UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE TELECOMUNICACIONES

INTEGRACIÓN DE SOLUCIONES DE CIBERSEGURIDAD EN SOFTWARE LIBRE PARA LA PROTECCIÓN DE LAS PYMES APLICADO PARA LA FUNDACIÓN DE ATENCIÓN AL DISCAPACITADO (F.A.D).

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Telecomunicaciones

AUTOR: JAIR ALEJANDRO MARÍN CASTILLO

TUTOR: JUAN CARLOS DOMÍNGUEZ AYALA

Quito – Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

YO, Jair Alejandro Marín Castillo, con documento de identificación N° 1724172448 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 15 de Julio de 2024.

Atentamente,

Jair Alejandro Marín Castillo
1724172448

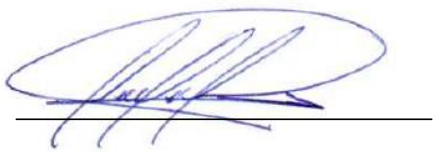
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA.

Yo Jair Alejandro Marín Castillo con documento de identificación No.1724172448, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Proyecto Técnico: " Integración de soluciones de ciberseguridad en software libre para la protección de las pymes aplicado para la Fundación de Atención al Discapacitado (F.A.D) ", el cual ha sido desarrollado para optar por el título de Ingeniero en Telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana

Quito, 15 de Julio del año 2024.

Atentamente,



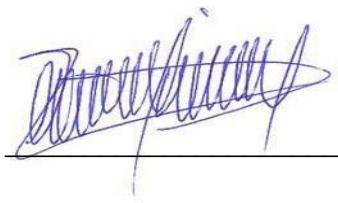
Jair Alejandro Marín Castillo
1724172448

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Juan Carlos Domínguez Ayala con documento de identificación N°1713195590, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: INTEGRACIÓN DE SOLUCIONES DE CIBERSEGURIDAD EN SOFTWARE LIBRE PARA LA PROTECCIÓN DE LAS PYMES APLICADO PARA LA FUNDACIÓN DE ATENCIÓN AL DISCAPACITADO (F.A.D). realizado por Jair Alejandro Marín Castillo, con documento de identificación N° 1724172448 obteniendo como resultado final el trabajo de titulación bajo la opción: Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 15 de Julio del año 2024.

Atentamente,



Ing. Juan Carlos Domínguez Ayala, Msc
1713195590

DEDICATORIA

Dedico esta Trabajo a mis padres, Agustín y Liliana, por su incondicional amor, sacrificio y constante apoyo me han guiado en cada paso de mi vida. Agradezco por siempre creer en mí, por brindarme la fortaleza necesaria para enfrentar cada desafío y por inspirarme a perseguir sueños con determinación. Su ejemplo de perseverancia y dedicación ha sido la base sobre la cual he construido todos mis logros.

A mi hermano, Lenin, por ser mi compañero de vida, mi apoyo y motivación para salir adelante cada día tu presencia me impulsa a ser un mejor ejemplo y esforzarme cada día más.

A mi tía Rosario por su cariño, sus palabras de aliento y sus consejos, Gracias por ser una constante fuente de apoyo y consuelo en mi vida, brindándome animo en todo momento, por no verme solamente como un sobrino más sino como a otro de tus hijos.

Sin ustedes este logro no habría sido posible.

Jair Alejandro Marín Castillo

AGRADECIMIENTO

Mi agradecimiento al Ing. Juan Carlos Domínguez Ayala, mi tutor de tesis por su guía, paciencia y dedicación a lo largo de este proyecto. Su conocimiento y experiencia han sido una fuente de aprendizaje y su compromiso con mi formación ha sido esencial para el desarrollo de esta tesis. Gracias por sus valiosos consejos, su disponibilidad constante y por creer en mi capacidad para llevar a cabo este trabajo. Su apoyo ha sido fundamental para superar cada reto que se presentó en el camino.

Jair Alejandro Marín Castillo

INDICE DE CONTENIDO

Resumen....12

Abstract....13

CAPÍTULO 1....14

1.1 PROBLEMA DE ESTUDIO....14

1.2 OBJETIVOS....15

1.2.1 OBJETIVOS GENERAL....15

1.2.2 OBJETIVOS ESPECÍFICOS....15

1.3 JUSTIFICACIÓN....15

1.4 METODOLOGIA....16

1.4.1 Paradigma de la investigación....16

1.4.2 Tipo de investigación....17

1.4.3 Alcance....17

1.4.4 Unidad de Análisis....17

1.5 Marco Teórico....17

1.5.1 CIBERSEGURIDAD....17

1.5.2 Amenazas Cibernéticas....19

1.5.3 Medidas de ciberseguridad....22

1.5.4 Herramientas de ciberseguridad 24

1.5.5 SOFTWARE LIBRE 26

1.5.6 Tipos de Software Libre 27

1.5.7 Principales licencias de software libre 28

1.5.8 Principales herramientas de ciberseguridad en software libre 29

1.5.9 PYMES 34

CAPÍTULO 2 38

2.1 Analizar la Situación Actual de la Seguridad Cibernética de la F.A.D. 38

2.1.1. Descripción de la infraestructura de red. 38

2.1.2. Áreas de Trabajo en F.A.D. 38

2.1.3. Especificaciones de dispositivos de FAD 40

2.1.4. Levantamiento de topologia de red 44

2.1.5. Descripción de la Topología de Red de F.A.D. 45

2.1.6. Estructura de la Red 45

2.1.7. Características de la topología de la Red de F.A.D. 46

2.1.8. Evaluación de Medidas de Seguridad Implementadas 46

2.1.9. Identificación de Fortalezas y Debilidades 47

2.2 Evaluar las Soluciones de Ciberseguridad Disponibles para Proteger la F.A.D que Utilizan Software Libre Contra las Amenazas y Riesgos Identificados. 48

2.2.1. Tipos de Amenazas 49

2.2.2. Evaluación de Riesgos 50

2.2.3. Métodos de Evaluación 50

2.2.4. Evaluación de Herramientas y Tecnologías Específicas 51

2.2.5. Proceso de Evaluación 51

2.3 Analizar los requisitos técnicos y operativos necesarios para la implementación efectiva de soluciones de ciberseguridad en software libre para proteger la F.A.D. 52

2.3.1. Requisitos de Operaciones (..... 53

2.3.2. Requisitos de Técnicos 53

2.4 Simulación del Diseño de la Solución Integrada de Ciberseguridad en Software Libre para la Protección de la F.A.D. 54

2.4.1. Componentes de solución. 55

2.4.2. Proceso de Implementación 64

CONCLUSIONES 66

RECOMENDACIONES 67

REFERENCIAS 68

ÍNDICE DE FIGURAS

Figura 1 representación gráfica de cómo funciona un firewall 30

Figura 2 Clasificación Nacional PYMES Cámara de Comercio de Quito 34

Figura 3 Proceso de instalacion - ClamAV 55

Figura 4 Conexion de ClamAV 55

Figura 5 Proceso de Scaneo - ClamAV 56

Figura 6 Interfaz de Usuario - VeraCrypt.....57

Figura 7 Inicio de Proceso creación de cifrado.....57

Figura 8 Almacenamiento del Volumen.....58

Figura 9 Algoritmos de cifrado.....58

Figura 10 – Asignación de espacio del Volumen 59

Figura 11 Seguridad del Volumen.....59

Figura 12 *Formato del Volumen*.....60

Figura 13 Volumen Creado.....60

Figura 14 Configuración para montar el volumen.....61

Figura 15 Volumen Montado.....61

Figura 16 *Interfaz Bitwarden*.....62

Figura 17 Gestionar contraseñas Guardadas.....63

ÍNDICE DE TABLAS

Tabla 1 *Detalles de Dispositivos de la FAD* 40

Tabla 2 *Especificación Equipos de Red* 44

Resumen

El presente informe aborda la implementación de una estrategia de ciberseguridad utilizando soluciones de software libre para la Fundación de Atención al Discapacitado (F.A.D.). La evaluación de la infraestructura actual de la F.A.D. reveló varios puntos críticos que necesitan mejoras significativas para proteger de manera efectiva sus activos de información.

Se identificó que la infraestructura de red centralizada en un módem principal facilita la gestión de la seguridad, aunque se han implementado medidas básicas como firewalls y antivirus en todos los dispositivos, estas no son suficientes para enfrentar amenazas avanzadas. Además, algunos dispositivos presentan limitaciones en hardware, específicamente en memoria RAM y procesadores, lo que afecta su rendimiento y capacidad para ejecutar software de seguridad avanzado.

La propuesta de solución incluye una serie de recomendaciones técnicas y operativas para mejorar la postura de seguridad de la F.A.D. Entre las recomendaciones, se destaca la necesidad de aumentar la memoria RAM y evaluar la actualización de procesadores en dispositivos críticos. Para fortalecer la seguridad, se sugiere la implementación de herramientas de software libre como ClamAV para escaneos antivirus, VeraCrypt para el cifrado de datos sensibles, y Bitwarden para la gestión segura de contraseñas.

Estas medidas están diseñadas para establecer una solución de ciberseguridad completa que resguarde los activos de información de la F.A.D., asegurando la confidencialidad, integridad y disponibilidad de los datos críticos de la organización.

Palabras claves:

Ciberseguridad, Software libre, Infraestructura, Herramientas, Protección.

Abstract

This report addresses the implementation of a cybersecurity strategy using free software solutions for the Disability Care Foundation (F.A.D.). The evaluation of the F.A.D. current infrastructure revealed several critical points that need significant improvements to effectively protect its information assets.

It was identified that the network infrastructure centralized in a main modem facilitates the management of security, although basic measures such as firewalls and antivirus have been implemented on all devices, these are not enough to face advanced threats. In addition, some devices have limitations on hardware, specifically on RAM and processors, which affects their performance and ability to run advanced security software. Disabling remote services also limits network management and monitoring.

The solution proposal includes a series of technical and operational recommendations to improve the security posture of the F.A.D. Among the recommendations, the need to increase RAM and evaluate the update of processors in critical devices is highlighted. To strengthen security, we suggest the implementation of free software tools such as ClamAV for antivirus scans, VeraCrypt for encryption of sensitive data, and Bitwarden for secure password management.

These measures are designed to create a comprehensive cybersecurity solution that protects the FDA's information assets, ensuring the confidentiality, integrity and availability of the organization's critical data.

Keywords:

Cybersecurity, Free Software, Infrastructure, Tools, Protection.

CAPÍTULO 1

1.1 PROBLEMA DE ESTUDIO

La ciberseguridad es un aspecto crítico para la integridad y continuidad de las operaciones de organizaciones en la actualidad. Este es un desafío aún mayor para las PYMES, que a menudo enfrentan limitaciones de los recursos y experiencia en la ejecución de medidas de ciberseguridad efectivas. (De Docusign, 2023) La Fundación de Atención al Discapacitado (F.A.D) es un ejemplo paradigmático de las vulnerabilidades que enfrentan las PYMES debido a la falta de infraestructura de red y un nivel insuficiente de seguridad informática.

Según la OEA, (2019) el aumento constante de los ciberataques, la sofisticación de las amenazas y la falta de conciencia y recursos en las organizaciones han llevado a un incremento en la vulnerabilidad de las PYMES convirtiéndolas en un blanco atractivo para los ciberdelincuentes, dada la percepción de medidas de seguridad más débiles en comparación con empresas de mayor envergadura. Las PYMES deben tomar medidas para protegerse activamente y mejorar su seguridad informática, como realizar copias de seguridad regulares, actualizar y parchear los sistemas, restringir el uso de privilegios de administrador, y educar a los empleados sobre las amenazas en línea.

Es crucial que la Fundación de Atención al Discapacitado (F.A.D), como entidad dedicada a brindar servicios a personas con discapacidad, proteja la privacidad y confidencialidad de los datos de sus beneficiarios. Como ya mencioné anteriormente, su actual nivel de seguridad cibernética es limitado y eso la deja expuesta a una variedad de amenazas en un entorno digital cada vez más hostil.

