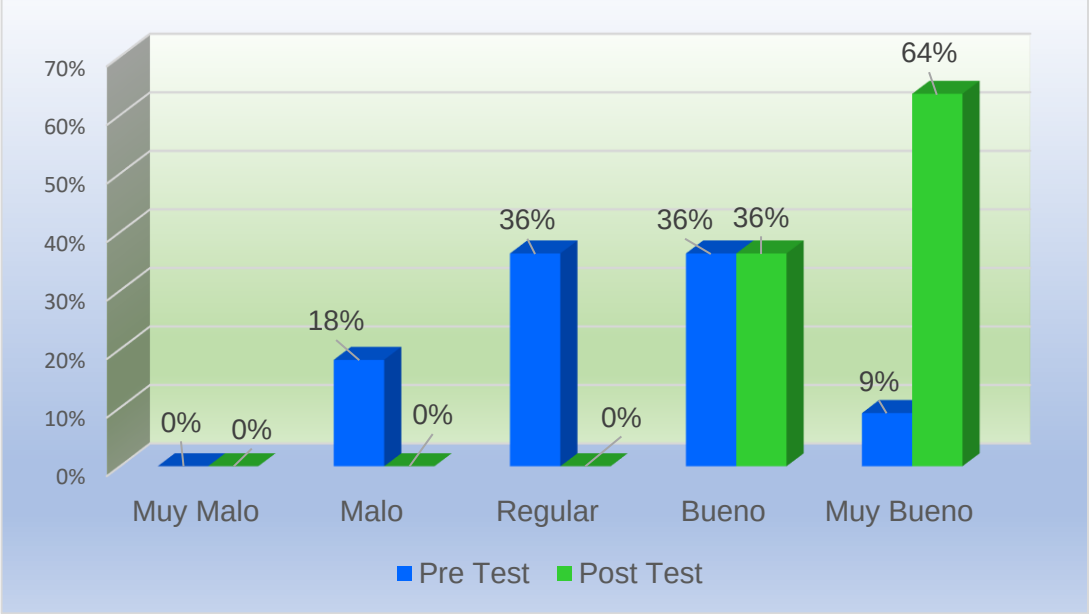
5.1.1 Procesamiento de datos de la dimensión iniciación

Tabla 12: Distribución de frecuencia del pre y post test

Iniciación	Pre Test		Post Test	
	Frecuencia	Porcentajes	Frecuencias	Porcentajes
Muy Malo	0	0%	0	0%
Malo	2	18%	0	0%
Regular	4	36%	0	0%
Bueno	4	36%	4	36%
Muy Bueno	1	9%	7	64%
Total	11	100%	11	100%

Fuente: Anexo 4 y 5

Figura 11: Barras porcentuales del pre y post test



Fuente: tabla 12

En el análisis de la tabla 12 y figura 11, se observa que la plataforma de protección de terminales en la empresa IM SELVA SAC ha permitido identificar y abordar problemas críticos en los sistemas de información, mejorando significativamente la iniciación de la seguridad de la información. En el pre test, se observó que el 18% de las evaluaciones se clasificaron como "Malo" y el 36% como "Regular", lo que evidenciaba deficiencias importantes en la seguridad inicial. Sin

embargo, tras la implementación de la plataforma, los resultados del post test muestran una mejora notable: el 64% de las evaluaciones se clasificaron como "Muy Bueno" y el 36% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo" o "Malo" en el post test, lo que indica una eliminación de los problemas más graves. Estos resultados demuestran que la plataforma ha sido efectiva en mejorar la iniciación de la seguridad de la información, cumpliendo con el objetivo de identificar y solucionar los problemas existentes en los sistemas de información de la empresa.

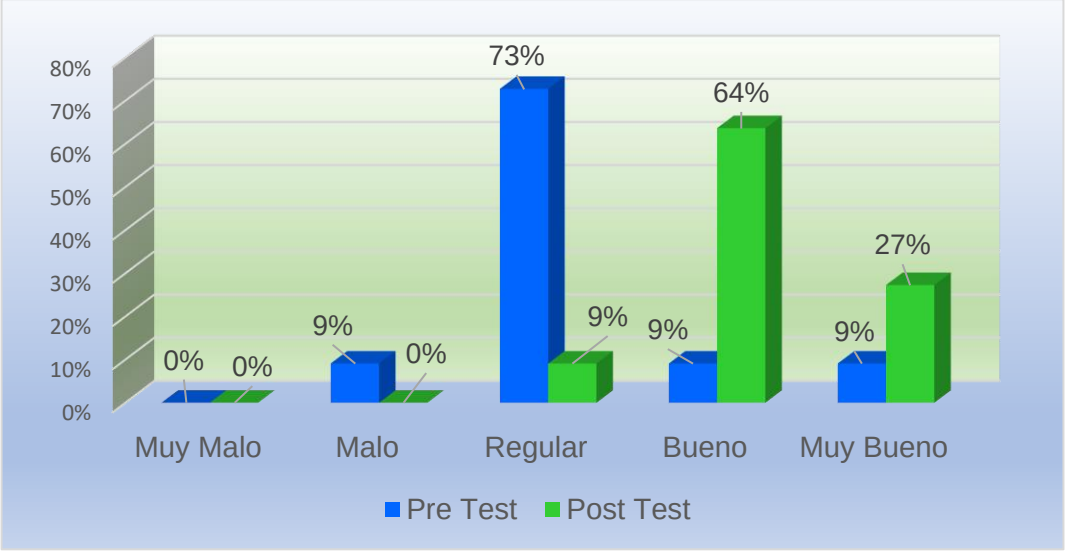
5.1.2 Procesamiento de datos de la dimensión planificación

Tabla 13: Distribución de frecuencia del pre y post test

Planificación	Pre Test		Post Test	
	Frecuencia	Porcentajes	Frecuencias	Porcentajes
Muy Malo	0	0%	0	0%
Malo	1	9%	0	0%
Regular	8	73%	1	9%
Bueno	1	9%	7	64%
Muy Bueno	1	9%	3	27%
Total	11	100%	11	100%

Fuente: Anexo 4 y 5

Figura 12: Barras porcentuales del pre y post test



Fuente: tabla 13

En el marco de la tabla 13 y figura 12, se evidencia que la plataforma de protección de terminales en la empresa IM SELVA SAC ha permitido determinar las características esenciales de la planificación de tareas y actividades para mejorar la seguridad de la información. En el pre test, se observó que el 73% de las evaluaciones se clasificaron como "Regular" y el 9% como "Malo", lo que indicaba una planificación deficiente y poco efectiva. Sin embargo, tras la implementación de la plataforma, los resultados del post

test muestran una mejora significativa: el 64% de las evaluaciones se clasificaron como "Bueno" y el 27% como "Muy Bueno". Solo el 9% permaneció en la categoría de "Regular" y no se registraron evaluaciones en las categorías de "Muy Malo" o "Malo". Estos resultados demuestran que la plataforma ha sido efectiva en mejorar la planificación de las tareas y actividades, cumpliendo con el objetivo de identificar y fortalecer las características necesarias para una mejor seguridad de la información en la empresa.

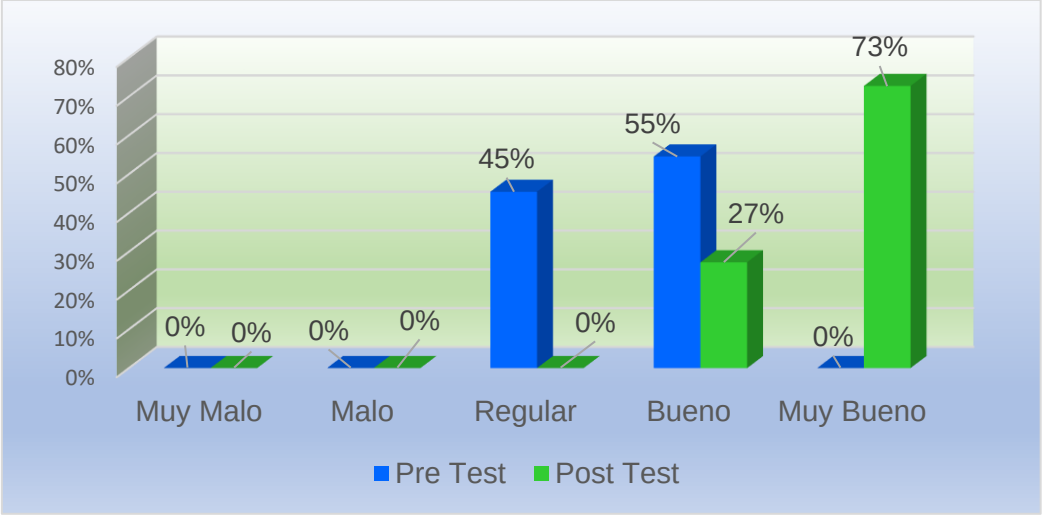
5.1.3 Procesamiento de datos de la dimensión ejecución

Tabla 14: Distribución de frecuencia del pre y post test

Ejecución	Pre Test		Post Test	
	Frecuencia	Porcentajes	Frecuencias	Porcentajes
Muy Malo	0	0%	0	0%
Malo	0	0%	0	0%
Regular	5	45%	0	0%
Bueno	6	55%	3	27%
Muy Bueno	0	0%	8	73%
Total	11	100%	11	100%

Fuente: Anexo 4 y 5

Figura 13: Barras porcentuales del pre y post test



Fuente: tabla 14

En el contexto de la tabla 14 y figura 13, se observa que la plataforma de protección de terminales en la empresa IM SELVA SAC ha demostrado ser altamente efectiva en la mejora de la ejecución de la seguridad de la información. En el pre test, el 45% de las evaluaciones se clasificaron como "Regular" y el 55% como "Bueno", lo que indicaba una ejecución aceptable, pero con margen de mejora. Tras la implementación de la plataforma, los resultados del post test revelan una mejora significativa: el 73% de las evaluaciones se clasificaron como "Muy Bueno" y el 27% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post test, lo que evidencia una eliminación de las deficiencias

previas. Estos resultados confirman que la plataforma ha sido efectiva en la implementación de actividades y tareas, mejorando considerablemente la ejecución de la seguridad de la información en la empresa y cumpliendo con el objetivo planteado en esta investigación.

