



**UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN,
FINANZAS E INFORMÁTICA**

PROCESO DE TITULACIÓN

ABRIL 2022 – SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O FIN DE CARRERA ESTUDIO DE CASO

PRUEBA PRACTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO(A) EN SISTEMAS

TEMA:

ANÁLISIS TÉCNICO DE LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS

DE LA UNIDAD EDUCATIVA ENEIDA UQUILLAS DE ROJAS.

EGRESADO:

EDDER SANTIAGO CASTILLO LEON

TUTOR:

ING. JOFFRE VICENTE LEÓN ACURIO

AÑO 2022

RESUMEN

El presente trabajo de investigación corresponde al tema de Análisis Técnico de la seguridad en sistemas informáticos estudio que tuvo como lugar de origen la Unidad Educativa “Eneida Uquillas de Rojas”, fue fundada en 1946, y está ubicada en el recinto La Teresa, en la Parroquia Febres Cordero, donde residen unos 200 estudiantes, el propósito de la investigación es con el objetivo de realizar un análisis técnico en el sistema informático de la Unidad Educativa, para mejorar la seguridad en sus sistemas de información, para la cual colaboraron 12 maestros que sirvieron de muestra en el estudio, donde se utilizó una investigación de nivel descriptivo, esta es el primer nivel en taxonomía de la investigación científica, donde permite recopilar, analizar, y poder entablar una relación acorde al tema, para el proceso de esta investigación se utilizó la investigación de campo que mediante la observación directa permite poner en evidencia si existe vulnerabilidades en los sistemas de cómputo de manera ágil y precisa, en la cual se espera encontrar unidades antiguas, sistemas operativos sin soporte, routers o sistemas de cableado en mal estado, etc. También se elaboró una pequeña encuesta que dio como conclusión que, en la unidad, se encontró evidencia que el Windows con el que cuenta la institución es Windows 7, un sistema operativo que ya no tiene soporte y es una coladera hablando en términos informáticos, por lo que esto representa una gran vulnerabilidad en la actualidad.

Palabras Claves: análisis técnico, seguridad, ciberseguridad, sistema, seguridad de la información, soporte.

ABSTRACT

The present research work corresponds to the subject of Technical Analysis of security in computer systems, a study that had as its place of origin the Educational Unit "Eneida Uquillas de Rojas", it was founded in 1946, and is located in the La Teresa campus, in the Febres Cordero Parish, where some 200 students reside, the purpose of the research is to carry out a technical analysis in the computer system of the Educational Unit, to improve the security of its information systems, for which 12 teachers who collaborated served as a sample in the study, where a descriptive level investigation was used, this is the first level in taxonomy of scientific research, where it allows collecting, analyzing, and being able to establish a relationship according to the theme, for the process of this investigation used field research that through direct observation allows to show if there are vulnerabilities in computer systems in an agile and precise way, in which it is expected to find old units, unsupported operating systems, routers or wiring systems in poor condition, etc. A small survey was also carried out that concluded that, in the unit, evidence was found that the Windows that the institution has is Windows 7, an operating system that is no longer supported and is a drain speaking in computer terms, for what this represents a great vulnerability at present.

Keywords: technical analysis, security, cybersecurity, system, information security, support.

ÍNDICE DE CONTENIDOS

RESUMEN.....	2
ABSTRACT.....	3
1. INTRODUCCIÓN.....	5
2. DESARROLLO.....	6
2.1 Justificación.....	6
2.2 OBJETIVOS.....	7
2.3 SUSTENTO TEÓRICO.....	8
2.3.1 Seguridad Informática.....	8
2.3.2 Principales Tipos de Seguridad.....	8
2.3.3 Hardware.....	8
2.3.4 Software.....	9
2.3.5 Seguridad en las Redes.....	9
2.3.6 Principales Tipos de Amenazas a los Sistemas Informáticos.....	10
2.3.7 Vulnerabilidades y amenazas informáticas.....	10
2.3.8 Vulnerabilidad.....	10
2.3.9 Amenaza Informática.....	10
2.3.10 Amenazas de Malware.....	11
2.3.11 Clasificación del Malware.....	11
2.3.12 Spyware.....	11
2.3.13 RootKit.....	12
2.3.14 Virus.....	12
2.3.15 Gusano.....	12
2.3.16 Troyano.....	12
2.3.17 Vulnerabilidades de Sistema.....	13
2.3.18 Amenazas de Ataques externas.....	13
2.3.19 DDOS.....	13
2.3.20 Vulnerabilidades producidas por contraseñas.....	14
2.3.21 Vulnerabilidades producidas por usuarios.....	14
2.3.22 Pilares importantes en la información.....	15
2.3.23 Confidencialidad:.....	15
2.3.24 Integridad:.....	15
2.3.25 Disponibilidad:.....	15
2.4 Marco Metodológico.....	16
2.5 Resultados Obtenidos.....	16
2.6 Discusión de Resultados.....	25
3. Conclusiones.....	26
4. Referencias.....	27
5. Anexos.....	29
24.....	; Error! Marcador no definido.
100%.....	; Error! Marcador no definido.
1 Minuto.....	; Error! Marcador no definido.