Esta tesis se enfoca en abordar este problema al proponer la "Integración de Soluciones de Ciberseguridad en Software Libre" como una estrategia viable y accesible para fortalecer la seguridad informática de la F.A.D. El uso de software libre no solo ofrece una alternativa económicamente viable para las PYMES, sino que también permite adaptar soluciones a las necesidades específicas de la organización, brindando una mayor flexibilidad en la implementación de medidas de ciberseguridad. (Economista, 2012)

1.2 OBJETIVOS

1.2.1 OBJETIVOS GENERAL

Integrar soluciones de ciberseguridad en software libre que sean adecuadas para las necesidades y recursos de la Fundación de Atención al Discapacitado.

1.2.2 OBJETIVOS ESPECÍFICOS

- Analizar el escenario actual de la seguridad cibernética de la F.A.D.
- Evaluar las soluciones de ciberseguridad disponibles para proteger la F.A.D que utilizan software libre contra las amenazas y riesgos identificados.
- Analizar los requisitos técnicos y operativos necesarios para la implementación efectiva de soluciones de ciberseguridad en software libre para proteger la F.A.D.
- Simular el diseño de la solución integrada de ciberseguridad en software libre para la protección de la F.A.D.

1.3 JUSTIFICACIÓN

La seguridad informática es un tema crítico para cualquier organización, en especial para las pymes que no cuentan con los recursos y conocimientos necesarios para implementar

soluciones de ciberseguridad adecuadas el aumento de los ataques cibernéticos y la complejidad que representan los mismos hacen que las PYMES sean más vulnerables (Unir, 2021)

La Fundación de Atención al Discapacitado (F.A.D) es un ejemplo de una organización que cuenta con una seguridad informática muy baja, lo que la hace vulnerable a cualquier tipo de ataque cibernético, sumado la falta de experiencia y de recursos para implementar una infraestructura de red eficaz la cual ayudaría a brindar soluciones de ciberseguridad adecuadas.

Ante esta situación, es necesario buscar alternativas accesibles para la PYMES que le permitan proteger sus sistemas y datos sin incurrir en costos elevados. Una opción puede ser la integración de soluciones de ciberseguridad en software libre, que puede ser una alternativa accesible para esta empresa.

Es crucial destacar que las herramientas seleccionadas estarán dirigidas específicamente hacia los endpoint, los cuales representan puntos vulnerables en la red de cualquier organización. Enfoques centrados en proteger estos puntos finales pueden fortalecer significativamente la postura de seguridad de una organización como la F.A.D frente a amenazas cibernéticas.

1.4 METODOLOGIA

1.4.1 Paradigma de la investigación

El paradigma de la investigación es positivista, ya que se centra en la búsqueda de explicaciones objetivas y verificables sobre la efectividad de las soluciones de ciberseguridad en software libre para la protección de FAD.

1.4.2 Tipo de investigación

El tipo de investigación que presenta el proyecto es experimental.

1.4.3 Alcance

El alcance que presenta el proyecto corresponde a una investigación de tipo descriptiva, dado que los resultados obtenidos se mostraran al encargado de la FAD, logrando mostrar que la nueva integración de soluciones en software libre presenta una mejoría en la seguridad.

1.4.4 Unidad de Análisis

La fundación de Atención al Discapacitado

1.5 Marco Teórico

1.5.1 CIBERSEGURIDAD

La ciberseguridad es el conjunto de prácticas, tecnologías y procesos destinados a la protección de los sistemas, redes y datos frente a posibles daños, ataques malintencionados o accesos no permitidos. Su principal objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información (Euncet, 2024).

La ciberseguridad abarca un amplio espectro de medidas diseñadas para proteger activos digitales contra amenazas en constante evolución. Esto incluye desde la implementación de sofisticadas tecnologías de defensa hasta la adopción de políticas y procedimientos que fortalezcan la resistencia de sistemas y redes ante ataques cibernéticos. Su importancia radica en garantizar la confidencialidad, asegurando que la información sensible esté protegida contra accesos no autorizados; la integridad, evitando modificaciones no autorizadas en los datos; y la disponibilidad, asegurando que los sistemas y datos estén disponibles cuando sean necesarios para usuarios legítimos.

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio. (Teldat, 2023)

La ciberseguridad es crucial para garantizar la seguridad, privacidad y accesibilidad de los datos y sistemas en un mundo cada vez más complejo y conectado. Las estrategias de ciberseguridad deben reinventarse constantemente debido a la creciente sofisticación de las amenazas emergentes. Por lo tanto, mitigar los riesgos y mantener seguros los activos digitales de una empresa será posible mediante la implementación de medidas proactivas, así como el conocimiento y la adherencia a las mejores prácticas de seguridad cibernética.

En la actualidad, la implementación de medidas de ciberseguridad se debe a que se encuentran más dispositivos conectados que personas, y los atacantes son cada vez más creativos. (ALAS, 2022)

La ciberseguridad ha crecido en el siglo XXI por diversas razones. El creciente número de dispositivos conectados a Internet es uno de ellos. El Internet de las cosas ha llevado a estimar que existen más dispositivos conectados que personas. Internet puede apuntar a diversos dispositivos interconectados, como teléfonos inteligentes, computadoras, electrodomésticos y equipos industriales, todos los cuales son susceptibles a ataques cibernéticos.

Además, los atacantes cibernéticos están constantemente evolucionando en sus métodos y técnicas. Son cada vez más sofisticados y creativos en la manera en que diseñan y ejecutan sus ataques. Utilizan herramientas automatizadas, técnicas de ingeniería social avanzadas y explotan vulnerabilidades en sistemas y software para comprometer la seguridad

de organizaciones y usuarios individuales.

Un reciente informe en el que intervinieron 1.100 responsables de protección de la información de todo el mundo reveló que el 91% de las entidades encuestadas experimentaron al menos un incidente de ciberseguridad en el 2023.

Según el mismo informe, el 86% de los ejecutivos afirmó que su enfoque de protección de datos tuvo una contribución significativa y positiva en los negocios. (Zendesk, 2024)

Con la alta prevalencia de este fenómeno, existe una constante y generalizada amenaza cibernética, esta amenaza representa la urgente necesidad de reforzar las medidas de seguridad en todas las industrias para protegerse de los ataques potencialmente devastadores. Como ya se mencionó, un 86% de entrevistados consideraron que su orientación a la protección de datos contribuye de manera reveladora y efectiva a sus negocios. Dado que inversiones en ciberseguridad son críticas no solo para prevenir incidentes, sino también para mejorar el rendimiento y la estabilidad de la organización, eso convierte la seguridad de la información en ventaja en el competitivo mercado. Por lo tanto, la protección de datos beneficia el negocio. En consecuencia, cada vez más, las empresas ven la ciberseguridad no solo como un costo necesario, sino como una inversión estratégica. Eso llevará a una mayor inversión en tecnologías de seguridad avanzadas y capacitación, mejorando, en última instancia, su capacidad de adaptación cibernética.

1.5.2 Amenazas Cibernéticas

Las ciber amenazas son intentos malintencionados de acceder a los datos sensibles de una empresa, como a la información de sus empleados, sus consumidores relacionada con el desarrollo de su actividad. (Cisco, 2024)

Además de acceder a información confidencial, las amenazas cibernéticas también

pueden apuntar a interrumpir las operaciones normales de una organización mediante ataques de denegación de servicio (DDoS), que sobrecargan los sistemas y los hacen inaccesibles para usuarios legítimos. Estos incidentes no solo tienen el potencial de causar pérdidas financieras significativas, sino también de dañar la reputación de la empresa y erosionar la confianza de los clientes y socios comerciales.

Los ataques cibernéticos pueden afectar a una amplia gama de entidades y personas en la sociedad actual. Aunque las grandes organizaciones suelen ser blanco frecuente, cualquier individuo o entidad que maneje información valiosa puede ser vulnerable. Los motivos detrás de estos ataques suelen incluir: (Kaira, 2023)

Algunos de las amenazas cibernéticas más comunes implican incidentes de seguridad cibernética, que incluyen la recopilación de datos sensibles de clientes y personal, la toma de control de información financiera, el acceso no autorizado a sistemas de TI para realizar transacciones financieras, la obtención de secretos comerciales y la manipulación de información personal y de sesiones. Además, se señala la realización de ataques dirigidos a entidades gubernamentales y la exigencia de rescates económicos a cambio de la restauración de datos secuestrados. Estas acciones ilustran diversas estrategias empleadas por actores malintencionados para obtener beneficios económicos o información estratégica, destacando la importancia de medidas de seguridad robustas para proteger contra tales amenazas.

1.1.1.1Ingeniería social:

Se trata de métodos empleados por delincuentes cibernéticos para influir psicológicamente en individuos con el fin de obtener datos personales sensibles o acceder ilegalmente a sistemas de información confidencial. (Docusign, 2023)

Los ciberdelincuentes utilizan la ingeniería social para manipular psicológicamente a las personas y acceder a los sistemas de información, obteniendo datos confidenciales o accediendo a sistemas de información

Phishing:

Se trata de ataques de phishing por correo electrónico que intentan obtener información confidencial, como datos personales, contraseñas y detalles de tarjetas de crédito, mediante el uso de comunicaciones engañosas que parecen legítimas. (Institute, 2021)

Los ataques de phishing efectuados por correo electrónico son algo común y suponen un peligro importante. Los correos electrónicos que parecen provenir de fuentes confiables, como bancos, muchas veces por empresas o servicios en línea populares, la mayoría de las veces son el blanco de ciberdelincuentes que intentan engañar a los usuarios para que revelen información confidencial o hagan clic en enlaces maliciosos. Revise los correos electrónicos y asegúrese de que sean auténticos antes de brindar información personal o confidencial del usuario.

1.1.1.2Malware:

Se refiere a programas maliciosos creados con el propósito de acceder sin autorización, deshabilitar sistemas informáticos y computadoras, que pueden incluir virus, gusanos informáticos y troyanos. (Teldat, 2023)

Los archivos se vuelven vulnerables a los virus, que luego se propagan durante la ejecución. Los gusanos utilizan recursos para replicarse automáticamente en las redes. Los troyanos no existen, simplemente hacen un montón de cosas, como robar datos u otorgar acceso remoto a los sistemas. Mantenerse seguro en línea implica utilizar software de seguridad moderno.

1.1.1.3Ransomware:

El ransomware es un tipo de software malicioso utilizado por delincuentes para extorsionar dinero. Estos ciberdelincuentes exigen un rescate a cambio de descifrar los datos que han cifrado o para desbloquear el dispositivo de la víctima. (Cisco, 2024)

Las amenazas cibernéticas más comunes incluyen métodos de ingeniería social para manipular psicológicamente a las personas y obtener datos sensibles o acceso a sistemas confidenciales. El phishing busca obtener información personal mediante correos electrónicos engañosos. El malware, como virus, gusanos y troyanos, está diseñado para acceder y deshabilitar sistemas informáticos. Por último, el ransomware se utiliza para extorsionar dinero mediante el cifrado de datos y la exigencia de un rescate para recuperar la información o desbloquear dispositivos.

1.5.3 Medidas de ciberseguridad

La ciberseguridad abarca una serie completa de medidas preventivas y reactivas adoptadas por las organizaciones para proteger sus activos digitales contra diversas amenazas cibernéticas cada vez más sofisticadas. Estas estrategias no solo buscan salvaguardar los sistemas informáticos y redes de una empresa, sino también asegurar la integridad de los datos sensibles y mantener la continuidad de las operaciones comerciales en un entorno digital interconectado y dinámico.

Estas son las principales medidas que las empresas deben adoptar en materia de ciberseguridad. (Ciberseg, 2019)

1. Actualización de dispositivos y equipos

2. Elaborar una política de ciberseguridad

3. Protegerse frente al malware

4. Realizar copias de seguridad

5. Establecer controles de acceso

6. Proteger la red corporativa

7. Proteger la red inalámbrica (WIFI)

8. Proteger los dispositivos móviles

9. Gestionar los soportes de almacenamiento

10. Registrar y analizar la actividad

Los recursos físicos y tecnológicos esenciales para asegurar que nuestros datos personales, en posesión de entidades obligadas, permanezcan íntegros, confidenciales y disponibles, con el objetivo de prevenir daños, modificaciones, pérdidas, destrucción, así como el uso o la transmisión no autorizados. (Imfoem, s.f.)