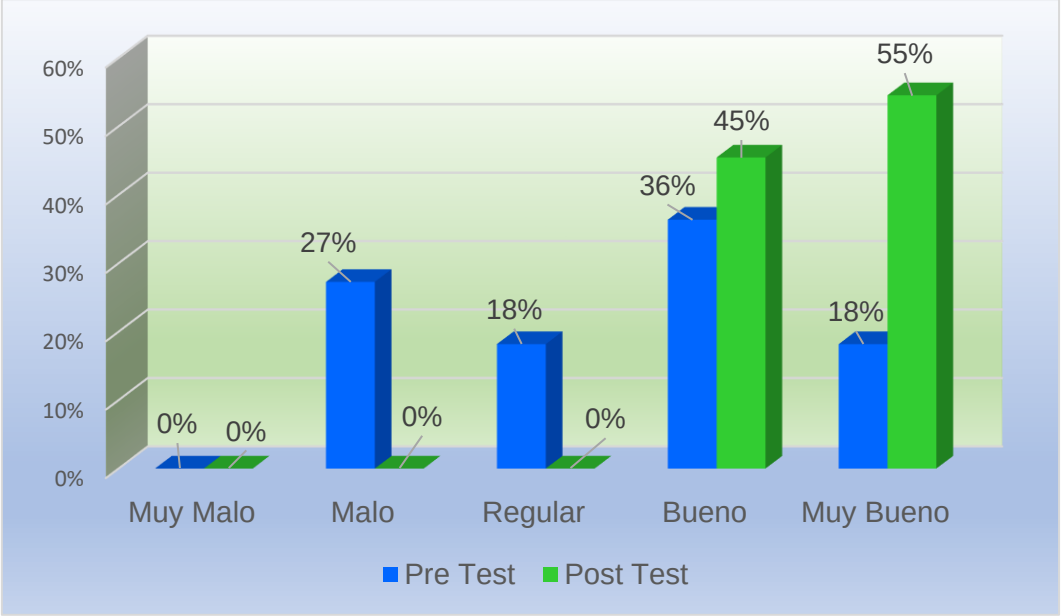
5.1.4 Procesamiento de datos de la dimensión seguimiento

Tabla 15: Distribución de frecuencia del pre y post test

Seguimiento	Pre Test		Post Test	
	Frecuencia	Porcentajes	Frecuencias	Porcentajes
Muy Malo	0	0%	0	0%
Malo	3	27%	0	0%
Regular	2	18%	0	0%
Bueno	4	36%	5	45%
Muy Bueno	2	18%	6	55%
Total	11	100%	11	100%

Fuente: Anexo 4 y 5

Figura 14: Barras porcentuales del pre y post test de la dimensión seguimiento



Fuente: tabla 15

En el contexto de la tabla 15 y figura 14, se observa que la implementación de una plataforma de protección de terminales en la empresa IM SELVA SAC ha permitido establecer pautas claras de seguimiento y control de medidas para mejorar la seguridad de la información. En el pre test, se observó que el 27% de las evaluaciones se clasificaron como "Malo" y el 18% como "Regular", lo que indicaba una falta de seguimiento y control adecuado. Sin embargo, tras la implementación de la plataforma, los resultados del post test muestran una mejora significativa: el 55%

de las evaluaciones se clasificaron como "Muy Bueno" y el 45% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en establecer y mejorar las pautas de seguimiento y control de medidas, cumpliendo con el objetivo de esta investigación y fortaleciendo la seguridad de la información en la empresa.

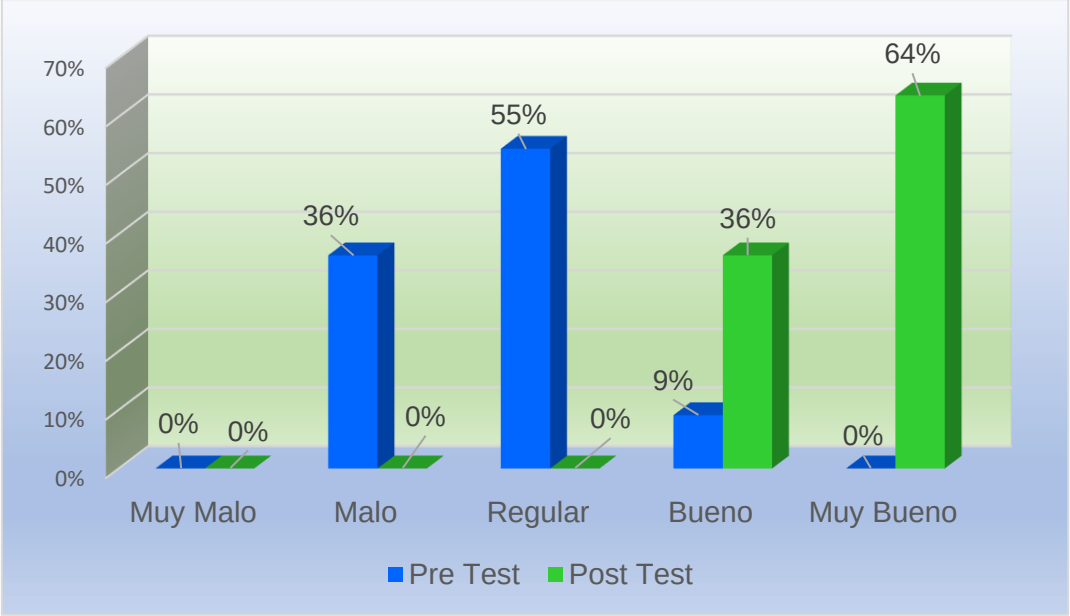
5.1.5 Procesamiento de datos de la dimensión cierre

Tabla 16: Distribución de frecuencia del pre y post test

Cierre	Pre Test		Post Test	
	Frecuencia	Porcentajes	Frecuencias	Porcentajes
Muy Malo	0	0%	0	0%
Malo	4	36%	0	0%
Regular	6	55%	0	0%
Bueno	1	9%	4	36%
Muy Bueno	0	0%	7	64%
Total	11	100%	11	100%

Fuente: Anexo 4 y 5

Figura 15: Barras porcentuales del pre y post test de la dimensión cierre



Fuente: tabla 16

En el contexto de la tabla 16 y figura 15, se observa que la implementación de una plataforma de protección de terminales en la empresa IM SELVA SAC ha permitido identificar y mejorar significativamente las características de seguridad de la información. En el pre test, el 36% de las evaluaciones se clasificaron como "Malo" y el 55% como "Regular", lo que indicaba una seguridad insuficiente y la necesidad de mejoras sustanciales. Tras la implementación de la plataforma, los resultados del

post test muestran una mejora notable: el 64% de las evaluaciones se clasificaron como "Muy Bueno" y el 36% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en mejorar las características de seguridad de la información, cumpliendo con el objetivo de esta investigación y fortaleciendo la protección de los datos en la empresa.

5.2. Prueba de Hipótesis

En todo trabajo de investigación se requiere probar la hipótesis ello se realizó de la variable dependiente, tal como lo menciona (Hernández Sampieri, Fernandez Collado, & Baptista Lucio, 2010), que afirma que “se realiza sobre una variable (regularmente y de manera teórica: dependiente). Si hay diferentes variables, se efectuará varias pruebas” de Wilcoxon.

(Alvarado Pintado & Agurto Mejía, 2009), El procedimiento**,** para probar una hipótesis es:

I. Redacción de las hipótesis.
II. Determinar el nivel de Alfa
III. Elección de la prueba estadística.
IV. Aplicación de la prueba estadística
V. Toma de decisión en la hipótesis general

5.2.1 Prueba de la hipótesis general

I. Redacción de las hipótesis.

H_o = “La Implementar de una Plataforma de Protección de Terminales no mejora la seguridad de la información de la empresa IM SELVA SAC.

H_1 = La Implementar de una Plataforma de Protección de Terminales mejora la seguridad de la información de la empresa IM SELVA SAC.

II. Determinar el nivel de Alfa

$Alfa = 5\ \% = 0.05$, **,**pero como es de doble cola es $\propto = 0.025$”

Nota. Los criterios del nivel de significancia, ya no se presentarán en las demás pruebas de hipótesis porque siempre serán los mismos criterios.

III. Elección de la prueba estadística.

Es un estudio “trasversal de muestras relacionadas, por lo que se aplicara la prueba t de Student.

Lectura de P – Valor.

- Normalidad se debe de corroborar que la variable aleatoria en ambos grupos se distribuye normalmente. Para ello se utilizó la prueba de Chapiro Wilk por que el tamaño de la muestra es menor que 33. El criterio para determinar si la (VA) se distribuye normalmente es:
  - P–valor $\geq \propto$. Aceptar el Ho = Los datos**,** provienen de una distribución normal
  - P–valor $< \propto$. Aceptar la H_1 = Los datos no provienen de una distribución normal.”

Nota. Los criterios de la prueba de normalidad ya no se presentan en las demás pruebas de hipótesis porque siempre serán los mismos criterios.