1. INTRODUCCIÓN

La seguridad en las computadoras es un tema que no se debe minimizar, cada vez más son las unidades educativas que poseen un sistema informático para el envío y recepción de información que es importante para las actividades diarias en la que están involucrados tanto los docentes como la información de los estudiantes, y esta debe ser inviolable, manteniendo la confidencialidad, siendo así la seguridad informática como la mejor aliada de las empresas, universidades, etc. (UNIR, 2021).

Por este motivo el propósito del caso de estudio es brindar una mejor seguridad en los equipos de cómputos de la Unidad Educativa Eneida Uquillas de Rojas cuya institución posee computadoras que no han sido debidamente revisadas ni parcheadas y sobre todo tiene mucho tiempo sin alguna revisión técnica por lo que el riesgo en su seguridad es relativamente alto, pudiendo ser blanco de ataques a sus equipos por parte de personal ajeno a la institución.

Por tal razón se ha utilizado un tipo de investigación cualitativa, que ayuda a describir el escenario mediante la observación directa de los equipos informáticos que posee la Unidad Educativa Eneida Uquillas Rojas, y establecer una causa-efecto de las vulnerabilidades encontradas que posteriormente se guardan en una bitácora, para establecer la mejor herramienta que mitigue tal falla en las computadoras.

Siendo este caso de estudio posible, por la integración de conocimientos adquiridos a lo largo del periodo académico que dura la carrera de sistemas, en los cuales hay materias desde redes, sistemas operativos, pasando por la seguridad de información o ciberseguridad, dando la posibilidad de ejecutar conocimientos adquiridos a lo largo de la carrera universitaria en la Universidad Técnica de Babahoyo.

Cabe recalcar que la Unidad Educativa Eneida Uquillas de Rojas, fue fundada en 1946, y está ubicada en el recinto La Teresa, en la Parroquia Febres Cordero, donde residen unos 200 estudiantes que diariamente van a recibir sus lecciones, otro dato es que no hay personal en el área de informática, por lo que se supone que no debe haber un mantenimiento técnico en varios años, y como último punto para este proceso se usa la línea de investigación “Sistemas de información y comunicación, emprendimiento e innovación”, en conjunto con la sub línea “Redes de tecnologías inteligentes de software y hardware”.

2. DESARROLLO

2.1 Justificación

Mediante un análisis a los sistemas de información en la Unidad Educativa Eneida Uquillas de Rojas, se podrá minimizar el impacto que un desastre ocasionado por alguna infiltración de Malware o Rasonware afecte la integridad de la información que maneja la institución y dejando inutilizado la forma de envío de información que maneja la institución escolar, ocasionando lentitud en los procesos que pasarían a ser realizados manualmente.

El mal uso de los recursos informáticos puede ocasionar desastres en los datos que maneja una institución, de estas vulnerabilidades se aprovechan muchos atacantes por los fallos de seguridad que quedan en los equipos que son usados para las labores administrativas, que en ocasiones el no tener un sistema completamente robusto pueden ocasionar pérdidas tanto de información sensibles como también pérdidas en la infraestructura educativa, siendo blancos potenciales a infecciones de tipo malware.

También es fundamental que el personal que labora en dicha institución pueda hacer conciencia de la importancia de mantener un sistema con un nivel de seguridad alto, para no pasar contratiempos que implique fuga de información sensible que pueda afectar la integridad de algún docente que labora en el lugar, donde cada vez más se observa como la seguridad informática en las instituciones son casi nulas, no teniendo conciencia de la importancia que es mantener los datos de manera segura, por el bien de la institución, donde una pérdida de datos en la actualidad implica perder una parte vital que permite la vida digital.