Básico:

Estas son las medidas de seguridad básicas que deben aplicarse de manera obligatoria en todos los sistemas y bases de datos personales.

Medio:

Se refiere a la implementación de medidas de seguridad necesarias para bases de datos o sistemas que contengan información sobre infracciones administrativas o penales, finanzas públicas, servicios financieros, datos patrimoniales, y también datos personales que permitan obtener una evaluación integral de la personalidad del individuo.

Alto:

Son las medidas de seguridad que se deben aplicar a bases de datos o sistemas que contengan información relacionada con la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, datos biométricos, genéticos o vida sexual. Además, estas medidas también son pertinentes para los datos recopilados con fines policiales, de seguridad pública, prevención, investigación y persecución de delitos. (Imfoem, s.f.)

1.5.4 Herramientas de ciberseguridad

Antivirus

El software antivirus es una herramienta diseñada para detectar, proteger y eliminar programas maliciosos. Aunque su nombre sugiere que se centra exclusivamente en virus, en realidad, ofrece protección contra una amplia gama de amenazas cibernéticas. (QuestionPro, 2023)

El software antivirus es un agente de protección crítico en la seguridad en la red, ya que asegura la protección frente a todas las posibles formas de peligros informáticos. Su habilidad para detectar, bloquear y eliminar los diferentes tipos de peligros que existen pasa tanto por los virus como por otros tipos de malware como el troyano, el ransomware, el spyware son una garantía de seguridad frente a nuestros archivos y sistemas. Si a esto se le añade el hecho que esta tecnología como técnica en seguridad trata de manera permanente análisis proactivos y las actualizaciones periódicas de las definiciones de peligros, por tanto, refuerza su defensa contra las nuevas formas de amenazas en la red en línea que cada día surgen. Por esta razón, el software antivirus es y será una herramienta básica tanto para un usuario doméstico como para una empresa que quiera mantener sus ordenadores protegidos frente a las amenazas que hoy representa el conjunto de las amenazas que existen en la red en línea.

Firewalls

son sistemas de seguridad diseñados para proteger redes informáticas al controlar y filtrar el tráfico de red según reglas predefinidas. Su función principal consiste en evitar accesos no autorizados a redes privadas y filtrar el tráfico en función de direcciones IP, protocolos y puertos. Pueden ser implementados tanto en forma de hardware como de software. (QuestionPro, 2023)

Además de los virus, el software antivirus es necesario para detectar, proteger y eliminar una variedad de amenazas en línea, cuya función principal es proteger sistemas de intrusiones maliciosas y ladrones de datos y es una defensa fundamental para sistemas de computadora.

Sistema de Detección y Prevención de Instrucciones (IDS/IPS)

El sistema de detección de intrusiones (IDS) es una tecnología de seguridad que monitorea la red o los sistemas informáticos en busca de actividades sospechosas o violaciones de políticas de seguridad. (QuestionPro, 2023)

Para un monitoreo y detección de actividades sospechosas en redes y sistemas, los sistemas de detección de intrusiones (IDS) son esenciales, mientras que, para un bloqueo activo de las intrusiones detectadas, los sistemas de prevención de intrusiones (IPS) son necesarios. Juntos, son fundamentales para la seguridad informática mediante la identificación y la respuesta a las amenazas en tiempo real.

Escaneo de vulnerabilidades

Estas herramientas analizan sistemas y redes en busca de posibles vulnerabilidades que podrían ser explotadas por atacantes. Identifican y evalúan las deficiencias del sistema, proponen recomendaciones para solucionar errores y clasifican las vulnerabilidades según su grado de riesgo. (QuestionPro, 2023)

Un escaneo de vulnerabilidad también tiene un papel fundamental, ya que ayuda a evaluar las deficiencias en sistemas y redes. De esta manera, se obtiene una visión clara de los riesgos potenciales que pueden ser explotados por los atacantes. Esto ayuda a los equipos de seguridad a tomar medidas preventivas y correctivas para mitigar esos riesgos y fortalecer la infraestructura de seguridad.

Redes Privadas Virtuales (VPN)

Su función principal es proteger la privacidad y la seguridad de la información transmitida, permitiendo a los usuarios navegar de manera más segura y acceder a recursos de red de forma remota. (QuestionPro, 2023)

Mediante el uso de protocolos de cifrado robustos, una VPN permite a los usuarios navegar por Internet de manera más segura y acceder de forma remota a recursos de red que de otra manera podrían estar restringidos geográficamente o protegidos por cortafuegos. Esto es posible al establecer un túnel virtual seguro que encripta todos los datos transmitidos bloqueando que ataques maliciosos accedan a la información privada.

Además de proporcionar un nivel adicional de seguridad, las VPN también ofrecen otros beneficios significativos. También son utilizadas por individuos preocupados por la privacidad en línea, ya que ocultan la dirección IP real del usuario y enmascaran su ubicación geográfica, ayudando así a preservar el anonimato mientras se navega por Internet.

1.5.5 SOFTWARE LIBRE

El software libre fomenta la transparencia, la cooperación y la comunidad de desarrollo, promoviendo valores de libertad y empoderamiento de los usuarios. Ejemplos populares de software libre incluyen el sistema operativo GNU/Linux, la suite ofimática LibreOffice y el navegador web Mozilla Firefox. Se caracteriza por ser colaborativo, accesible en términos de

costo, y proporciona a los usuarios la oportunidad de participar activamente en su desarrollo y mejora continua. (Libre., 2021)

El concepto de software libre se relaciona con una categoría de programas que enfatizan la libertad de los usuarios y la comunidad. Desarrollo de programas que permiten a los usuarios ejecutar, copiar, distribuir, estudiar, modificar y mejorar sin restricciones. Para garantizar estas libertades, se utilizan licencias específicas que abren el código fuente y permiten a los usuarios y desarrolladores adaptarlos de acuerdo con sus propias necesidades e intereses. Una de las características más importantes de los programas libres es fortalecer el trabajo en equipo. Al permitir la contribución activa de la comunidad individual y el desarrollo continuo del programa. Al hacerlo, no solo se promueve la innovación tecnológica, sino que también permite a los usuarios y desarrolladores enfrentar nuevos desafíos y demandas digitales.

Según la definición de software libre, se destacan cuatro libertades fundamentales para los usuarios:

- Independencia de utilizar el software para cualquier propósito.
- La independencia de evaluar y entender cómo funciona del sistema.
- La libertad de redistribuir copias del software para beneficiar a otros.

La libertad de modificar y mejorar el software, así como distribuir esas versiones mejoradas, enriqueciendo así a toda la comunidad con las mejoras realizadas por diferentes contribuidores. (GNU, s.f.)

1.5.6 Tipos de Software Libre

El software libre engloba una amplia variedad de programas que cubren diferentes

campos, que van desde sistemas operativos hasta herramientas de diseño y ciberseguridad. Estos programas ofrecen a los usuarios la libertad de utilizar, modificar y distribuir el software. A continuación, se describen algunos de los tipos principales de software libre:

Sistemas operativos GNU/Linux:

- Ubuntu
- Fedora
- Debian
- Kali Linux
- CentOS
- Linux Mint

Navegadores Web:

- Mozilla Firefox
- Brave
- Tor Browser
- Opera

Editores de Texto y Programación:

- GNU Emacs
- Vim
- Aton
- Visual Studio Code

1.5.7 Principales licencias de software libre

Las licencias de software libre son contratos legales que establecen las condiciones bajo

las cuales se puede utilizar, modificar y distribuir el software. A continuación, se enumeran las principales licencias de software libre, junto con una breve explicación: (Rodriguez, 2023)

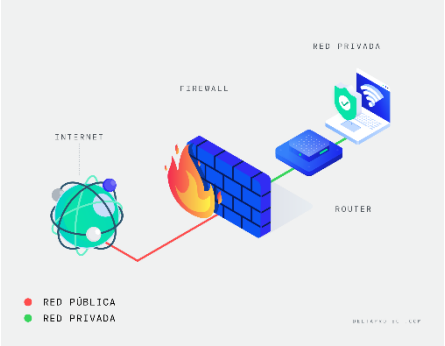
- **GPL (GNU General Public License)**: Esta licencia permite la modificación y redistribución del código fuente bajo los mismos términos de la licencia GPL.
- **LGPL (GNU Lesser General Public License)**: Permite el uso de bibliotecas de código en software no libre, con ciertas restricciones que son menos estrictas que las de la GPL.
- **BSD (Berkeley Software Distribution)**: Esta licencia permite el uso, modificación y redistribución del código fuente con muy pocas restricciones.
- **MIT**: Permite el uso, modificación y redistribución del código fuente con pocas restricciones, similares a las de la licencia BSD
- **Apache**: Esta licencia permite el uso, modificación y redistribución del código fuente, aunque impone algunas condiciones específicas que deben cumplirse.

1.5.8 Principales herramientas de ciberseguridad en software libre

Firewalls:

sistemas de seguridad protegen las redes informáticas al controlar el tráfico de datos entrante y saliente de acuerdo con normas de seguridad. Funcionan como un muro entre una red privada interna y redes externas, como Internet, filtrando y bloqueando potenciales amenazas y accesos no autorizados.

Figura 1 *representación gráfica de cómo funciona un*



NOTA: Adaptado de Cortafuegos [Imagen] por deltaprotect,2021 https://www.deltaprotect.com/blog/que-es-un-firewall

Entre las principales soluciones de firewall de software libre se encuentran:

- **pfSense:** Solución de firewall y router de código abierto que proporciona seguridad perimetral y control de tráfico de red.
- **IPFire:** Distribución de Linux que funciona como firewall, router y proxy, ofreciendo herramientas avanzadas de seguridad de red.
- **Untangle NG Firewall:** Solución de firewall y gateway de código abierto que incluye filtrado de contenido, VPN y antivirus.
- **Endian Firewall Community:** Distribución de firewall y router con herramientas de seguridad como VPN, filtrado de contenido y anti-malware.

Estas soluciones de firewall de software libre son fundamentales para proteger redes empresariales y domésticas, asegurando que el tráfico de red sea monitoreado y filtrado según las políticas de seguridad establecidas. Ofrecen funcionalidades avanzadas que ayudan a prevenir intrusiones y garantizan la seguridad de información transmitida a través de la red.

Antivirus y Antimalware

El software anti-malware son programas diseñados para proteger los dispositivos informáticos contra software malicioso, como virus, spyware, ransomware y otros tipos de amenazas. Los antivirus se centran en detectar y eliminar virus tradicionales que pueden infectar y dañar archivos o sistemas operativos. Dicho esto, el anti-malware puede evitar la aparición de una infección viral y eliminar los archivos infectados. (Malwarebytes, 2020)

El software antivirus se encarga de identificar y eliminar software malicioso, protegiendo los sistemas contra virus, gusanos, troyanos y otras formas de malware. Aquí se presentan algunas de las principales herramientas de antivirus de software libre:

- **ClamAV:** Es un programa antivirus de código abierto que detecta y elimina malware como virus, troyanos y gusanos.
- **Avira Free Antivirus:** Ofrece una solución gratuita que proporciona protección básica contra virus y malware.
- **Avast Free Antivirus:** Este antivirus gratuito protege contra una amplia variedad de amenazas cibernéticas.
- **Lynis:** Se trata de una herramienta de auditoría y escaneo de seguridad diseñada para sistemas Unix. Realiza pruebas de seguridad y detecta rootkits y malware.

Estas herramientas son esenciales para mantener la integridad y seguridad de los sistemas informáticos, especialmente en entornos donde la protección contra amenazas cibernéticas es crucial. Utilizan técnicas avanzadas para detectar y neutralizar cualquier intento de infiltración o daño causado por software malicioso.