Tabla 17: Prueba de normalidad de la hipótesis general

Pruebas de normalidad				
	Seguridad de la información	Shapiro-Wilk		
		Estadístico	gl	Sig.
Hipótesis general	Pre Test	,943	11	,551
	Post test	,950	11	,640

*. Esto es un límite inferior de la significación verdadera

a. Corrección de significación de Lilliefors

Fuente: anexo 4 y 5

Tabla 18: Prueba de normalidad de la variable seguridad de la información

Toma de cesión de la prueba de normalidad		
P–valor Grupo de Pre Test = 0.551	$>$	$\propto = 0.025$
P–valor del grupo de Post Test = 0.640	$>$	$\propto = 0.025$

Conclusión: La variable: seguridad de la información de la empresa IM SELVA SAC, se comportan normalmente, por lo que se aplicara la prueba t de Student.

Fuente: tabla 17

IV. Prueba t de Student para muestras relacionadas

El criterio para decidir es:

- Si la “probabilidad obtenida de P–valor $\leq \propto$. Se rechaza el Ho (Se acepta la H_1)
- Si la probabilidad obtenida**,** de P–valor $> \propto$. Se rechaza la H_1 (Se acepta el Ho).”

Tabla 19: Prueba t de Student para muestras relacionadas

Prueba de muestras emparejadas

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
seguridad de la información: Post – Pre Test	1,3742424	,2155566	,0649928	1,2294295	1,5190553	21,145	10	,000

V. Toma de decisión en la hipótesis general

Tabla 20: Toma de decisión de la hipótesis general

Decisión estadística		
P–valor = 0.000	$<$	$\propto = 0.025$

Por lo que se rechaza la Hipótesis nula y se acepta la Hipótesis de Investigación.

La Implementar de una Plataforma de Protección de Terminales mejora la seguridad de la información de la empresa IM SELVA SAC.

Fuente: Tabla 19

5.2.2 Prueba de la primera hipótesis especifica

I. Redacción de las hipótesis.

H_o = “La identificación de los problemas respecto a los sistemas de información no mejora la iniciación de seguridad de la información de la empresa IM SELVA SAC.

H_1 = La identificación de los problemas respecto a los sistemas de información mejora la iniciación de seguridad de la información de la empresa IM SELVA SAC.

II. Elección de la prueba estadística.

Tabla 21: Prueba de normalidad de la primera hipótesis especifica

Pruebas de normalidad

	Seguridad de la información	Shapiro-Wilk		
		Estadístico	gl	Sig.
Primera Hipótesis especifica	Pre Test	,950	11	,641
	Post test	,899	11	,181

*. Esto es un límite inferior de la significación verdadera

a. Corrección de significación de Lilliefors

Fuente: anexo 4 y 5

Tabla 22: Toma de decisión de la prueba de normalidad de la dimensión iniciación.

Toma de cesión de la prueba de normalidad		
P–valor Grupo de Pre Test = 0.641	>	$\propto = 0.025$
P–valor del grupo de Post Test = 0.181	>	$\propto = 0.025$

Conclusión: La dimensión: iniciación en el proceso de seguridad de la información de la empresa IM SELVA SAC, se comportan normalmente, por lo que se aplicara la prueba t de Student.

Fuente: tabla 21

III. Prueba t de Student para muestras relacionadas

El criterio para decidir es:

- Si la "probabilidad obtenida de P–valor $\leq \propto$. Se rechaza el Ho (Se acepta la H_1)
- Si la probabilidad obtenida de P–valor $> \propto$. Se rechaza la H_1 (Se acepta el Ho)."

Tabla 23: Prueba t de Student para muestras relacionadas

Prueba de muestras emparejadas

	Diferencias emparejadas							
				95% de intervalo de confianza de la diferencia				
	Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Iniciación Post – Pre Test	1,2727273	,9045340	,2727273	,6650530	1,8804015	4,667	10	,001

Fuente: anexo 4 y 5

IV. Toma de decisión en la primera hipótesis especifica

Tabla 24: Toma de decisión de la primera hipótesis especifica

	Decisión estadística	
P–valor = 0.001	$<$	$\propto = 0.025$

Por lo que, se rechaza la Hipótesis nula y se acepta la Hipótesis de Investigación. La identificación de los problemas respecto a los sistemas de información mejora la iniciación de seguridad de la información de la empresa IM SELVA SAC.

Fuente: Tabla 23

5.2.3 Prueba de la segunda hipótesis especifica

I. Redacción de las hipótesis.

H_0 = “La implementación de una plataforma de protección de terminales no mejoran la planificación de la seguridad de la información de la empresa IM SELVA SAC.

H_1 = La implementación de una plataforma de protección de terminales mejoran la planificación de la seguridad de la información de la empresa IM SELVA SAC.

II. Elección de la prueba estadística.

Tabla 25: Prueba de normalidad de la segunda hipótesis especifica

Pruebas de normalidad

	Seguridad de la información	Shapiro-Wilk		
		Estadístico	gl	Sig.
Segunda Hipótesis especifica	Pre Test	,909	11	,236
	Post test	,949	11	,635

*. Esto es un límite inferior de la significación verdadera

a. Corrección de significación de Lilliefors

Fuente: anexo 4 y 5

Tabla 26: Toma de decisión de la prueba de normalidad de la dimensión planificación.

Toma de cesión de la prueba de normalidad		
P–valor Grupo de Pre Test = 0.236	$>$	$\propto = 0.025$
P–valor del grupo de Post Test = 0.635	$>$	$\propto = 0.025$

Conclusión: La dimensión: Planificación en el proceso de seguridad de la información de la empresa IM SELVA SAC, se comportan normalmente, por lo que se aplicara la prueba t de Student.

Fuente: tabla 25

III. Prueba t de Student para muestras relacionadas

El criterio para decidir es:

- Si la "probabilidad obtenida de P–valor $\leq \propto$. Se rechaza el Ho (Se acepta la H_1)
- Si la probabilidad obtenida, de P–valor $> \propto$. Se rechaza la H_1 (Se acepta el Ho)."

Tabla 27: Prueba t de Student para muestras relacionadas

Prueba de muestras emparejadas

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
Planificación Post – Pre Test	1,1212121	,6544332	,1973190	,6815579	1,5608663	5,682	10	,000

Fuente: anexo 4 y 5

IV. Toma de decisión de la segunda hipótesis especifica

Tabla 28: Toma de decisión de la segunda hipótesis especifica

Decisión ,estadística		
P–valor = 0.000	$<$	$\propto = 0.025$

Por lo que se rechaza la Hipótesis nula y se acepta la Hipótesis de Investigación.

La implementación de una plataforma de protección de terminales mejora la planificación de la seguridad de la información de la empresa IM SELVA SAC.

Fuente: Tabla 27

5.2.4 Prueba de la tercera hipótesis especifica

I. Redacción de las hipótesis.

H_o = "La implementación de actividades y tareas no mejoran de ejecución de seguridad de la información de la empresa IM SELVA SAC.

H_1 = La implementación de actividades y tareas mejoran de ejecución de seguridad de la información de la empresa IM SELVA SAC.

II. Elección de la prueba estadística.

Tabla 29: Prueba de normalidad de la tercera hipótesis especifica

Pruebas de normalidad

	Seguridad de la información	Shapiro-Wilk		
		Estadístico	gl	Sig.
Tercera Hipótesis especifica	Pre Test	,937	11	,483
	Post test	,909	11	,237

*. Esto es un límite inferior de la significación verdadera

a. Corrección de significación de Lilliefors

Fuente: anexo 4 y 5

Tabla 30: Toma de decisión de la prueba de normalidad de la dimensión ejecución.

Toma de cesión de la prueba de normalidad		
P–valor Grupo de Pre Test = 0.483	$>$	$\propto = 0.025$
P–valor del grupo de Post, Test = 0.237	$>$	$\propto = 0.025$

Conclusión: La dimensión: Ejecución en el proceso de seguridad de la información de la empresa IM SELVA SAC, se comportan normalmente, por lo que se aplicara la prueba t de Student.

Fuente: tabla 29

III. Prueba t de Student para muestras relacionadas

El criterio para decidir es:

Tabla 31: Prueba t de Student para muestras relacionadas

Prueba de muestras emparejadas

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
Ejecución Post – Pre Test	1,2954545	,5456439	,1645178	,9288860	1,6620231	7,874	10	,000

Fuente: anexo 4 y 5

IV. Toma de decisión de la tercera hipótesis especifica

Tabla 32: Toma de decisión de la tercera hipótesis especifica

Decisión estadística		
P–valor = 0.000	$<$	$\propto = 0.025$

Por lo que se rechaza la Hipótesis nula y se acepta la Hipótesis de Investigación.

La implementación de actividades y tareas mejoran de ejecución de seguridad de la información de la empresa IM SELVA SAC.

Fuente: Tabla 31

5.2.5 Prueba de la cuarta hipótesis especifica

I. Redacción de las hipótesis.

H_o = Las pautas de seguimiento, control de medidas y acciones no mejoran la seguridad de la información de la empresa IM SELVA SAC.

H_1 = Las pautas de seguimiento, control de medidas y acciones mejoran la seguridad de la información de la empresa IM SELVA SAC.

II. Elección de la prueba estadística.

Tabla 33: Prueba de normalidad de la cuarta hipótesis especifica

Pruebas de normalidad

	Seguridad de la información	Shapiro-Wilk		
		Estadístico	gl	Sig.
Cuarta Hipótesis especifica	Pre Test	,907	11	,227
	Post test	,893	11	,150

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: anexo 4 y 5

Tabla 34: Toma de decisión de la prueba de normalidad de la dimensión seguimiento.

Toma de cesión de la prueba de normalidad		
P–valor Grupo de Pre Test = 0.227	>	$\propto = 0.025$
P–valor del grupo de Post Test = 0.150	>	$\propto = 0.025$

Conclusión: La dimensión: Seguimiento en el proceso de seguridad de la información de la empresa IM SELVA SAC, se comportan normalmente, por lo que se aplicara la prueba t de Student.