El caso de estudio también tiene un grado de innovador dado que en la Unidad Educativa Eneida Uquillas de Rojas no se han dado estudios de este tipo en el cual se pueda enseñar a los docentes que ahí laboran la importancia de mantener un equipo en óptimas condiciones, que no solo sirve para el trabajo diario, también sirve para salvaguardar la confidencialidad de la información que se maneja en la escuela, esto es crucial para las autoridades educativas que laboran, también el proyecto es factible, tanto por los permisos solicitados donde las autoridades están presto a colaborar, como el de la búsqueda de información para el sustento que aproxime a conocer a profundidad mediante el uso de libros, artículos científicos académicos, o folletos de impacto y relevancia para la investigación.

2.2 OBJETIVOS

Objetivo General

Realizar un análisis técnico en el sistema informático de la Unidad Educativa “Eneida Uquillas de Rojas” perteneciente a la Parroquia Febres Cordero - Babahoyo, para mejorar la seguridad en sus sistemas de información.

Objetivos Específicos

- Realizar una investigación detallada de las vulnerabilidades y problemas a los que se enfrentan los sistemas de información.
- Diagnosticar los puntos débiles encontrados en el análisis de los sistemas de información en la Unidad Educativa Eneida Uquillas Rojas.
- Realizar las sugerencias respectivas para corregir las vulnerabilidades críticas en el sistema de información a las autoridades respectivas de la Unidad Educativa Eneida Uquillas de Rojas.

2.3 SUSTENTO TEÓRICO

2.3.1 Seguridad Informática

Unir (2021) sostiene que la seguridad informática, también conocida como ciberseguridad, hace referencia a la protección de la información y, en particular, su tratamiento, con el objetivo de evitar la manipulación de datos y datos por parte de personas no autorizadas, su objetivo principal es que las personas, equipos y datos estén protegidos contra daños y amenazas de terceros (pág. 1). Esto en palabras propias no es más que el cuidado que se debe mantener en que los sistemas estén bien protegidos sin que exista brechas o vulnerabilidades en el sistema que sean blanco de los ciberdelincuentes.

Es por esto que esta disciplina en el campo de la tecnología de la información es responsable de la protección de la confidencialidad de los sistemas informáticos donde se ha convertido en una parte indispensable de las actividades comerciales y empresariales. Es claro que no existen sistemas infalibles, por lo que las organizaciones que se comunican a través del mundo deben buscar los mecanismos adecuados para garantizar la seguridad de sus datos, a través de ciertos tipos de seguridad que existen y debería implementarse en las agencias (UNIR, 2021).

2.3.2 Principales Tipos de Seguridad

Las fallas de seguridad que pueden comprometer el sano desarrollo de los procesos informáticos de una institución pueden venir desde varias direcciones y son:

2.3.3 Hardware

Unir (2021), indique que la seguridad está relacionada con los dispositivos de protección utilizados para proteger los sistemas y redes, aplicaciones y programas contra amenazas externas contra diversos riesgos, el método más utilizado es la gestión de servidores proxy no disruptivos, cortafuegos, módulos de seguridad de hardware y prevención de pérdida de datos. Esta seguridad también se refiere a proteger la data del daño físico. Para Intel compañía de microchips (2022), cuando se trata de proteger el hardware de sus computadoras, muchos administradores de TI primero piensan en comprar software, como programas antimalware o antivirus, sin embargo, los

ataques cibernéticos bajan en la pila del sistema. La seguridad del software por sí sola ya no es suficiente para proteger las computadoras, la protección debe estar integrada en el propio hardware (pág. 1).

2.3.4 Software

Estruga Niura (2021), afirma que es responsable de salvaguardar la información almacenada en los sistemas informáticos. Es el principal responsable de bloquear y prevenir ataques de piratas informáticos maliciosos en programas y datos de la empresa. Donde existen un buen número de prestaciones en servicios de programas informáticos para prevenir un ataque en común, estos suelen ser desde antivirus, hasta programas de detección de intrusos que se encarga de proporcionar un entorno que evita muchos ataques provenientes de la red (pág. 1).