Sistemas de Identificación y Prevención de Intrusos (IDS/IPS)

Los sistemas IDS/IPS supervisan el tráfico de red en búsqueda de actividades sospechosas y actúan para evitar intrusiones. Las principales herramientas IDS/IPS de código abierto son:

- **Snort:** Sistema de prevención y detección de intrusiones de código abierto que supervisa el tráfico de red en busca de actividades sospechosas.
- **Suricata:** Suricata inspecciona el tráfico de red utilizando diversos métodos, incluyendo detección basada en firmas, detección de anomalías y análisis de protocolos.
- **Bro (Zeek):** Funciona como un motor de análisis pasivo que captura y analiza el tráfico de red, proporcionando un conjunto detallado de logs y datos que permiten a los administradores de seguridad investigar y responder a los eventos de seguridad.
- **OSSEC:** Sistema de detección de intrusos basado en host (HIDS) que monitorea y analiza los logs del sistema en busca de actividad sospechosa.

Herramientas de Cifrado

El cifrado de datos es un proceso esencial que garantiza la seguridad y la privacidad al codificar información de manera que solo pueda ser interpretada por individuos autorizados, protegiendo así la confidencialidad y la integridad de los datos. Este método se aplica mediante diversas herramientas de software libre, cada una diseñada para cubrir diferentes necesidades y contextos: (Kapersky, 2024)

El cifrado de datos es una práctica esencial en la seguridad informática, el cual ayuda a proteger la confidencialidad e integridad de la información, esto se logra al codificar los datos de manera que solo pueda ser entendida por personas autorizadas. En resumen, el proceso consiste en transformar los datos originales en una forma ilegible mediante el uso de algoritmos matemáticos y claves de cifrado. Dichas herramientas de software libre no solo ofrecen métodos robustos para proteger datos sensibles, sino que también en la medida que permiten a

los usuarios y desarrolladores tener control sobre cómo implementan y mantienen la seguridad de la información en sus sistemas y aplicaciones.

- **GnuPG:** Conocido por su capacidad para cifrar y firmar datos, GnuPG asegura la confidencialidad y la integridad de la información a través de técnicas de cifrado de extremo a extremo.
- **VeraCrypt:** Esta herramienta se especializa en el cifrado de discos y particiones, proporcionando una capa adicional de seguridad mediante el cifrado en tiempo real para discos completos o volúmenes específicos.
- **OpenSSL:** Ampliamente reconocida por su robusta biblioteca de herramientas de criptografía, OpenSSL ofrece funcionalidades avanzadas como cifrado, firma digital y gestión de certificados, fundamentales para asegurar la comunicación y los datos sensibles.
- **Cryptsetup/LUKS:** Estas herramientas son indispensables en entornos Linux para configurar el cifrado de discos completos utilizando LUKS (Linux Unified Key Setup), garantizando una protección integral de los datos almacenados.
- **Keybase:** Esta plataforma facilita el cifrado de extremo a extremo para la mensajería segura y el almacenamiento de archivos, permitiendo a los usuarios comunicarse de manera protegida y compartir archivos cifrados de forma segura.

Proxys:

Los proxys actúan como intermediarios entre los usuarios y los recursos de Internet, proporcionando anonimato, filtrado de contenido y seguridad adicional. Las principales herramientas de proxy de software libre incluyen: (Barbosa, 2020)

- **Squid:** Proxy caché de alto rendimiento para páginas web, que también ofrece control

de acceso y aceleración de caché.

- **Privoxy:** Proxy web sin caché con avanzadas capacidades de filtrado de contenido y mejora de privacidad.
- **Varnish Cache:** Acelerador de aplicaciones web, también utilizado como proxy inverso para mejorar la velocidad y eficiencia de los sitios web.
- **HAProxy:** Solución de proxy y balanceador de carga de alto rendimiento, utilizado para distribuir el tráfico entre múltiples servidores.
- **Tinyproxy:** Proxy HTTP ligero y rápido, ideal para entornos con recursos limitados.

1.5.9 PYMES

PYMES en Ecuador se refiere a un conjunto de pequeñas y medianas empresas que comparten características similares en sus procesos de crecimientos: Estas características incluyen la cantidad de empleados, el número de ventas, la experiencia en el ámbito laboral.

Según el boletín de la cámara de comercio de Quito clasifica como pymes según el siguiente gráfico.

Figura 2 *Clasificación Nacional PYMES Cámara de Comercio de Quito*

Variables	Micro Empresa	Pequeña Empresa	Mediana Empresa	Grandes Empresas
Personal ocupado	De 1 - 9	De 10 - 49	De 50 - 199	≥ 200
Valor bruto de ventas anuales	≤ 100.000	100.001 - 1.000.000	1.000.001 - 5.000.000	> 5.000.000
Monto de activos	Hasta US$ 100.000	De US$ 100.001 hasta US$ 750.000	De US$ 750.001 hasta US$ 3.999.999	≥ 4.000.000

A partir de la Figura 2 que clasifica las empresas en Microempresa, Pequeña Empresa, Mediana Empresa y Grandes Empresas, podemos sacar las siguientes conclusiones:

Diversificación de Empresas por Tamaño:

- Las empresas se pueden clasificar en cuatro categorías principales basadas en su personal ocupado, el valor bruto de sus ventas anuales y el monto de sus activos.
- Esto permite una mejor organización y entendimiento de las distintas escalas de negocios y sus características económicas.

Importancia del Tamaño en la Economía:

- Las micro y pequeñas empresas, a pesar de tener menor cantidad de empleados y recursos, son esenciales para la economía, especialmente en términos de empleo y desarrollo local.
- Las medianas y grandes empresas, por su parte, tienden a tener un mayor impacto económico debido a sus mayores ingresos y activos, y suelen ser más influyentes en el mercado global.

Diferencias en Recursos y Capacidad Operativa:

- Microempresas: Generalmente tienen recursos limitados y operan a una escala muy local. Su capacidad de crecimiento está vinculada a obtener apoyo financiero y aumentar su cuota de mercado.
- Pequeñas Empresas: Tienen una mayor capacidad operativa que las microempresas y pueden expandirse más allá del mercado local. Pueden acceder a ciertos créditos y programas de apoyo que no están disponibles para las microempresas.
- Medianas Empresas: Su capacidad de inversión y operativa es significativamente mayor. Pueden competir a nivel regional y, en algunos casos, internacional.

- Grandes Empresas: Tienen una estructura compleja y una amplia capacidad de recursos. Pueden influir en mercados internacionales y tienen acceso a una variedad de recursos financieros y tecnológicos.

Necesidad de Políticas Específicas:

- Cada categoría de empresa tiene necesidades diferentes en términos de financiamiento, regulación, capacitación y desarrollo de infraestructura.
- Las políticas públicas y programas de apoyo deben ser diseñados específicamente para cada grupo para maximizar su efectividad y fomentar el crecimiento sostenible.

Impacto en el Empleo:

- Las micro y pequeñas empresas son cruciales para la creación de empleo, especialmente en economías emergentes donde pueden absorber una gran parte de la fuerza laboral.
- Las medianas y grandes empresas también juegan un papel importante, no solo en la creación de empleo, sino también en ofrecer trabajos más estables y, a menudo, mejor remunerados.

Escalabilidad y Crecimiento:

La transición de una empresa de una categoría a otra implica un cambio significativo en su estructura operativa y en la gestión de sus recursos.

Las empresas que logran escalar la situación inicial de su empresa a niveles más altos frecuentemente suelen necesitar apoyo en términos de financiamiento, asesoramiento empresarial y acceso a nuevos mercados.

En resumen, la clasificación de las empresas según su tamaño y recursos permite entender mejor sus características y necesidades específicas. Esto es fundamental para el

desarrollo de políticas efectivas que apoyen su crecimiento y contribuyan al desarrollo económico general.

Las PYMES son fundamentales para la economía de Ecuador, ya que generan una gran cantidad de empleo y son esenciales para reducir el desempleo y el subempleo, estas contribuyen al desarrollo económico de diversas regiones, incluidas las áreas rurales y menos desarrolladas, fomentando así la descentralización económica. Además, son una fuente de innovación y competitividad, adaptándose rápidamente a las condiciones cambiantes del mercado y desarrollando nuevos productos y servicios. Estas empresas aportan significativamente al Producto Interno Bruto (PIB) del país, fortaleciendo la economía nacional y promoviendo la diversificación económica, lo que disminuye la dependencia de sectores específicos y grandes corporaciones.

Un 44% de las pequeñas y medianas empresas sufrieron al menos 1 ataque cibernético en 2021, según un estudio de Hiscox efectuado en diversos territorios, y para 2022 se prevé que hayan incrementado. Los ciber atacantes han puesto el foco en las empresas pequeñas y medianas, ya que usualmente las medidas de seguridad suelen ser más débiles o incluso inexistentes. (Teldat, 2023)

CAPÍTULO 2

2.1 Analizar la Situación Actual de la Seguridad Cibernética de la F.A.D.

En el segundo capítulo se enfocará en la creación de una línea base de ciberseguridad para la fundación de atención al discapacitado (F.A.D.). Esta línea base servirá como punto de referencia esencial para evaluar la postura de ciberseguridad actual de la organización estableciendo mejoras continuas en la protección de sus activos de información. Se realizará una evaluación detallada de la infraestructura tecnológica de F.A.D., incluyendo la identificación de activos críticos, la topología de red y las medidas de seguridad implementadas actual mente.

2.1.1. Descripción de la infraestructura de red.

La infraestructura de red de la Fundación de Atención al Discapacitado (F.A.D.) está compuesta por una amplia gama de componentes físicos y lógicos que soportan las operaciones diarias de la organización. Este análisis detallado incluirá una revisión de los dispositivos de red, estaciones de trabajo, sistemas de almacenamiento y otros elementos cruciales para el funcionamiento de la red y los sistemas de información de la F.A.D. El objetivo es identificar las fortalezas y debilidades de la estructura tecnológica, proporcionando una base sólida para implementar mejoras en la seguridad cibernética. A continuación, se describen los principales elementos de la infraestructura tecnológica de F.A.D.

2.1.2. Áreas de Trabajo en F.A.D.

La fundación de Atención al Discapacitado está organizada en varias áreas de trabajo, cada una con funciones específicas que contribuyen al cumplimiento de su misión. Las principales áreas analizadas en este estudio son:

- Área de Oficina
- Área de Recepción
- Área de Formación y Capacitación
- Área de Costura

2.1.3. Especificaciones de dispositivos de FAD

Tabla 1 *Detalles de Dispositivos de la FAD*

Oficina						
Nombre de equipo	**Modelo**	**Procesador**	**Sistema operativo**	**Antivirus**	**Servicios de seguridad**	**RAM**
PC Administrador	BIOSTAR Group H110MC	Intel Core I7	Microsoft Windows 10 Enterprise LTSC	Kaspersky	• Firewall Windows defender • Registro remoto (desactivado) • Enrutamiento y acceso remoto (desactivado)	4 GB

					• Escritorio remoto (desactivado)	
Impresora	Epson – L395					
Recepción						
Pc secretaria			Microsoft Windows 10 Pro		• Firewall Windows defender • Registro remoto (desactivado) • Enrutamiento y acceso remoto (desactivado) • Escritorio remoto (desactivado)	2 GB

Formación y capacitación						
Portátil 1	Toshiba - Satellite L855	Intel Core I7	Microsoft Windows 10 enterprise ltsc	Avast free	• Firewall Windows defender • Registro remoto (desactivado) • Enrutamiento y acceso remoto (desactivado) Escritorio remoto (desactivado)	6 GB

Portátil 2	Lenovo – 81st	AMD – A6	Microsoft Windows 10 Pro	Avast free	• Firewall Windows defender • Registro remoto (desactivado) • Enrutamiento y acceso remoto (desactivado) • Escritorio remoto (desactivado)	4 GB

La arquitectura de la red de F.A.D. está diseñada para realizar una distribución eficiente de los dispositivos en dos módems, de forma que optimiza el uso de la red y trata de garantizar que cada área tenga la conexión más accesible. El módem CNT supone 3 dispositivos, como la

impresora, el ordenador de la oficina y el de la recepción, por lo que propone una centralización en las operaciones de tipo administrativo o de atención al público. Por otro lado, tenemos el módem Costura está destinado al ámbito formativo, e interconecta dos portátiles, lo cual crea un modelo más flexible y móvil en las actividades educativas.