Fuente: tabla 23

III. Prueba t de Student para muestras relacionadas

El criterio para decidir es:

Tabla 35: Prueba t de Student para muestras relacionadas

Prueba de muestras emparejadas

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
Seguimiento Post – Pre Test	1,2272727	1,1037127	,3327819	,4857884	1,9687570	3,688	10	,004

Fuente: anexo 4 y 5

IV. Toma de decisión de la cuarta hipótesis especifica

Tabla 36: Toma de decisión de la cuarta hipótesis especifica

Decisión estadística		
P–valor = 0.000	$<$	$\propto = 0.025$

Por lo que se rechaza la Hipótesis nula y se acepta la Hipótesis de Investigación.

Las pautas de seguimiento, control de medidas y acciones mejoran la seguridad de la información de la empresa IM SELVA SAC.

Fuente: Tabla 35

5.2.6 Prueba de la quinta hipótesis especifica

I. Redacción de las hipótesis.

H_o = Las características de la plataforma de protección de terminales identificadas no mejoran la seguridad de la información de la empresa IM SELVA SAC.

H_1 = Las características de la plataforma de protección de terminales identificadas mejoran la seguridad de la información de la empresa IM SELVA SAC.

II. Elección de la prueba estadística.

Tabla 37: Prueba de normalidad de la quinta hipótesis especifica

Pruebas de normalidad

	Seguridad de la información	Shapiro-Wilk		
		Estadístico	gl	Sig.
Quinta Hipótesis especifica	Pre Test	,920	11	,321
	Post test	,899	11	,181

*. Esto es un límite inferior de la significación verdadera

a. Corrección de significación de Lilliefors

Fuente: anexo 4 y 5

Tabla 38: Toma de decisión de la prueba de normalidad de la dimensión cierre.

Toma decisión de la prueba de normalidad		
P–valor Grupo de Pre Test = 0.321	>	$\propto = 0.025$
P–valor del grupo de Post Test = 0.181	>	$\propto = 0.025$

Conclusión: La dimensión: Cierre en el proceso de seguridad de la información de la empresa IM SELVA SAC, se comportan normalmente, por lo que se aplicara la prueba t de Student.

Fuente: tabla 37

III. Prueba t de Student para muestras relacionadas

El criterio para decidir es:

Tabla 39: Prueba t de Student para muestras relacionadas

Prueba de muestras emparejadas

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo, de confianza de la diferencia Inferior	Superior			
Cierre Post – Pre Test	1,9545455	,6105139	,1840769	1,5443966	2,3646943	10,618	10	,000

Fuente: anexo 4 y 5

IV. Toma de decisión de la quinta hipótesis especifica

Tabla 40: Toma de decisión de la quinta hipótesis especifica

Decisión estadística		
P–valor = 0.000	$<$	$\propto = 0.025$

Por lo que se rechaza la Hipótesis nula y se acepta la Hipótesis de Investigación.

Las características de la plataforma de protección de terminales identificadas mejoran la seguridad de la información de la empresa IM SELVA SAC.

Fuente: Tabla 39

5.3. Discusión

Luego de haber demostrado la hipótesis, se concluyó que la implementación de una plataforma de protección de terminales es una estrategia eficaz para mejorar la seguridad de la información en la empresa IM SELVA SAC. Los datos presentados en la Tabla y Figura 1 evidencian una mejora significativa en los resultados del pre-test y post-test. Inicialmente, el 100% de las evaluaciones se clasificaron como "Regular", lo que indicaba una seguridad de la información insuficiente. Sin embargo, tras la implementación de la plataforma, se observó una notable mejora: el 64% de las evaluaciones se clasificaron como "Bueno" y el 36% como "Muy Bueno". No se registraron evaluaciones en las categorías de "Muy Malo" o "Malo" en ninguno de los dos tests, lo que refuerza la efectividad de la plataforma implementada. Estos resultados confirman que la plataforma de protección de terminales ha cumplido con el objetivo planteado en esta investigación, mejorando considerablemente la seguridad de la información en la empresa.

Por otro lado, la conclusión anterior se contrapone con los hallazgos de Guevara Tucta (2019) en su estudio titulado “Sistema de Gestión de Seguridad de la Información Basado en la Norma**,** ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación”. Guevara Tucta afirma que, por una parte, las claves de usuarios proporcionadas por el departamento de sistemas no se modifican periódicamente y, por otra, no es posible verificar si las claves personales administradas por los mismos funcionarios para el manejo de los sistemas institucionales son lo suficientemente fuertes y confiables.

Ambas conclusiones se encuentran respaldadas por lo que afirma Aarness (2024). Una estrategia de seguridad de endpoints es fundamental, ya que cada punto final remoto puede ser un punto de partida para un ataque. Con el rápido cambio hacia el trabajo remoto, el número de terminales no hará más que aumentar. Según un artículo de Forbes de 2023, el 12,7% de los empleados estadounidenses trabajan de forma remota y el 28,2% tienen acuerdos de trabajo híbridos. Aunque la mayoría de los empleados están actualmente en la oficina, se espera que el número de trabajadores remotos crezca a 32,6 millones para 2025, lo que representará el 22% de la fuerza laboral estadounidense. El riesgo que representan los puntos finales y los datos confidenciales es un desafío que no desaparecerá.

Asimismo, en la primera demostración de la hipótesis específica, se determinó que la identificación y resolución de problemas en los sistemas de información ha contribuido significativamente a la mejora de la seguridad de la información en IM SELVA SAC. El análisis de la Tabla y Figura 2 muestra que la plataforma de protección de terminales ha permitido identificar y abordar problemas críticos en los sistemas de información, mejorando notablemente la seguridad inicial. En el pre-test, el 18% de las evaluaciones se clasificaron como "Malo" y el 36% como "Regular", lo que evidenciaba deficiencias importantes. Sin embargo, tras la implementación de la plataforma, los resultados del post-test muestran una mejora notable: el 64% de las evaluaciones se clasificaron como "Muy Bueno" y el 36% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo" o "Malo" en el post-test, lo que indica una eliminación de los problemas más graves. Estos resultados demuestran que la plataforma ha sido efectiva en

mejorar la seguridad de la información, cumpliendo con el objetivo de identificar y solucionar los problemas existentes en los sistemas de información de la empresa.

Este resultado guarda relación con lo encontrado por Álvarez Basaldúa (2018) en su estudio titulado “Seguridad en Informática (Auditoría de Sistemas)”, donde se afirma que los sistemas pueden mejorar su seguridad aprendiendo de los errores pasados. Las auditorías de los sistemas permiten conocer, en el momento de su realización, la situación exacta de los activos de información en cuanto a protección, control y medidas de seguridad.

Por lo tanto, ambos resultados se encuentran respaldados por lo que afirma Checkpoint (2024). Una solución de protección de terminales debe proporcionar protección integral para terminales y redes empresariales. Algunas de las características básicas de una solución de seguridad para terminales incluyen antimalware, que debe detectar y prevenir infecciones, gusanos y otros tipos de malware.

Asimismo, la planificación de tareas y actividades ha sido optimizada gracias a la implementación de la plataforma de protección de terminales, lo que ha mejorado la seguridad de la información en IM SELVA SAC. Según los datos de la Tabla y Figura 3, en el pre-test, el 73% de las evaluaciones se clasificaron como "Regular" y el 9% como "Malo", lo que indicaba una planificación deficiente. Sin embargo, tras la implementación de la plataforma, los resultados del post-test muestran una mejora significativa: el 64% de las evaluaciones se clasificaron como "Bueno" y el 27% como "Muy Bueno". Solo el 9% permaneció en la categoría de "Regular" y no se registraron evaluaciones en las categorías de "Muy Malo" o "Malo". Estos resultados

demuestran que la plataforma ha sido efectiva en mejorar la planificación de las tareas y actividades, cumpliendo con el objetivo de identificar y fortalecer las características necesarias para una mejor seguridad de la información en la empresa.

Esta investigación guarda relación con lo que afirma Huincho Ramos (2019) en su estudio titulado “Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaría Región Huancavelica”. Huincho Ramos concluye que los usuarios potenciales de la comisaría PNP de la región de Huancavelica, y de manera general de nuestra institución, deben ser capaces de superar el problema cultural, sobreponerse al temor natural y apreciar el horizonte de utilidades, aplicaciones, así como el ahorro de tiempo y dinero que ofrece la seguridad de la información, lo cual será posible a partir de una adecuada implementación y capacitación.

Ambas conclusiones se encuentran respaldadas por lo expresado por Checkpoint (2024). Una solución de protección de terminales debe proporcionar protección integral para terminales y redes empresariales. A medida que crecen el trabajo remoto y el uso de dispositivos personales (BYOD), la capacidad de hacer cumplir las políticas de seguridad de una organización se ha vuelto más importante. La solución de punto final debe evaluar los dispositivos y solo permitir conexiones a la red corporativa si cumplen con la política corporativa.

Asimismo, la implementación de actividades y tareas ha demostrado ser altamente efectiva para mejorar la ejecución de la seguridad de la información en la empresa IM SELVA SAC. Según los datos presentados en la Tabla y Figura 4, los resultados del pre-test y post-test evidencian una mejora

significativa. Inicialmente, el 45% de las evaluaciones se clasificaron como "Regular" y el 55% como "Bueno", lo que indicaba una ejecución aceptable, pero con margen de mejora. Sin embargo, tras la implementación de la plataforma, los resultados del post-test revelan una mejora notable: el 73% de las evaluaciones se clasificaron como "Muy Bueno" y el 27% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post-test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en la implementación de actividades y tareas, mejorando considerablemente la ejecución de la seguridad de la información en la empresa y cumpliendo con el objetivo planteado en esta investigación.