2.3.5 Seguridad en las Redes

Gómez A. (2022), indica que la seguridad de la información en redes es la que está relacionada con el diseño de actividades destinadas a proteger los datos accesibles a través de la red y que probablemente se modifiquen o utilicen indebidamente. Las principales amenazas en este dominio son: troyanos, phishing, spyware, robo de datos y robo de identidad y otros programas maliciosos ya descritos como malware (pág. 10).

De esta manera analizo y es que los productos de software de seguridad de red evitan el acceso no autorizado a las redes informáticas. Las organizaciones utilizan estas aplicaciones para evitar intrusiones no autorizadas, maliciosas o inadvertidas en sistemas seguros. Las soluciones de seguridad de red están diseñadas para reconocer el tráfico legítimo en las complejas redes empresariales actuales y los eventos anormales para una mayor investigación. También realizan auditorías de seguridad y cumplimiento normativo, pueden incluir funciones antispam, antivirus y de intrusión. El software de seguridad de redes está relacionado con los sistemas de seguridad informática y las herramientas de supervisión de redes (Gómez, 2022, pág. 12).

Para Cisco (2022), la red cambió la forma en que vivimos, trabajamos y jugamos, todas las organizaciones que desean proporcionar servicios solicitados de clientes y empleados necesitan proteger su red. La seguridad de la red también ayuda a proteger a los equipos sensibles de cualquier ataque que provenga de redes ajenas, a la que está normalmente el equipo de trabajo donde se mantienen los equipos (pág. 1).

2.3.6 Principales Tipos de Amenazas a los Sistemas Informáticos

2.3.7 Vulnerabilidades y amenazas informáticas

La dependencia de las empresas de la tecnología de la información para llevar a cabo sus actividades comerciales principales ha generado un alto nivel de preocupación por la seguridad cibernética. Las vulnerabilidades y amenazas de TI suponen un riesgo para los sistemas y la información empresarial, especialmente en el entorno actual altamente digitalizado y dependiente de TI (AMBIT, 2020). Para tomar las medidas adecuadas para proteger la tecnología y la información de la empresa, es necesario conocer las principales amenazas y vulnerabilidades que amenazan la seguridad de la red de la empresa.

2.3.8 Vulnerabilidad

Moe Tibor (2020), indica que una vulnerabilidad de seguridad es un componente del código de software que identifica fallas de seguridad en aplicaciones, sistemas y redes para que los usuarios avanzados puedan explotarlas. Por lo general, se incluyen con otro software y se distribuyen en un kit, los exploits a menudo se alojan en las webs afectadas. Los piratas informáticos pueden enviar correos electrónicos de phishing para que las posibles víctimas visiten estas páginas web (Tibor , 2020, pág. 1).

Las vulnerabilidades son uno de los principales motivos por los que una empresa puede sufrir un ataque informático a sus sistemas. Por esta razón, siempre es recomendable actualizar las aplicaciones informáticas, sistemas de protección y sistemas operativos a las últimas versiones, ya que estas actualizaciones contienen muchas correcciones para las vulnerabilidades descubiertas y de esta forma se mantiene seguro el sistema.

2.3.9 Amenaza Informática

Una amenaza informática es cualquier acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas cibernéticas a las empresas provienen en gran medida de fuentes externas, aunque también existen amenazas internas por tal motivo siempre es necesario que se capacite al eslabón más débil que es el usuario el que trabaja al lado de la computadora donde siempre se aprovechan a base de ingeniería social, para poder sacar información válida que permita el ataque al sistema informático (Eulises Ortiz, 2020).

2.3.10 Amenazas de Malware

La empresa Oracle (2022), en su portal web define a malware como, un término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, troyanos, ransomware, spyware, adware, scareware, etc. Puede adoptar la forma de código ejecutable, contenido activo y otro software de tal manera que trate de pasar desapercibido para el usuario y de esta manera aprovecharse de él sistema (pág. 1). También el malware en definición corta es todo software que es perjudicial al sistema, así sea un adware, que es un software invasivo que otorga publicidad.

2.3.11 Clasificación del Malware

El malware o virus informático, a lo largo de la historia de evolución en temas computacionales ha tenido la siguiente clasificación:

- Spyware
- RootKit
- Virus
- Gusano
- Troyano
- Rasonware

2.3.12 Spyware

El software espía es un software malicioso que recopila información de una computadora y luego transmite esa información a una entidad externa sin el conocimiento o consentimiento del propietario de la computadora, siendo de manera sigilosa monitorizado, sin que la víctima sospeche de algún fallo en sus sistemas (Malwarebytes, 2022). Este programa por lo general viene en algún software o página web donde mediante un fallo del navegador se aprovechan para colarse en el sistema, y empieza a recabar información de la institución y del propio usuario encargado de trabajar en el sitio.