Los equipos de red son fundamentales para la conectividad y la comunicación entre los dispositivos en la infraestructura de F.A.D. La siguiente tabla proporciona los equipos de red utilizados en diferentes áreas de la fundación:

Tabla 2 *Especificación Equipos de Red*

Área	Equipo	Modelo	Cantidad
Oficina	Modem CNT (ISP)		1
Costura	Router TP-link	TL-WR840N	1

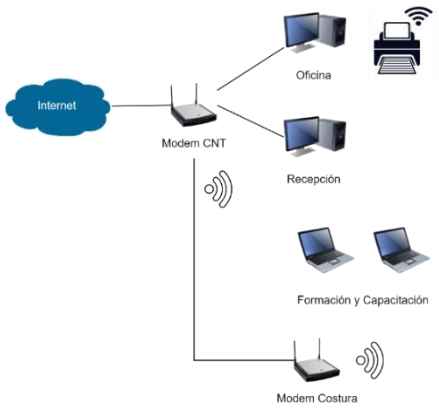
2.1.4. Levantamiento de topologia de red

Para comprender la estructura de la infraestructura tecnológica de la Fundación de Atención al Discapacitado (F.A.D.), es fundamental analizar su topología de red. Este análisis revela cómo los diversos dispositivos están interconectados y cómo fluye la información dentro de la organización. La topología de red ofrece una visión clara de las conexiones entre los dispositivos, permitiendo identificar puntos ulnerables y planificar mejoras en la seguridad y eficiencia de la red.

2.1.5. Descripción de la Topología de Red de F.A.D.

La topología de red de la F.A.D. sigue un modelo de conexión simple, adecuada para sus necesidades operativas. La red está estructurada alrededor de un módem principal proporcionado por CNT (Corporación Nacional de Telecomunicaciones), que actúa como el punto central de conexión para todos los dispositivos de la fundación. A continuación, se describe la conexión y disposición de los dispositivos en cada área de trabajo, basada en el diagrama de topología de red proporcionado.

Figura 1 *Topología de red de la Fundación de Atención al Discapacitado (F.A.D.).*



Nota La topología muestra una configuración en estrella donde los dispositivos se conectan a través de los switches y están centralizados por el router principal que gestiona el acceso a Internet. Creada por el autor.

2.1.6. Estructura de la Red

La topología de la red de F.A.D. es principalmente en estrella extendida (extended star), donde los switches actúan como nodos centrales y los dispositivos finales se conectan a estos switches. Los routers gestionan las conexiones a Internet y segmentan la red en VLANs para optimar la integridad y la eficiencia.

2.1.7. Características de la topología de la Red de F.A.D.

2.1.7.1.*Centralización en el Módem Principal:*

Todos los dispositivos de la fundación están conectados al módem principal proporcionado por CNT, actuando como el punto central de acceso a Internet y de interconexión interna.

2.1.7.2.Seguridad y Eficiencia:

Esta topología permite una gestión centralizada de las redes, lo que facilita la aplicación de una serie de medidas de protección, como cortafuegos y políticas de acceso, cruciales para proteger los activos de información de la organización.

2.1.7.3.Identificación de Puntos Vulnerables:

Al entender cómo están dispuestos los dispositivos y cómo se conectan, es posible identificar posibles puntos vulnerables en la red, tales como conexiones no seguras o configuraciones inadecuadas.

2.1.7.4.Planificación de Mejoras:

Con esta información detallada sobre la topología de red, F.A.D. puede planificar mejoras dirigidas a fortalecer la seguridad y eficiencia de la red, asegurando así un entorno tecnológico más robusto y confiable para apoyar sus operaciones.

2.1.8. Evaluación de Medidas de Seguridad Implementadas

2.1.8.1.Antivirus y Software de Seguridad

- Kaspersky: Utilizado en el PC del administrador en el área de oficina.
- Avast Free: Utilizado en los portátiles del área de formación y capacitación.

2.1.8.2.Servicios de Seguridad

- Firewall Windows Defender: Activo en todos los dispositivos.
- Registro Remoto: Desactivado en todos los dispositivos.
- Enrutamiento y Acceso Remoto: Desactivado en todos los dispositivos.
- Escritorio Remoto: Desactivado en todos los dispositivos.

2.1.9. Identificación de Fortalezas y Debilidades

2.1.9.1.Fortalezas

- Centralización de la Red: Simplifica la gestión y aumenta la seguridad.
- Medidas de Seguridad Básicas Implementadas: Todos los dispositivos cuentan con firewall y antivirus activos.

2.1.9.2. Debilidades

- Limitaciones en el Hardware: Algunos dispositivos tienen poca memoria RAM, lo que puede afectar su rendimiento y la capacidad para ejecutar software de seguridad avanzado.
- Desactivación de Servicios Remotos: Aunque mejora la seguridad, puede reducir la flexibilidad y la capacidad de respuesta ante incidentes.
- Dependencia de Software Antivirus Gratuito: El uso de antivirus gratuitos puede proporcionar una protección limitada en comparación con las versiones de pago.

A fin de evaluar la situación actual de la Fundación de Atención al Discapacitado y mejorar su infraestructura, se ha recopilado una línea base. La línea base es una compilación y resumen de factores claves, estructuras y sistemas en la organización. Tal línea le permitirá identificar ignorar de la organización y adelantarse y resolver problemas en ella. La línea base se desglosa en varios componentes principales. Uno de tales componentes es el análisis de la topología. Se define como una estructura que los dispositivos están interconectados y cómo fluye la información. De ello, uno puede definir áreas débiles en la red que luego se resuelven mediante mejoras.

2.2 Evaluar las Soluciones de Ciberseguridad Disponibles para Proteger la F.A.D que Utilizan Software Libre Contra las Amenazas y Riesgos Identificados.

La mayoría de las empresas comprenden que hay diversas ciber amenazas que pueden poner en riesgo sus operaciones. (Group, 2022)

Asegurar la ciberseguridad de una organización implica coordinar y preparar esfuerzos en múltiples niveles para proporcionar una protección integral a todo el sistema de información. Estos niveles incluyen: (Compusoluciones, 2024)

- Protección de aplicaciones
- Protección de datos
- Seguridad de redes
- Resiliencia ante desastres
- Seguridad en operaciones
- Formación de los consumidores

Se deben considerar las siguientes áreas clave: antivirus, firewalls, sistemas de

detección y prevención de intrusiones, cifrado de datos, y gestión de contraseñas. A continuación, se describen algunas de las soluciones más destacadas en cada área:

Existen varias razones por las cuales una organización puede ser vulnerable a un ataque:

1. Configuraciones incorrectas que pueden comprometer la seguridad.
2. Uso de software no actualizado o en fase de prueba.
3. Falta de aplicación de parches en el software y firmware.
4. Errores en el uso de software o protocolos de comunicación.
5. Diseño deficiente en la arquitectura de sistemas.
6. Implementación de contraseñas débiles o inseguras. (Compusoluciones, 2024)

2.2.1. Tipos de Amenazas

- Ataques Cibernéticos: Incluyen intentos de acceso no autorizado a sistemas críticos, explotación de vulnerabilidades de software, ataques de denegación de servicio (DoS), entre otros.
- Malware Específico para Sistemas Militares: Software malicioso diseñado para infiltrarse, dañar o comprometer sistemas de defensa militar.
- Ingeniería Social: Utilización de técnicas para engañar a usuarios y obtener acceso no autorizado o información confidencial.
- Filtraciones de Datos: Accesos no autorizados que resultan en la exposición de información clasificada o sensible.
- Fugas de Información: Acciones involuntarias o malintencionadas que resultan en la *divulgación de información crítica.*

2.2.2. Evaluación de Riesgos

- Impacto Potencial: Evaluar cómo cada tipo de amenaza podría afectar las operaciones y la seguridad de la F.A.D, incluyendo la interrupción de servicios, pérdida de datos sensibles o compromiso de la misión.
- Probabilidad de Ocurrencia: Determinar la probabilidad de que cada amenaza específica se materialice, considerando factores como la sofisticación de los adversarios, la visibilidad de los sistemas y las medidas de seguridad existentes.

2.2.3. Métodos de Evaluación

La revisión de infraestructura consiste en evaluar la seguridad de la red, sistemas informáticos y comunicaciones de una organización para identificar vulnerabilidades y puntos débiles potenciales. (Admin, 2021) Este proceso exhaustivo busca asegurar que las configuraciones sean adecuadas y que no existan fallos en el diseño de arquitecturas que puedan ser explotados por atacantes.

El análisis de vulnerabilidades implica el uso de herramientas automatizadas y técnicas manuales para detectar posibles brechas de seguridad en sistemas y aplicaciones. Es una medida proactiva para identificar y corregir vulnerabilidades antes de que sean aprovechadas por amenazas externas o internas.

Los ejercicios de Red Team son simulaciones de ataques llevadas a cabo por equipos internos o externos que actúan como adversarios reales. Estas prácticas evalúan la efectividad de las defensas de seguridad y la capacidad de respuesta ante incidentes, proporcionando una visión realista de la preparación de la organización frente a amenazas cibernéticas. (Díaz, 2024)

Las pruebas de penetración, por otro lado, son pruebas controladas diseñadas para explorar la seguridad de los sistemas mediante intentos controlados de explotación de

vulnerabilidades. (IBM, IBM, s.f.) Estas pruebas simulan un ataque real para identificar debilidades y proporcionar recomendaciones específicas para fortalecer la seguridad de la organización.

2.2.4. Evaluación de Herramientas y Tecnologías Específicas

2.2.4.1.Antivirus:

Evaluar soluciones de antivirus de código abierto que sean efectivas y actualizadas para proteger contra malware específico para sistemas militares.

2.2.4.2.Cifrado y Gestión de Contraseñas:

Implementar soluciones de cifrado y gestión de contraseñas que sean compatibles con los estándares de seguridad exigidos.

2.2.5. Proceso de Evaluación

Durante la revisión de infraestructura, se emplean diferentes técnicas y herramientas para llevar a cabo una evaluación exhaustiva:

2.2.5.1.Auditorías de Configuración:

Se revisan las configuraciones de todos los dispositivos de red y sistemas informáticos para asegurar que estén alineadas con las mejores prácticas de seguridad y que no haya configuraciones por defecto o débiles que puedan ser explotadas.

2.2.5.2.Análisis de Logs y Monitoreo:

Se analizan registros de eventos (logs) de sistemas y dispositivos de red para detectar patrones de tráfico sospechoso, intentos de acceso no autorizado, o actividades anómalas que puedan indicar una intrusión.

2.2.5.3.Escaneos de Vulnerabilidades:

Utilización de herramientas automatizadas para realizar escaneos de vulnerabilidades en la red y sistemas informáticos. Esto ayuda a identificar posibles puntos de entrada para ataques externos e internos y facilita la priorización de las correcciones necesarias.

Los ejercicios de Red Team son cruciales porque proporcionan una evaluación realista y práctica de la preparación de la organización frente a amenazas cibernéticas. Al simular escenarios de ataque, la F.A.D puede detectar y corregir vulnerabilidades antes de que sean explotadas por adversarios reales. Esto fortalece la capacidad de adaptarse cibernéticamente, mejora la respuesta a incidentes y asegura que los recursos críticos estén protegidos de manera efectiva.

2.3 Analizar los requisitos técnicos y operativos necesarios para la implementación efectiva de soluciones de ciberseguridad en software libre para proteger la F.A.D.

La protección de los activos de información de la Fundación de Atención al Discapacitado requiere una mejora y actualización robusta y eficiente de las soluciones de ciberseguridad para garantizar la protección de los activos de información de la fundación de atención al discapacitado.

A continuación, las matrices de tareas los requisitos técnicos y operativos necesarios para el despliegue de las soluciones de ciberseguridad que funcionen con software de código abierto. Se espera que estas soluciones mejoren significativamente la postura de seguridad de la empresa asegurando la privacidad, integridad y disponibilidad de la información. garantizando la privacidad, integridad y accesibilidad de los datos críticos.

2.3.1. Requisitos de Operaciones (

- Políticas granulares para el software general, el manejo de contraseñas y el software remoto y entrenamiento de incidentes y recuperación.

- Realizar Capacitación recurrente de ciberseguridad de la organización para el uso de software, fomentando el uso de nuevas herramientas y la preparación para desastres.

- Sistema de monitoreo de red continuo durante las 24 horas del día para detectar actividades inusuales.