El resultado anterior se encuentra respaldado por lo que encontró Silva Guerrero (2021) en su estudio titulado “Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021”. Silva Guerrero destaca que el compromiso de la alta dirección es crucial para el éxito de la implementación del SGSI, ya que permite involucrar y concientizar a los jefes de áreas y a todo el personal involucrado. Además, proporciona respaldo a las políticas y procedimientos implementados, que deben ser debidamente difundidos y documentados, permitiendo a los trabajadores conocer y entender el SGSI y las tareas y actividades que realizan. La documentación es esencial porque permite estar organizados y tener lineamientos definidos.

Ambos resultados se amparan en lo expresado por Checkpoint (2024), que afirma que una solución de protección de terminales debe proporcionar protección integral para terminales y redes empresariales. La inspección de

zona de pruebas es fundamental, ya que los puntos finales pueden infectarse mediante métodos como phishing y exploits. Las soluciones de seguridad de endpoints deben aislar e inspeccionar archivos en un entorno sandbox para identificar y evitar que contenido malicioso llegue a los endpoints.

Las pautas de seguimiento y control de medidas han mejorado significativamente la seguridad de la información en la empresa IM SELVA SAC. Según los datos presentados en la Tabla y Figura 5, la implementación de una plataforma de protección de terminales ha permitido establecer pautas claras y efectivas de seguimiento y control. En el pre-test, el 27% de las evaluaciones se clasificaron como "Malo" y el 18% como "Regular", lo que indicaba una falta de seguimiento y control adecuado. Sin embargo, tras la implementación de la plataforma, los resultados del post-test muestran una mejora notable: el 55% de las evaluaciones se clasificaron como "Muy Bueno" y el 45% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post-test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en establecer y mejorar las pautas de seguimiento y control de medidas, cumpliendo con el objetivo de esta investigación y fortaleciendo la seguridad de la información en la empresa.

Asimismo, esta investigación guarda relación con los hallazgos de Hernández Pinto (2019), en su estudio titulado “Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial”. En su conclusión, Hernández Pinto destacó que la incomprensión de la Gerencia y la falta de apoyo económico a la gestión de informática para implantar medidas de seguridad provocan una mayor exposición a los riesgos. La seguridad de

la información es una responsabilidad compartida por todos los niveles de la organización, que requiere del apoyo de todos ellos, pero debe estar dirigida por un plan y con la adecuada coordinación.

En concordancia con lo expresado por Cisco (2024), los atacantes se mantienen al día con las últimas tendencias de seguridad para lanzar ataques más sigilosos, lo que hace que las herramientas antivirus tradicionales queden obsoletas. La seguridad de endpoints combina la protección preventiva de una solución EPP con las capacidades de detección y auditoría de un EDR.

Para finalizar, las características de la plataforma de protección de terminales han mejorado significativamente la seguridad de la información en la empresa IM SELVA SAC. Según los datos presentados en la Tabla y Figura 6, la implementación de la plataforma ha permitido identificar y mejorar sustancialmente las características de seguridad de la información. En el pre-test, el 36% de las evaluaciones se clasificaron como "Malo" y el 55% como "Regular", lo que indicaba una seguridad insuficiente y la necesidad de mejoras sustanciales. Sin embargo, tras la implementación de la plataforma, los resultados del post-test muestran una mejora notable: el 64% de las evaluaciones se clasificaron como "Muy Bueno" y el 36% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post-test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en mejorar las características de seguridad de la información, cumpliendo con el objetivo de esta investigación y fortaleciendo la protección de los datos en la empresa.

Los resultados obtenidos guardan relación con los hallazgos de Álvarez Basaldúa (2018) en su estudio titulado “Seguridad en Informática (Auditoría de Sistemas)”. En sus conclusiones, Álvarez Basaldúa destacó que los servicios de auditoría comprenden el estudio de los sistemas para gestionar las vulnerabilidades presentes. Además, señaló que el continuo cambio en las configuraciones, la aparición de parches y mejoras en el software, así como la adquisición de nuevo hardware, hacen necesario que los sistemas estén periódicamente controlados mediante auditorías. Una auditoría de sistemas proporciona una radiografía completa de la situación de estos, asegurando que estén preparados para interconectarse y recomendando la realización de auditorías periódicas.

Ambos resultados se sustentan en la importancia de los terminales, que según Itconnect (2016), son dispositivos de hardware de comunicación electrónica que manejan la entrada y visualización de datos.

CONCLUSIONES

- La implementación de una plataforma de protección de terminales ha demostrado ser una estrategia eficaz para mejorar la seguridad de la información en la empresa IM SELVA SAC. Según los datos presentados en la Tabla y Figura 1, los resultados del pre-test y post-test evidencian una mejora significativa. Inicialmente, el 100% de las evaluaciones se clasificaron como "Regular", lo que indicaba una seguridad de la información insuficiente. Sin embargo, tras la implementación de la plataforma, se observó una notable mejora: el 64% de las evaluaciones se clasificaron como "Bueno" y el 36% como "Muy Bueno". No se registraron evaluaciones en las categorías de "Muy Malo" o "Malo" en ninguno de los dos tests, lo que refuerza la efectividad de la plataforma implementada. Estos resultados confirman que la plataforma de protección de terminales ha cumplido con el objetivo planteado en esta investigación, mejorando considerablemente la seguridad de la información en la empresa.
- La identificación y resolución de problemas en los sistemas de información también ha contribuido significativamente a la mejora de la seguridad de la información en IM SELVA SAC. El análisis de la Tabla y Figura 2 muestra que la plataforma de protección de terminales ha permitido identificar y abordar problemas críticos en los sistemas de información, mejorando notablemente la seguridad inicial. En el pre-test, el 18% de las evaluaciones se clasificaron como "Malo" y el 36% como "Regular", lo que evidenciaba deficiencias importantes. Tras la implementación de la plataforma, los resultados del post-test muestran una mejora notable: el 64% de las evaluaciones se clasificaron como "Muy Bueno" y el 36% como "Bueno".

No se registraron evaluaciones en las categorías de "Muy Malo" o "Malo" en el post-test, lo que indica una eliminación de los problemas más graves. Estos resultados demuestran que la plataforma ha sido efectiva en mejorar la seguridad de la información, cumpliendo con el objetivo de identificar y solucionar los problemas existentes en los sistemas de información de la empresa.

- Asimismo, la planificación de tareas y actividades ha sido optimizada gracias a la implementación de la plataforma de protección de terminales, lo que ha mejorado la seguridad de la información en IM SELVA SAC. Según los datos de la Tabla y Figura 3, en el pre-test, el 73% de las evaluaciones se clasificaron como "Regular" y el 9% como "Malo", lo que indicaba una planificación deficiente. Tras la implementación de la plataforma, los resultados del post-test muestran una mejora significativa: el 64% de las evaluaciones se clasificaron como "Bueno" y el 27% como "Muy Bueno". Solo el 9% permaneció en la categoría de "Regular" y no se registraron evaluaciones en las categorías de "Muy Malo" o "Malo". Estos resultados demuestran que la plataforma ha sido efectiva en mejorar la planificación de las tareas y actividades, cumpliendo con el objetivo de identificar y fortalecer las características necesarias para una mejor seguridad de la información en la empresa.
- También la implementación de actividades y tareas ha demostrado ser altamente efectiva para mejorar la seguridad de la información en la empresa IM SELVA SAC. Según los datos presentados en la Tabla y Figura 4, los resultados del pre-test y post-test evidencian una mejora significativa. Inicialmente, el 45% de las evaluaciones se clasificaron como "Regular" y

el 55% como "Bueno", lo que indicaba una ejecución aceptable, pero con margen de mejora. Tras la implementación de la plataforma, los resultados del post-test revelan una mejora notable: el 73% de las evaluaciones se clasificaron como "Muy Bueno" y el 27% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post-test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en la implementación de actividades y tareas, mejorando considerablemente la ejecución de la seguridad de la información en la empresa y cumpliendo con el objetivo planteado en esta investigación.

- Las pautas de seguimiento y control de medidas han mejorado significativamente la seguridad de la información en la empresa IM SELVA SAC. Según los datos de la Tabla y Figura 5, la implementación de una plataforma de protección de terminales ha permitido establecer pautas claras de seguimiento y control de medidas. En el pre-test, el 27% de las evaluaciones se clasificaron como "Malo" y el 18% como "Regular", lo que indicaba una falta de seguimiento y control adecuado. Sin embargo, tras la implementación de la plataforma, los resultados del post-test muestran una mejora significativa: el 55% de las evaluaciones se clasificaron como "Muy Bueno" y el 45% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post-test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en establecer y mejorar las pautas de seguimiento y control de medidas, cumpliendo con el objetivo de

esta investigación y fortaleciendo la seguridad de la información en la empresa.

- Para finalizar las características de la plataforma de protección de terminales han mejorado significativamente la seguridad de la información en la empresa IM SELVA SAC. Según los datos de la Tabla y Figura 6, la implementación de la plataforma ha permitido identificar y mejorar sustancialmente las características de seguridad de la información. En el pre-test, el 36% de las evaluaciones se clasificaron como "Malo" y el 55% como "Regular", lo que indicaba una seguridad insuficiente y la necesidad de mejoras sustanciales. Tras la implementación de la plataforma, los resultados del post-test muestran una mejora notable: el 64% de las evaluaciones se clasificaron como "Muy Bueno" y el 36% como "Bueno". No se registraron evaluaciones en las categorías de "Muy Malo", "Malo" o "Regular" en el post-test, lo que evidencia una eliminación de las deficiencias previas. Estos resultados confirman que la plataforma ha sido efectiva en mejorar las características de seguridad de la información, cumpliendo con el objetivo de esta investigación y fortaleciendo la protección de los datos en la empresa.