Selección de herramientas de software libre:

- Antivirus: *ClamAV*. Solución antivirus de código abierto compatible con Windows.
- Cifrado de datos: *VeraCrypt*. Software de cifrado de disco de código abierto para proteger datos sensibles.
- Gestión de contraseñas: Bitwarden. Gestor de contraseñas de código abierto para asegurar credenciales de acceso.

2.3.2. Requisitos de Técnicos

Capacidad de hardware:

Memoria RAM:

- Administrador de PC: 4 GB (considerar aumento a 8 GB).
- PC de la secretaria: 2 GB (considerar aumento a 4 GB).
- Laptops: 6 GB para Toshiba Satellite L855 y 4 GB para Lenovo 81st.

Procesadores:

- Intel Core i7 para PC Admin y satélite L855.
- AMD A6 para la computadora portátil LONEVO 81st, capaces de contener las aplicaciones requeridas.

Conectividad de red:

- Asegurarse de que todos los dispositivos estén conectados correctamente al módem principal y al enrutador para que el manejo sea centralizado.
- Configurar VLAN separadas para un mejor segmento de la red, reduciendo los riesgos.

Compatibilidad de software:

- El sistema operativo Windows 10 Enterprise LTSC y Windows 10 Pro deben ser compatibles con las herramientas de software libre seleccionadas.

2.4 Simulación del Diseño de la Solución Integrada de Ciberseguridad en Software Libre para la Protección de la F.A.D.

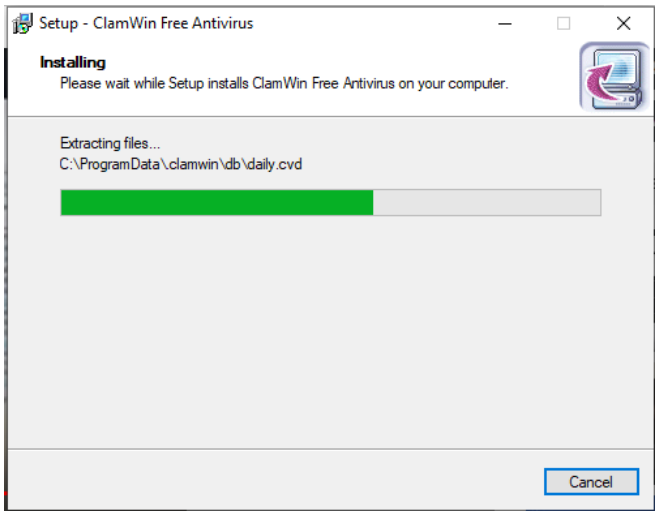
Una solución de ciberseguridad para la Fundación de Atención al Discapacitado implementada con software libre abordaría todos los aspectos importantes de seguridad. Abarcaría la protección de los endpoints, la red y los datos, así como también la gestión de accesos. A continuación, un diseño del simulado cubre una solución integrada para estos aspectos, utilizando software y herramientas de software libre.

2.4.1. Componentes de solución.

ClamAV es una solución antivirus y anti-malware open source que protege contra una amplia variedad de problemas. Se instalará en todos los puntos finales de F.A.D. para proteger sus archivos y sus correos electrónicos.

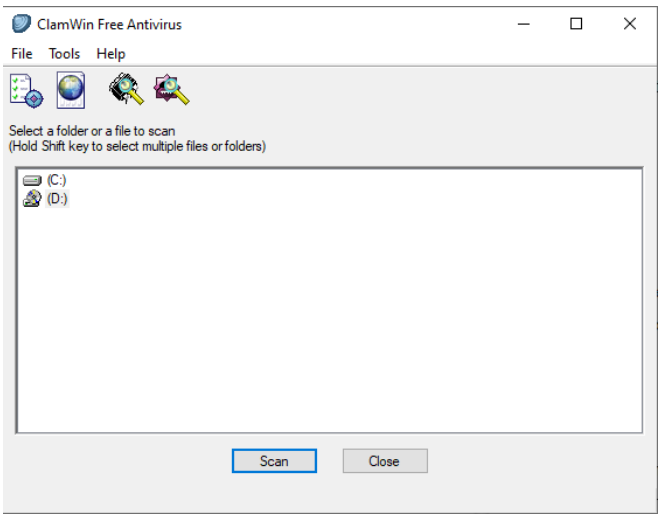
Instalación

Figura 3 *Proceso de instalación - ClamAV*



Ejecución

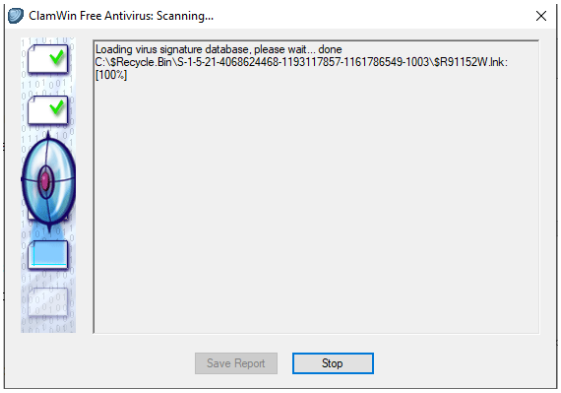
Figura 4 *Conexión de ClamAV*



En la ejecución del antivirus, Se conto con una interfaz sencilla, en la que se seleccionó carpetas

o unidades específicas para realizar el escaneo buscando posibles amenazas.

Figura 5 *Proceso de Escaneo - ClamAV*



Una vez seleccionada la carpeta que se requiere evaluar, ClamWin se ejecutó automáticamente procediendo a escanear los archivos seleccionados, analizando cada uno de los ellos buscando patrones y firmas de virus conocidos en su base de datos.

Ya finalizado el escaneo ClamWin creo un informe detallado que incluye cuantos archivos fueron escaneados, las amenazas que fueron identificadas y las acciones realizadas (Cuarentena, eliminación, entre otras)

En el caso de que ClamWin encuentre un archivo sospechoso, procede a registrarlo en el informe dependiendo de la configuración implementada puede poner los archivos identificados como infectados en cuarentena, eliminarlos automáticamente o solicitar que se decida qué hacer.

VeraCrypt es un software open source de protección de disco y de archivo que se montará en todos los desktops y servidores de F.A.D. para proteger la información crítica incluso si el dispositivo comprometido.

Figura 6 *Interfaz de Usuario - VeraCrypt*

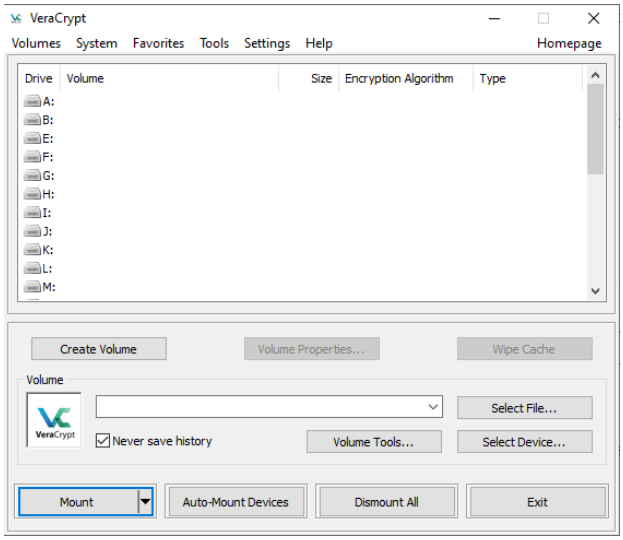
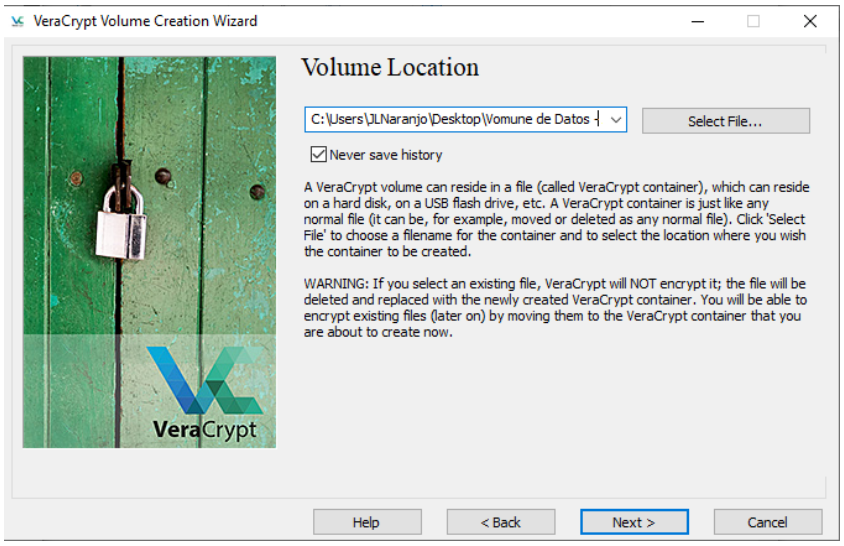


Figura 7 *Inicio de Proceso creación de cifrado*

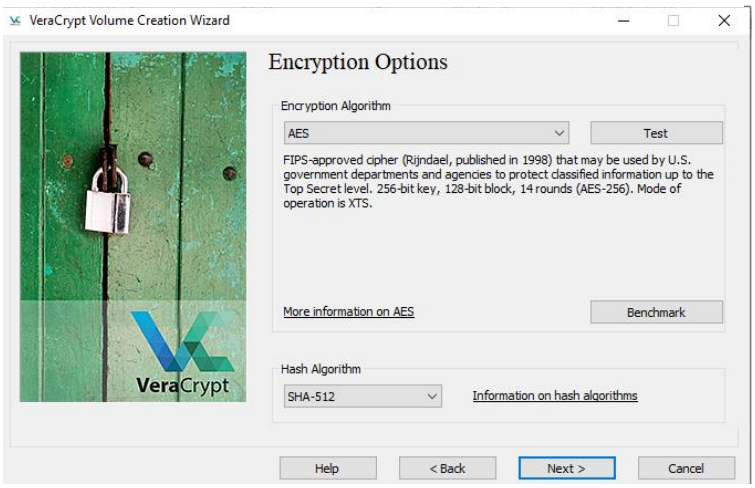
La finalidad de la creación del volumen es para generar una partición que actuó como un contenedor seguro donde los datos se almacenaran de forma cifrada.

Figura 8 *Almacenamiento del Volumen*



Se estableció la ubicación donde sugerimos almacenar la información que contendrá el volumen cifrado.

Figura 9 *Algoritmos de cifrado.*



Posterior a establecer la ubicación en la que se almacenará nuestro volumen, debemos elegir el algoritmo de cifrado, mismos que nos garantizaran la seguridad de los datos. La elección de AES para el cifrado **y** SHA-512 se basa en su ya probada seguridad, rendimiento y adopción de estándares de la industria. Esta mezcla asegura que los datos estén protegidos contra una amplia gama de amenazas y ataques criptográficos.

Figura 10 – Asignación de espacio del Volumen

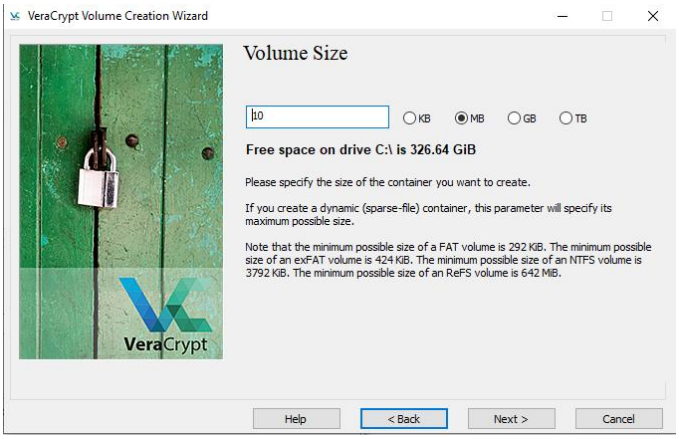


Figura 11 *Seguridad del Volumen*

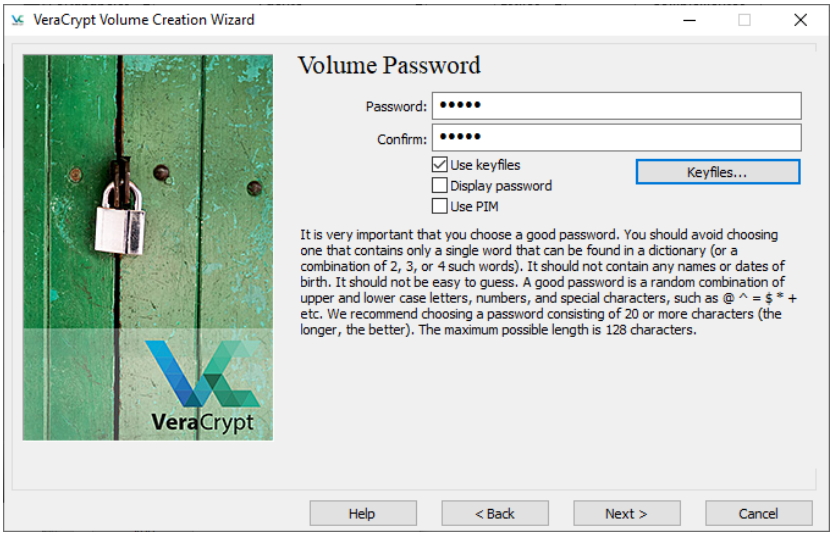
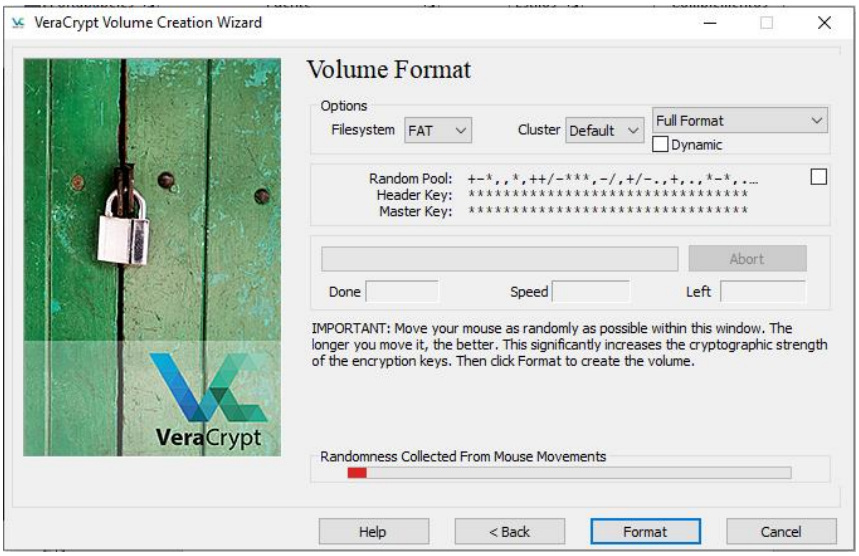
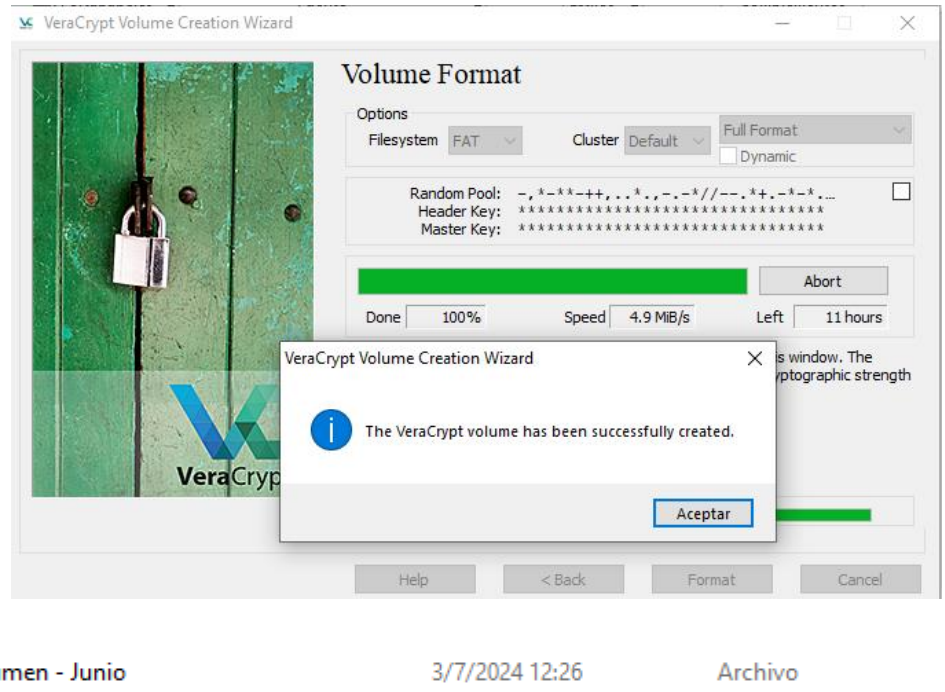


Figura 12 *Formato del Volumen*



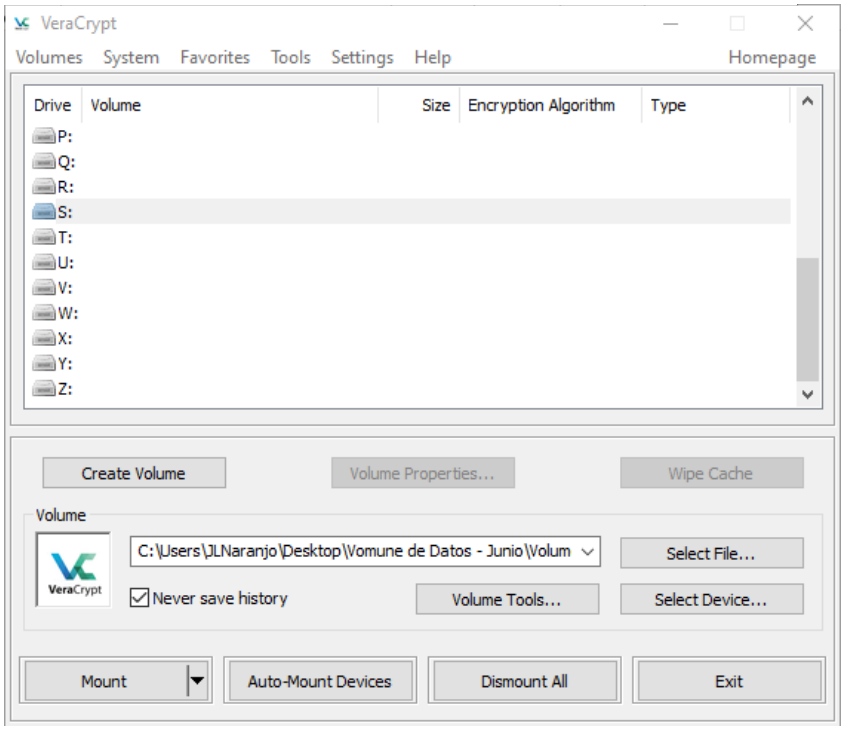
Protegimos el volumen de cifrado con una contraseña, y a su vez elegimos el formato, definiendo como se iban a estructurar los datos dentro del volumen y buscando fortalecer el cifrado de los datos.

Figura 13 *Volumen Creado*



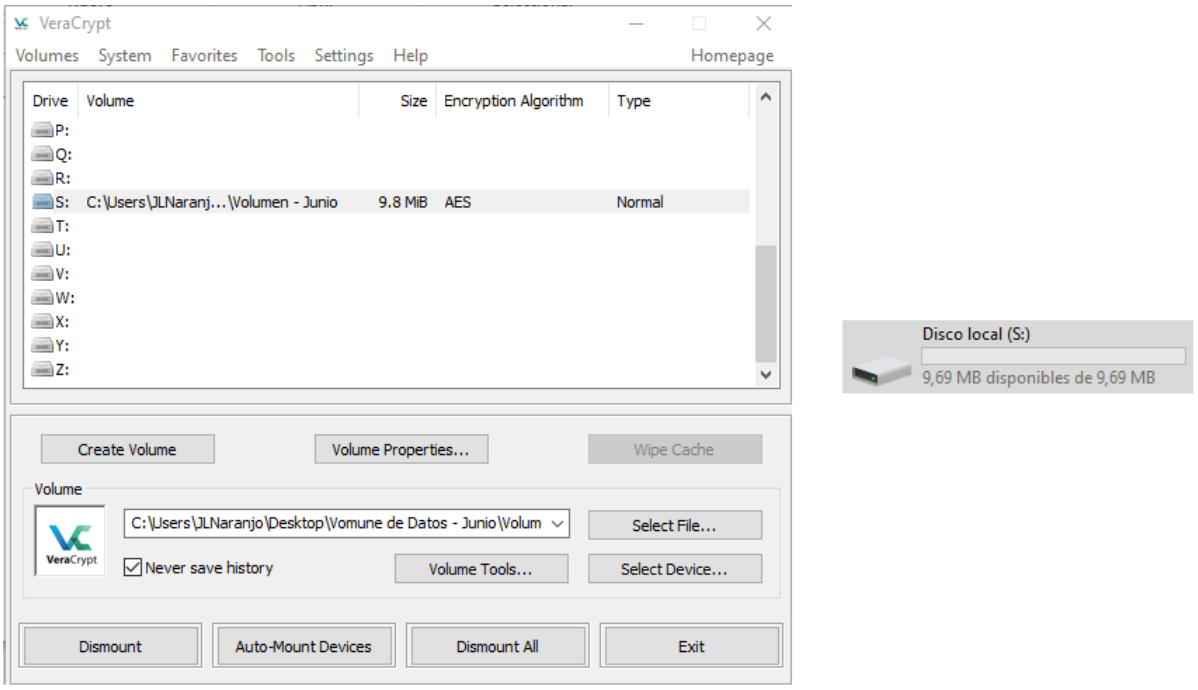
Volumen - Junio 3/7/2024 12:26 Archivo 10.240 KB

Figura 14 *Configuración para montar el volumen*



Una vez creado el volumen, se procedió a configurar el entorno para montar el volumen, se define en que unidad se requiere almacenar. Y seleccionamos el volumen solicitamos montar.

Figura 15 *Volumen Montado*



Como se aprecia, se creó el volumen, y aparece como una nueva unidad en el sistema operativo.

Como finalidad creamos un volumen para proteger la privacidad de datos sensibles, asegurando que solo las personas autorizadas puedan acceder o manipular dicha información.