RECOMENDACIONES

- Se recomienda realizar un diagnóstico exhaustivo de los sistemas de información actuales, identificando vulnerabilidades y puntos críticos que puedan comprometer la seguridad de la información. Este diagnóstico debe incluir una evaluación de las políticas de seguridad existentes, la infraestructura tecnológica y los procedimientos operativos. Además, es fundamental involucrar a todos los niveles de la organización para obtener una visión completa y precisa de los problemas existentes.
- Es esencial desarrollar un plan detallado que contemple todas las tareas y actividades necesarias para mejorar la seguridad de la información. Este plan debe incluir la definición de roles y responsabilidades, la asignación de recursos y la elaboración de un cronograma de implementación. Asimismo, se recomienda establecer indicadores de desempeño que permitan medir el avance y la efectividad de las acciones emprendidas.
- La implementación debe seguir un enfoque estructurado y sistemático, asegurando que todas las actividades y tareas se realicen de acuerdo con el plan establecido. Se recomienda utilizar metodologías ágiles que permitan una adaptación rápida a posibles cambios y la resolución eficiente de problemas. Además, es crucial capacitar al personal en el uso de la nueva plataforma y en las mejores prácticas de seguridad de la información.
- Para garantizar la sostenibilidad de las mejoras implementadas, es necesario establecer un sistema de seguimiento y control continuo. Este sistema debe incluir la realización de auditorías periódicas, la monitorización constante de los sistemas y la actualización regular de las medidas de seguridad. También se recomienda crear un comité de

seguridad de la información que supervise y coordine todas las acciones relacionadas con la protección de los datos.

- Es fundamental seleccionar una plataforma de protección de terminales que se ajuste a las necesidades específicas de la empresa. Esta plataforma debe ofrecer funcionalidades avanzadas de detección y respuesta ante amenazas, protección contra malware y gestión centralizada de la seguridad. Además, se recomienda evaluar la escalabilidad y flexibilidad de la plataforma para asegurar que pueda adaptarse a futuros requerimientos y cambios en el entorno tecnológico.

REFERENCIAS BIBLIOGRÁFICAS

Aarness, A. (2024). *crowdstrike*. Obtenido de https://www.crowdstrike.com/cybersecurity-101/endpoint-security/

Alay, B. (2024). *Gestión del talento humano y su efecto en la atención a los usuarios en la terminal terrestre de la ciudad de jipijapa, año 2023*. [Tesis de licenciatura, Universidad Estatal del Sur de Manabí, Ecuador]. https://repositorio.unesum.edu.ec/bitstream/53000/6967/1/Alay%20Miranda%20Brigitte%20Nicole.pdf

Alvarez, L. (2018). *Seguridad en informática (AUDITORÍA DE SISTEMAS).* Mexico: UI.

Careemergencytoolkit. (2024). Obtenido de https://www.careemergencytoolkit.org/topics-issues/5-protection/1-introduction/1-1-definition-of-protection/

Checkpoint. (2024). *checkpoint*. Obtenido de https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-security/

Cisco. (2024). *cisco*. Obtenido de https://www.cisco.com/c/en/us/products/security/endpoint-security/index.html

Estrada, S. y Guadamud, J. (2022). Percepción de inseguridad y violencia contra las mujeres en los espacios de uso público de los terminales terrestres. *Polo del Conocimiento,* 7(10). https://polodelconocimiento.com/ojs/index.php/es/article/view/4825

Fortinet. (2024). *fortinet*. Obtenido de https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security

Freire, D. y Hidalgo, D. (2024). *Simulación de la automatización del proceso de despacho de combustible y monitoreo mediante una plataforma basada en IOT para un terminar.* [tesis de licenciatura, Universidad Politécnica Salesiana, Ecuador]. https://dspace.ups.edu.ec/bitstream/123456789/26817/1/UPS-GT004926.pdf

Gladys, N. (2006). *Redalyc.*

Gómez, C. y Mero, F. (2023). *Propuesta de mejora de control de inventario de equipos de protección personal en un terminar portuario.* [Tesis de licenciatura, Universidad Politécnica Salesiana, Ecuador]. https://dspace.ups.edu.ec/bitstream/123456789/25099/1/UPS-GT004434.pdf

Goyzueta, J. (2023). *Instalación, supervisión, mantenimientos preventivos y correctivos de terminales de autoservicio (ATM'S) y sistemas electrónicos de seguridad para el sistema bancario.* [tesis de licenciatura, Universidad Católica de Santa María]. https://repositorio.ucsm.edu.pe/server/api/core/bitstreams/1dd6a1e9-5926-4a73-853e-f2cc50b6761b/content

Guevara, R. A. (2019). *SGSI basado en la norma iso 27001 para el dpto de tecnologías de la información y comunicación del distrito 18d01 de educación.* Ambato: UTA.

Hernández, M. (2019). *Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial.* Guayaquil: ESPL.

Huincho, W. (2019). *SGSI para mejorar la protección de tipo informática de la Comisaria de la Región Huancavelica.* Cerro de Pasco: UNDAC.

Ibarra, C. (2011). *Metodología de la Investigación.*

Itconnect. (22 de 11 de 2016). Obtenido de https://itconnect.uw.edu/tools-services-support/teaching-learning/workshops/online-tutorials/what-is-a-terminal/

López, M., Montes, R. y Ramírez, M. (2023). Evaluación de riesgos (ER) en un terminal de buques tanqueros basada en la norma ISO-31000:2018 y técnicas cuali-cuantitativas. Ingeniería, 33(2). https://www.scielo.sa.cr/pdf/ingenieria/v33n2/2215-2652-ingenieria-33-02-99.pdf

Lutkevich, B. (16 de 03 de 2024). *techtarget*. Obtenido de https://www.techtarget.com/searchcustomerexperience/definition/implementation

Murillo, W. (2008). *Investigacion Científica.*

Pinzón, S., Acevedo, G., León, J y Granados, M. (2021). Desarrollo e implementación de unidad de monitoreo remoto para aplicaciones de protección catódica. *Repositorio Universidad de Pamplona,* 1(1). https://www.unipamplona.edu.co/unipamplona/portalIG/home_79/recursos/memorias/memorias_cieta_2023/11032024/cieta-2023-100.pdf

Rouse, M. (2020). *techopedia*. Obtenido de https://www.techopedia.com/definition/3411/platform-computing

Ruíz, T. (2022). *Terminal terrestre interprovincial e internacional en el sur de Lima.* [Tesis de licenciatura, Universidad Peruana de Ciencias Aplicadas]. https://repositorioacademico.upc.edu.pe/handle/10757/660291

Sharma, S. (2023). *Analisis Cuantitativo*. Obtenido de Hotjar: https://www.hotjar.com/quantitative-data-analysis/

Silva Guerrero, A. (2021). *Implementación de un SGSI para mejorar la SI en una empresa MYPE - 2021.* Lima: UTP.

Simplilearn. (2023). Obtenido de https://www.simplilearn.com/what-is-data-collection-article

Vergara Quiroz, G. (2017). *Seguridad de información y la calidad del servicio en la Universidad Nacional Federico Villarreal.* Lima: UCV.

ANEXOS

Anexo 1. Matriz de consistencia

<table>
<tr><th>PROBLEMAS</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES</th><th>METODOLOGÍA DE LA INVESTIGACIÓN</th></tr>
<tr>
<td>¿La implementación de una Plataforma de Protección de Terminales mejora la seguridad de la información de la Empresa IM SELVA SAC?</td>
<td>Demostrar que la Plataforma de Protección de Terminales para la mejora de seguridad de la información de la empresa IM SELVA SAC.</td>
<td>La Implementación de una Plataforma de Protección de Terminales mejora la seguridad de la información de la empresa IM SELVA SAC.</td>
<td rowspan="2">Variable independiente:
Plataforma de Terminales
<table>
<tr><th>Dimensión</th><th>Indicador</th></tr>
<tr><td>Evaluación</td><td>Soluciones de Protección de Terminales.</td></tr>
<tr><td>Características.</td><td>Características de la solución de Protección de Terminales</td></tr>
<tr><td>Controles</td><td>Configuraciones de controles de seguridad.</td></tr>
<tr><td>Seguridad</td><td>Nivel de seguridad de los activos de TI.</td></tr>
</table>
Variable dependiente:
Seguridad de la Información.
<table>
<tr><th>Dimensión</th><th>Indicador</th></tr>
<tr><td>Iniciación</td><td>Problemas.</td></tr>
<tr><td>Planificación</td><td>Roles.
Responsabilidades.
Control.</td></tr>
<tr><td>Ejecución</td><td>Activos.
Políticas.
Riegos.
Controles.</td></tr>
<tr><td>Seguimiento</td><td>Indicadores</td></tr>
<tr><td>Cierre</td><td>Conformidad.</td></tr>
</table>
</td>
<td rowspan="2">Tipo de Investigación:
Investigación Aplicada

Nivel de Investigación:
Nivel Experimental

Método de Investigación:
Deductivo

Diseño de la Investigación:
Diseño Experimental

Población
Esta comprendido de todo el personal de TI quienes tienen como función principal salvaguardar la información de la organización, estos empleados hacen un total de 11, que lo conformar 01 jefe, 02 Administradores de Servidores, 02 Administradores de Sistemas, 04 Asistentes de TI y 02 de soporte.

Muestra
Porque el número total de usuarios no es grande, es conveniente hacer uso del método no probabilístico. Por lo tanto, se optó por un muestreo por conveniencia y la muestra es</td>
</tr>
<tr>
<td>• ¿Cuáles son los problemas respecto a los sistemas de información que corresponden a la mejora la seguridad de la información de la empresa IM SELVA SAC?
• ¿Qué características posee la planificación de la tares y actividades para la mejora de seguridad de la información de la empresa IM SELVA SAC?
• ¿Cuáles con las actividades y tareas a implementarse, para la mejora de seguridad de la información de la empresa IM SELVA SAC?
• ¿De qué manera el seguimiento, control de</td>
<td>• Identificar los problemas respecto a los sistemas de información que corresponden para mejorar la seguridad de la información de la empresa IM SELVA SAC.
• Determinar las características posee la planificación de la tares y actividades para mejorar de seguridad de la información de la empresa IM SELVA SAC.
• Implementar las actividades y tareas para mejorar de seguridad de la información de la</td>
<td>• La identificación de los problemas respecto a los sistemas de información mejora la seguridad de la información de la empresa IM SELVA SAC.
• Las características de la planificación de la tares y actividades mejoran la de seguridad de la información de la empresa IM SELVA SAC.
• La implementación de actividades y tareas mejoran de seguridad de la información de la empresa IM SELVA SAC.
• Las pautas de seguimiento, control de medidas y acciones mejoran la seguridad de la información de la empresa IM SELVA SAC.</td>
</tr>
</table>

medidas y acciones implementadas mejoran la, seguridad de la información de la empresa IM SELVA SAC? • ¿Qué características posee la plataforma de protección de terminales para mejorar la seguridad de la información de la empresa IM SELVA SAC?	empresa IM SELVA SAC. • Determinar las pautas de seguimiento, control de medidas y acciones para mejorar la seguridad de la información de la empresa IM SELVA SAC. • Identificar las características de la plataforma de protección de terminales para mejorar la seguridad de la información de la empresa IM SELVA SAC.	• Las características de la plataforma de protección de terminales identificadas mejoran la seguridad de la información de la empresa IM SELVA SAC.		el total de la población, siendo este un número total de 11 empleados.

Anexo 2. Cuestionario de preguntas, para la recolección de datos

CUESTIONARIO: IMPLEMENTACIÓN DE UNA PLATAFORMA DE PROTECCIÓN TERMINALES PARA LA SEGURIDAD DE LA INFORMACIÓN

"Implementación de una Plataforma de Protección Terminales para la seguridad de la información de la empresa IM SELVA SAC.".

INDICACIONES

- Marque con X en el cuadro que considere**,** el valor adecuado como respuesta**,** a las preguntas específicas.

LEYENDA

Descripción	Muy Malo	Malo	Regular	Bueno	Muy Bueno
Valoración	1	2	3	4	5

ESCALA DE LIKERT

Variable dependiente: Seguridad de Información

P1. Según su apreciación, ¿Qué valoración le asignaría al número de problemas presentados con respecto a la seguridad**,** de la información?

Valoración	1	2	3	4	5

P2. Según su apreciación, ¿Qué valoración le asignaría al número de problemas presentados de seguridad de**,** la información solucionados?

Valoración	1	2	3	4	5

P3. Según su apreciación, ¿Qué valoración les asignaría a los roles asignados al personal para atender actividades**,** de seguridad de la información?

Valoración	1	2	3	4	5

P4. Según su apreciación, ¿Qué valoración les asignaría a las responsabilidades asignadas al personal para atender actividades de seguridad de la información?

Valoración	1	2	3	4	5

P5. Según su apreciación, ¿Qué valoración les asignaría a controles propuestos para la seguridad de la información?

Valoración	1	2	3	4	5

P6. Según su apreciación, ¿Qué valoración les asignaría a los activos de información críticos que son gestionados por la seguridad de la información?

Valoración	1	2	3	4	5

P7. Según su apreciación, ¿Qué valoración les asignaría a las políticas de seguridad de la información para salvaguardar los activos críticos?

Valoración	1	2	3	4	5

P8. Según su apreciación, ¿Qué valoración le asignaría al proceso de gestión de riesgos de los activos críticos de información?

Valoración	1	2	3	4	5

P9. Según su apreciación, ¿Qué valoración a los controles implementados para garantizar la seguridad de la información?

Valoración	1	2	3	4	5

P10. Según su apreciación, ¿Qué valoración a la forma de gestionar los indicadores de seguimiento de gestión de la seguridad de la información?

Valoración	1	2	3	4	5

P11. Según su apreciación, ¿Qué valoración a la conformidad por la gestión de la seguridad de la información implementada?

Anexo 3. Validación de los instrumentos por expertos

I. DATOS PERSONALES

1.1. APELLIDO Y NOMBRE DEL INFORMANTE: .....
1.2. GRADO ACADÉMICO: .....
1.3. INSTITUCIÓN DONDE LABORA: .....
1.4. TÍTULO DE LA INVESTIGACIÓN: .....
.....
1.5. AUTOR DEL INSTRUMENTO: .....
1.6. NOMBRE DEL INSTRUMENTO: .....

II. ASPECTO A EVALUAR: (CALIFICACIÓN CUANTITATIVA)

INDICADORES DEL INSTRUMENTO DE EVALUACION	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01. CLARIDAD	Está formulado con lenguaje apropiado.					
02. OBJETIVIDAD	Está expresado con conductas observables.					
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad.					
04. ORGANIZACIÓN	Existe una organización lógica del instrumento.					
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad.					
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos.					
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios.					
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores.					
09. METODOLOGIA	Las estrategias responden al propósito del estudio.					
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías.					
Sub Total						
TOTAL						

Valoración cuantitativa (total x0.4) .....
Valoración cualitativa .....
Valoración de aplicabilidad .....

Leyenda:
01-13 Importante
14-16 Aceptable con recomendación
17-20 Aceptable

Lugar y Fecha: .....
Firma y Post – Firma del Experto: .....
DNI: .....

39

Anexo 4. Base de datos

Pre test de la variable seguridad de la información

Seguridad de la Información																			
Codigo	Iniciación			Planificación				Ejecución					Seguimiento			Cierre			Variable
	Items_1	Items_2		Items_3	Items_4	Items_5		Items_6	Items_7	Items_8	Items_9		Items_10	Items_11		Items_12	Items_13		
1	3	1	2.00	3	3	4	3.33	1	5	5	1	3	5	4	4.50	2	5	3.50	3.267
2	2	4	3.00	3	1	4	2.67	3	3	2	4	3	5	4	4.50	2	1	1.50	2.933
3	3	2	2.50	5	2	3	3.33	5	4	3	5	4	2	1	1.50	3	1	2.00	2.717
4	5	4	4.50	3	1	5	3.00	2	4	5	3	4	2	1	1.50	2	3	2.50	3.000
5	2	4	3.00	2	4	5	3.67	2	2	1	5	3	4	3	3.50	2	3	2.50	3.033
6	5	2	3.50	1	2	5	2.67	2	3	5	5	4	2	3	2.50	3	1	2.00	2.883
7	3	4	3.50	2	3	4	3.00	3	5	5	1	4	4	3	3.50	2	3	2.50	3.200
8	1	3	2.00	3	1	2	2.00	3	5	3	4	4	4	3	3.50	3	2	2.50	2.750
9	1	4	2.50	1	5	3	3.00	3	2	5	1	3	4	3	3.50	2	4	3.00	2.950
10	4	3	3.50	5	4	5	4.67	2	1	3	4	3	3	3	3.00	3	2	2.50	3.233
11	3	5	4.00	4	1	4	3.00	2	4	5	5	4	2	2	2.00	3	1	2.00	3.000

Post test de la variable seguridad de la información

Seguridad de la Información																			
Codigo	Iniciación			Planificación				Ejecución					Seguimiento			Cierre			Variable
	Items_1	Items_2		Items_3	Items_4	Items_5		Items_6	Items_7	Items_8	Items_9		Items_10	Items_11		Items_11	Items_12		
1	4	4	4.0000	3	5	5	4.3333	5	4	5	5	4.7500	4	5	4.5000	5	4	4.50	4.4167
2	4	4	4.0000	3	5	4	4.0000	5	4	3	4	4.0000	4	4	4.0000	5	3	4.00	4.0000
3	3	5	4.0000	3	5	3	3.6667	5	4	5	4	4.5000	5	4	4.5000	5	4	4.50	4.2333
4	3	4	3.5000	5	4	3	4.0000	5	4	5	5	4.7500	4	4	4.0000	5	3	4.00	4.0500
5	5	4	4.5000	5	5	5	5.0000	5	4	3	5	4.2500	4	5	4.5000	4	5	4.50	4.5500
6	5	4	4.5000	5	5	3	4.3333	5	5	5	5	5.0000	4	3	3.5000	3	4	3.50	4.1667
7	5	4	4.5000	4	5	3	4.0000	5	5	5	5	5.0000	5	5	5.0000	5	5	5.00	4.7000
8	4	5	4.5000	4	3	3	3.3333	4	5	4	5	4.5000	4	4	4.0000	5	5	5.00	4.2667
9	5	4	4.5000	5	5	5	5.0000	4	4	5	4	4.2500	4	4	4.0000	3	5	4.00	4.3500
10	5	5	5.0000	4	4	5	4.3333	5	4	5	5	4.7500	5	4	4.5000	4	5	4.50	4.6167
11	5	5	5.0000	4	5	5	4.6667	5	5	5	5	5.0000	4	5	4.5000	4	5	4.50	4.7333

Anexo 5. Estructura de fichas para la aplicación de un Sistema de Protección de Terminales

- Alcance del SGSI

Alcance del SGSI

Objetivos:

Precisar los límites del SGSI, donde se va a aplicar (procesos), que recursos se van a utilizar, en que tiempo, el costo; para ellos, se definen los siguientes entregables.

- Descripción del problema.
- Acta de constitución.

Alcance:

El SGSI será aplicado al proceso relacionado con las tecnologías de información.