Bitwarden

Bitwarden es una herramienta de gestión de claves de sistema open-source. Permitirá a los empleados de F.A.D. almacenar y organizar las contraseñas de forma segura, reduciendo así el nivel de vulnerabilidad por falta de contraseñas Diseño de la Solución Integrada

Figura 16 *Interfaz Bitwarden*

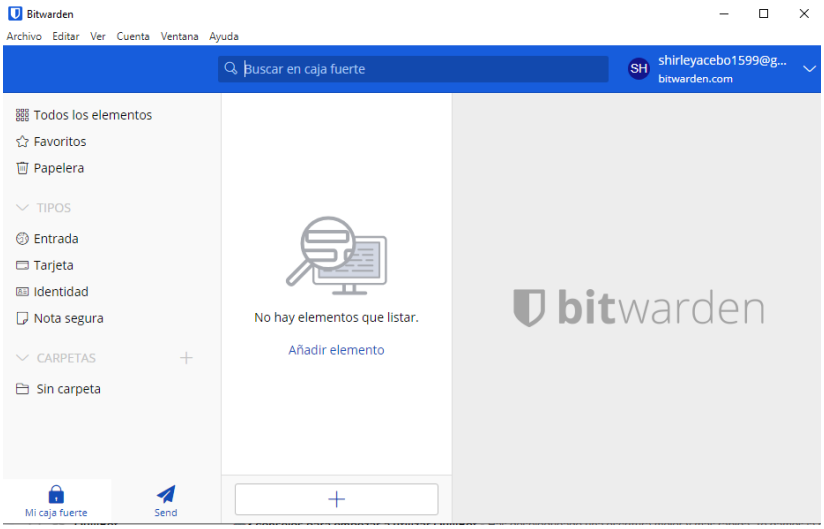
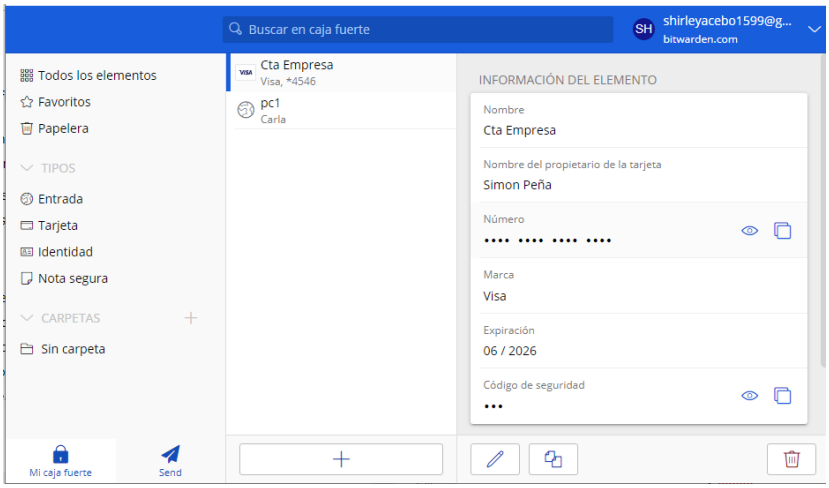


Figura 17 *Gestionar contraseñas Guardadas*



La finalidad de la implementación de esta herramienta se debe a que proporciona de manera segura y eficiente gestionar las contraseñas y datos confidenciales, garantizando la seguridad mediante encriptación robusta.

Protección de Endpoints

ClamAV: Instalado en todos los PCs y portátiles. Configurado para realizar escaneos periódicos y en tiempo real de archivos y correos electrónicos.

VeraCrypt: Usado para cifrar discos duros y particiones en PCs y portátiles que manejan datos sensibles.

Gestión Centralizada de Seguridad

ELK Stack: Logstash recolectará logs de pfSense, Snort, ClamAV y otros dispositivos de red. Elasticsearch almacenará estos logs y Kibana proporcionará paneles de visualización para monitorear la seguridad en tiempo real.

Bitwarden: Implementado como servicio centralizado para la gestión de contraseñas. Los empleados accederán a Bitwarden para generar, almacenar y recuperar contraseñas

seguras.

Respaldo y Recuperación

Duplicati: Configurado para realizar respaldos incrementales diarios de los datos críticos, con almacenamiento cifrado en servidores locales y en la nube.

2.4.2. Proceso de Implementación

2.4.2.1.Preparación del Entorno

- Auditoría del mundo real: Realizar una auditoría de toda su infraestructura.
- Identificación y clasificación de datos críticos y los dispositivos que los manejan.

2.4.2.2.Instalación de Componentes y Configuración

- ClamAV: instalar en todos sus endpoint y programar escaneos regulares y actualizar definiciones de virus.
- VeraCrypt: configurar cifrado completo en todos los dispositivos que manejan datos sensibles.
- Bitwarden: implementar en un servidor dedicado y crear una cuenta para cada miembro de su organización.

2.4.2.3.Implementación de Pruebas y Validación

- Hacer pruebas de penetración y evaluaciones de vulnerabilidad.
- Validar la configuración implementada y su funcionamiento adecuado.
- Reajustar la configuración según sea necesario para mejorar la performance.

2.4.2.4.Implementación de Capacitación y Sensibilización

- Organizar entrenamiento en todas las nuevas herramientas y políticas.
- Implementar sesiones recurrentes de concientización sobre ciberseguridad.

2.4.2.5.Implementación de Monitoreo y Mantenimiento

- Programa de monitoreo continúo usando ELK Stack.
- Actualizaciones de horario y mantenimiento programadas para todas las soluciones de software libre.

CONCLUSIONES

La Fundación de Atención al Discapacitado (F·A·D·) cuenta con una infraestructura de red centralizada en un módem principal, lo cual facilita la gestión y administración de la seguridad de la red· Esta centralización es ventajosa porque permite un control más eficiente y una mejor supervisión de la actividad en la red, lo que es esencial para la implementación de medidas de seguridad robustas·

Actualmente, tiene implementadas medidas de seguridad básicas, como firewalls y antivirus en todos los dispositivos· Sin embargo, estas medidas son insuficientes para proteger contra amenazas avanzadas· La evolución constante de las ciber amenazas requiere soluciones de seguridad más sofisticadas y actualizadas para asegurar una protección efectiva·

Algunos dispositivos presentan limitaciones en memoria RAM y procesadores Estas limitaciones pueden afectar el rendimiento y la capacidad de ejecutar software de seguridad avanzado, Es crucial mejorar el hardware de estos dispositivos para garantizar que puedan soportar las demandas de las nuevas soluciones de ciberseguridad·

La desactivación de servicios remotos en la infraestructura de la F·A·D· restringe la capacidad de gestión y monitoreo remoto de la red dicha limitación puede dificultar la implementación de una supervisión continua y proactiva, esencial para identificar y responder rápidamente a las amenazas cibernéticas·

Como conclusiones identificamos que hay una clara necesidad de actualizar las soluciones de seguridad actuales y proporcionar capacitación recurrente al personal, la actualización de herramientas de seguridad es fundamental para mantenerse al día con las amenazas emergentes, y la capacitación regular del personal en el uso de estas herramientas y en la preparación para desastres es vital para crear una cultura de seguridad dentro de la

organización·

RECOMENDACIONES

- Para mejorar el rendimiento y la capacidad de ejecutar soluciones de seguridad avanzadas, es esencial aumentar la memoria RAM de los dispositivos críticos, como las PCs del administrador y los laptops· Además, es necesario evaluar la actualización de procesadores en estos dispositivos para asegurar un rendimiento óptimo y alineado con los requisitos de las soluciones de ciberseguridad**.**
- Se deben implementar soluciones de software libre eficaces, como ClamAV para escaneos periódicos y en tiempo real de archivos y correos electrónicos, VeraCrypt para cifrar discos duros y particiones, y Bitwarden para la gestión segura de contraseñas, reduciendo el riesgo de brechas de seguridad**.**
- Configurar VLANs para segmentar la red es crucial para reducir riesgos y mejorar la seguridad, limitando el alcance de posibles ataques y facilitando la administración de la seguridad en diferentes áreas de la red**.**
- La implementación de ELK Stack permitirá recolectar y analizar logs de seguridad en tiempo real, proporcionando visibilidad completa de las actividades de la red y facilitando la detección oportuna de actividades inusuales**.**
- Programar pruebas de penetración periódicas es vital para identificar y corregir vulnerabilidades antes de que sean explotadas, asegurando que la organización mantenga una defensa cibernética robusta**.**

REFERENCIAS

Admin. (13 de Diciembre de 2021). *Roldanasociados*. Obtenido de https://roldanasociados.co/conservacion-y-mantenimiento-de-infraestructura/

ALAS, N. (5 de Agosto de 2022). Obtenido de https://noticiasalas.com/tendencias-en-ciberseguridad-y-proteccion-de-datos/

Albarrán, C. &. (17 de MAYO de 2024). Obtenido de https://www.redestelecom.es/especiales/que-es-una-vpn-para-que-sirve-y-como-funciona/

Barbosa, D. C. (02 de Enero de 2020). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

Bodnar, D. (29 de Octubre de 2020). *Avast*. Obtenido de https://www.avast.com/es-es/c-social-engineering

Ciberseg. (19 de Noviembre de 2019). *Ciberseguridad*. Obtenido de https://ciberseguridad.com/normativa/espana/medidas/

Cisco. (23 de febrero de 2024). *Anatomía de un ataque*. Obtenido de https://www.scribbr.es/citar/generador/folders/2rhk4fvzAhJ8pSPNRu6IRw/lists/WNxSGXq9pyjgwhH3Ner4X/

Compusoluciones. (12 de JUNIO de 2024). Obtenido de https://www.compusoluciones.com/soluciones/ciberseguridad/

De Docusign, C. (5 de Julio de 2023). *docusign.* Obtenido de https://www.docusign.com/es-mx/blog/lciberseguridad-en-las-pymes

Díaz, D. M. (26 de enero de 2024). *bitlifemedia.* Obtenido de

https://bitlifemedia.com/2024/01/la-importancia-de-los-ejercicios-de-red-team/

Docusign. (5 de Julio de 2023). Obtenido de https://www.scribbr.es/citar/generador/folders/5qgHXyqOYZjRlGgH0K2jE2/lists/6fCmlH1njtBlLIfJj4udAm/

Economista, E. (12 de Diciembre de 2012). *El Economista*. Obtenido de https://www.eleconomista.com.mx/el-empresario/Software-libre-opcion-para-pymes-20121227-0132.html

Euncet. (10 de junio de 2024). Obtenido de https://blog.euncet.com/ciberseguridad-pymes#%C2%BFCUAL_ES_LA_ESTRUCTURA_DE_UN_SISTEMA_INFORMATICO_SEGURO

Firewall, C. N. (10 de febrero de 2023). Obtenido de Cisco: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

GNU. (s.f.). Obtenido de https://www.gnu.org/philosophy/free-sw.es.html

Group, O. C. (14 de MARZO de 2022). Obtenido de https://www.orbit.es/8-soluciones-de-ciberseguridad-imprescindibles/

IBM. (s.f.). Obtenido de https://www.ibm.com/es-es/topics/intrusion-detection-system

IBM. (s.f.). *IBM*. Obtenido de https://www.ibm.com/mx-es/topics/penetration-testing

Imfoem. (s.f.).

Institute, C. R. (21 de Septiembre de 2021). *Cyber Readiness Institute*. Obtenido de https://cyberreadinessinstitute.org/es/news-and-events/fortalecimiento-de-la-postura-de-ciberseguridad-de-la-comunidad-de-pequenas-empresas-de-estados-unidos/

Kaira. (2023). Estas son las 10 amenazas Cibernéticas más comunes. *Canvia*.

Kapersky. (05 de Abril de 2021). Obtenido de https://latam.kaspersky.com/about/press-releases/2021_mas-de-la-mitad-de-las-victimas-de-ransomware-paga-el-rescate-pero-solo-un-cuarto-recupera-sus-datos

Kapersky. (13 de junio de 2024). Obtenido de https://latam.kaspersky.com/resource-center/definitions/encryption

Libre., U.-O. d. (9 de Noviembre de 2021). *UCM*. Obtenido de https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Malwarebytes. (3 de Junio de 2020). Obtenido de https://es.malwarebytes.com/antivirus/#:~:text=En%20gran%20parte%2C%20%E2%80%9Cantivirus%E2%80%9D,proteger%20y%20eliminar%20software%20malicioso.

OEA. (2019). *DESAFÍOS DEL RIESGO*. Cicte.

QuestionPro. (17 de Enero de 2023). Obtenido de https://www.questionpro.com/blog/es/seguridad-informatica-para-pymes/

Rodriguez, D. (13 de MAYO de 2023). *TecnoSoluciones*. Obtenido de https://tecnosoluciones.com/licencias-de-software-de-codigo-abierto-open-source/

RoleCatcher. (Noviembre de 2023). Obtenido de https://rolecatcher.com/es/habilidades/habilidades-duras/trabajar-con-computadoras/configuracion-y-proteccion-de-sistemas-informaticos/eliminar-virus-informaticos-o-malware-de-una-computadora/

Skyone. (22 de ABRIL de 2024). *Skyone*. Obtenido de

https://skyone.solutions/es/blog/evaluacion-de-vulnerabilidad-pentest-comprender-lvb6u52e/

Teldat. (26 de Abril de 2023). Obtenido de https://www.teldat.com/es/blog/principales-ciberataques-ciberseguridad-para-las-pymes/

Unir. (15 de Junio de 2021). *Unir Ecuador*. Obtenido de https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

Zendesk. (1 de Marzo de 2024). *¿Qué es la ciberseguridad y cuál es su relación con la IA?* Obtenido de https://www.zendesk.com.mx/blog/ciberseguridad/