Presupuesto:

La implementación del SGSI para el proceso de tecnologías de la información, se ha estimado en un valor de S/. ###, ###.##

Equipo de trabajo:

Será labor del comité de SGSI, conformado por los jefes de aminoración, presupuesto, informática.

Cronograma:

Según los detallado en el cronograma de la investigación.

- Fecha de control del documento

Fecha de control del documento

Nombre del documento

Código: XXXXX
Versión: XXXXX
Fecha de versión: XX/XX/XXXX
Creado por:
Aprobado por:
Nombre del archivo:

Historia de revisiones

Fecha	Versión	Modificado/creado	Descripción

Aprobación

Fecha	Nombre	Cargo	Sello y firma

- Fechar entrevista

Fechar entrevista

Esta entrevista se desarrolla con el objetivo de obtener información que describa el estado actual de la empresa con respecto a la seguridad de la información, se conocerá los requerimientos y necesidades de la organización precisa; por lo cual, debe responder las preguntas de manera concisa y de forma clara.
En cada una de las preguntas deberá responder con un sí o no, y luego deberá argumentar su respuesta:

Activo de información

Activos			
Pregunta	**Si**	**No**	**Detallar**
1. ¿Usted considera que es importante identificar y conocer los activos de información que maneja su área?			
2. ¿Ud. considera que se ha logrado identificar cuáles son los activos críticos de información el posee su área?			
3. ¿Cree usted que los activos de información obtenido poseen controles de garantizar la seguridad de los mismos?			
Amenazas			
4. ¿Usted tiene identificado cuáles son las amenazas que atentan contra sus activos de información?			
5. ¿Ud. que cree de las amenazas identificadas sobre los activos de información se encuentran bajo control?			
Vulnerabilidades			
6. ¿Usted tiene identificado las vulnerabilidades y afectan directamente sobre sus activos de información?			
7. ¿En las últimas semanas o meses ud. ha logrado identificar nuevas vulnerabilidades?			

Incidentes			
8. ¿Usted sabe, quién frecuencia se producen incidentes sobre los activos de información?			
9. ¿usted tiene identificado los incidentes de los activos de información?			
Controles			
10. ¿Ud. considera que los controles implementados asegurar los activos de información?			
11. ¿Usted cree que es fácil mantener los controles aplicados sobre los activos de información?			
Políticas			
12. ¿Cree usted que las políticas documentadas son importantes?			
13. ¿Cree usted que las políticas documentadas no interfieren con las actividades?			
Procedimiento			
14. ¿Cree ud. que los procedimientos documentados son importantes?			
15. ¿Cree usted los procedimientos no interfieren con sus actividades?			
16. ¿Cree ud. que los procedimientos ayudan a las actividades?			
Confidencialidad			
17. ¿Cree usted que los controles preservan la confidencialidad?			
Integridad			
18. ¿Cree usted que los controles preservan la integridad?			
Disponibilidad			
19. ¿Cree usted que los controles preservan la disponibilidad?			

- Informe costo-beneficio

Informe de costo – beneficio

Debido a la falta de seguridad la empresa ha pasado por problemas; en tal sentido, se ha estimado que producto de ello si altos costos han sido afectados los cuales influye de forma negativa en la organización.

Beneficios logrados por la implementación del SGSI

- **Costos de penalidades de carácter legal o riesgos asociados**

Criterios	**Costo S/ (anual)**
○ Perdida de continuidad en el servicio:	15, 000.00
○ Incumplimiento de procedimientos	4, 000.00
○ En cumplimiento o de protección de datos personales de acuerdo a ley.	20, 000.00
○ Perdida de equipos informáticos	15, 000.00
○ Incumplimiento de contratos con clientes.	5, 000.00
○ Penalización por el uso de programas no Licenciado.	20, 000.00
○ Perdida por la modificación de activos de información	8, 000.00
○ Incidentes en procesos y/o comparaciones	25, 000.00
Total	112, 000.00

- **Costos de implementación SGSI**

Criterios	Costo S/
○ Servicios	5, 200.00
○ Hardware	32, 000.00
○ Software	5. 000.00
○ Materiales	500.00
Total	42, 000.00

Costo : S/ 42, 000.00

Beneficio : S/ 69, 300.00

Beneficio/Costo : S/ 1.623 (beneficio superior al costo)

- Política de seguridad

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:

Versión:

Fecha de la de la versión:

Creado por:

Aprobado por:

Nombre del archivo:

Historias de revisiones

Fecha	Versión	Modificado/creado	Descripción

Aprobación

Fecha	Nombre	Cargo	Firma

Objetivo:

Salvaguardar los activos de información con la protección de la confidencialidad, integridad y disponibilidad, de toda la información que se manejan en el desarrollo de las actividades dentro de la organización.

Para el desarrollo de las políticas es necesario que se tome en cuenta la norma técnica de Peruana NTP-ISO/IEC 27001:2014, debido a que esta norma posee las vías adecuadas para la implementación correcta de un SGSI.

Alcance

Comprender a todos los colaboradores de la organización que poseen el vínculo laboral adecuado que les permita gestionar y tener acceso a los activos de información en cada uno de los procesos de estos desarrollan**.**

Los que se listan continuación son las políticas desarrolladas en la organización:

- **Seguridad de la información**
- **El área de recurso humanos**
- **Gestión de los activos**
- **Control de los accesos**
- **Criptografía de datos**
- **Seguridad física de también ambiental**
- **Seguridad de operaciones**
- **Seguridad de comunicación**
- **Relaciones con proveedores**
- **Gestión de incidentes**

- Manual de gestión

Manual de gestión de riesgos y oportunidades

Código:

Versión:

Fecha de versión:

Creado por:

Nombre del archivo:

Nivel de confidencialidad:

Historias de revisiones

Fecha	Versión	Modificado/creado	Descripción

Aprobación

Fecha	Nombre	Cargo	Firma

Definición del riesgo:

Viene a ser un evento que puede ocurrir y puede impedir el desarrollo de los procesos y actividades tener ambas y posibles pérdidas de tipo intangible o tangibles en la organización; por lo cual, es importante estimar la probabilidad y el impacto de estos.

Objetivo

Definir como un día con la finalidad de identificar evaluar y tratar los riesgos relacionados directamente con los activos de información con la finalidad de poder minimizar y prevenir cualquier posible daño.

Alcance

Este documento debe ser aplicado por todas las áreas de la organización

Gestión de riesgos y las oportunidades

Establecimiento del contexto

Análisis y valoración de riesgo

Tratamiento de riesgo

Oportunidades de seguridad para

- Análisis de riesgos

Análisis y valoración de los riesgos													
Nº	Id Activo	Activo	Valoración	Id Riesgo	Riesgo	Amenaza	Vulnerabilidad	Afecta			Riesgo Inherente		
								C	I	D	probabilidad	Cálculo de riesgo	Nivel de riesgo

A continuación, se muestra el análisis la valoración

Análisis y valoración de los riesgos								
Id Activo	Activo	Valoración	Afecta			Riesgo Inherente		
			C	I	D	probabilidad	Impacto	Nivel de riesgo
A1	Área de TI	Alto	X	X	X	Casi nunca	Desastroso	Tolerable
A2	Data center	Alto	X	X	X	Casi nuca	Desastroso	Tolerable
A3	Información	Muy alto	X	X	X	Probable	Mayor	Intolerable
A4	Datos de empleados	Medio	X	X	X	Probable	Mayor	Intolerable
A5	Datos de clientes	Muy alto	X	X	X	Probable	Mayor	Intolerable
A6	proxy	Alto	X	X	X	Probable	Moderado	Intolerable
A7	Servicios AD	Alto	X	X	X	Probable	Moderado	Intolerable
A8	Archivos compartidos	Medio	X	X	X	Muy Probable	Moderado	Extremo
A9	Correos electrónicos	Medio	X	X	X	Probable	Moderado	Tolerable
A10	Reportes	Valor alto	X	X	X	Muy probable	Mayor	Extremo
…	…	…	…	…	…	…	…	…

- Tratamiento de riesgos

Tratamiento de los riesgos y el establecimiento de controles

Tratamiento y selección de controles													
No	Id Activo	Activo	Nivel de riesgo	Estrategias	Categoría de control	Tipos	Controles preventivos o correctivos	Riego Residual					
								P	I	R	Riego residual	Eficacia del control	

Controles: Puede ser (preventivo, defectivo el correctivo)

Análisis y valoración de los riesgos						
Id Activo	Activo	Nivel de riesgo	Estrategia	Controles	Nivel residual	Eficacia
A1	Área de TI	Tolerable	Reducir	Detectores de humo, fuego, extintores	Aceptable	65%
A2	Data center	Intolerable	Reducir	Detectores de humo, fuego, extintores, UPS, sensores de temperatura	Aceptable	70%
A3	Información	Intolerable	Reducir	Copias de seguridad, equipos endpoint	Aceptable	60%
A4	Datos de empleados	Intolerable	Reducir	Copias de seguridad, equipos endpoint	Aceptable	60%

A5	Datos de clientes	Intolerable	Reducir	Copias de seguridad, equipos endpoint	Aceptable	60%
A6	proxy	Intolerable	Reducir	Configuración, documentación, restricciones	Tolerable	54%
A7	Servicios AD	Extremo	Reducir	Configuración, documentación, restricciones	Tolerable	50%
A8	Archivos compartidos	Tolerable	Reducir	Configuración, documentación, restricciones, equipos endpoint	Aceptable	60%
A9	Correos electrónicos	Extremo	Reducir	Configuración, documentación, restricciones, equipos endpoint	Aceptable	60%
A10	Reportes	Valor alto	Reducir	Configuración, documentación, restricciones, equipos endpoint	Aceptable	60%
…	…	…		…	…	…