2.3.13 RootKit

Un RootKit es un paquete de software malicioso diseñado para permanecer en una computadora mientras brinda acceso y control remotos. Los ciberdelincuentes los utilizan para alterar la computadora sin el conocimiento o consentimiento del usuario, este programa siempre está con un objetivo definido claro, y es él de proveer de acceso root de los sistemas a los que invade para tener control de todo en él sistema (Red Seguridad , 2021).

2.3.14 Virus

Matachana (2020), indica que los virus informáticos, son una amenaza para la sociedad, problemas que no se ha manejado de la forma más correcta, porque siempre están afectado a otras personas, por lo general este virus mantiene siempre un orden de ataque y un objetivo que es planteado por los ciberdelincuentes, como el ataque de infraestructuras militares, de gobierno, instituciones educativas, bancos, etc. (pág. 10)

2.3.15 Gusano

Es uno de los malware más comunes que atacan los equipos y sistemas de una empresa porque no requiere la intervención del usuario ni la modificación de un archivo para infectar una computadora. El objetivo de los gusanos es replicar e infectar tanto como sea posible utilizando la red para hacerlo. Representan una amenaza para las redes corporativas porque una sola computadora infectada puede afectar a toda la red con el tiempo (Torres López, 2022). El gusano también es uno de los virus informáticos que más edad en el mundo de la computación mantiene, siendo uno de los primeros virus que afectaba desde hace tiempo las computadoras.

2.3.16 Troyano

Son un programa o fragmento de código que puede parecer legítimo y seguro, pero en realidad es malware. Los troyanos son software incrustado en programas pirateados y generalmente están diseñados para espiar a las personas infectadas o robar datos. Muchos troyanos también descargan malware después de la instalación, otro objetivo es siempre abrir una puerta trasera que posteriormente será explotada por él atacante, que probablemente quiere sacar información confidencial sin perder el control del equipo (Avast, 2022).

2.3.17 Vulnerabilidades de Sistema

Los sistemas y aplicaciones informáticas suelen tener algunas fallas en su diseño, estructura o código que provocan inestabilidad. No importa cuán pequeño sea el delito, ya sea un punto de acceso externo o un ataque interno, siempre puede amenazar los sistemas y la información. Por lo consiguiente, los de extremos peligros son:

- Error de configuración.
- Error de gestión de recursos.
- Error de validación en el sistema.
- Error de accesos a directorios.
- Error en la gestión de permiso.

2.3.18 Amenazas de Ataques externas

Siempre en un ataque es más probable que este venga del exterior, dado que los demás ataques que lo hacen desde el interior deben burlar la seguridad que muchas instituciones poseen como prohibido el personal no autorizado, etc. Por tal motivo los atacantes siempre tratan de explotar recursos externos que su único medio por el que lo realizan sea la misma internet o la gran red de redes, por tal m motivo entre los ataques más comunes tenemos los siguientes:

2.3.19 DDOS

Es un ataque de denegación de servicios distribuidos, ocurre cuando el servidor recibe una gran cantidad de solicitudes de acceso, lo que sobrecarga el sistema y hace que el servidor se bloquee o falle (retraso antes de recibir o bloquear mensajes de error). La mayoría de las computadoras (bots) utilizadas para llevar a cabo este tipo de ataque solo querrán ese servidor, de manera que la mayoría de los servicios sino es que completamente dejan de funcionar debido al colapso que esto ocurre al no poder gestionar tantas solicitudes o peticiones (Karsperky , 2022). Este ataque es muy popular debido a grandes organizaciones que los usan como los Anonymous.

2.3.20 Vulnerabilidades producidas por contraseñas

Con el trabajo remoto y la computación en la nube, la gestión de contraseñas se ha convertido en uno de los aspectos más importantes de la ciberseguridad. Se requiere usuario y contraseña para acceder a las plataformas de servicios de la empresa. El uso de contraseñas seguras crea vulnerabilidades de seguridad en los sistemas porque si son fáciles de descifrar, pueden exponer el acceso de terceros no autorizados que pueden robar, modificar o eliminar información, modificar sistemas o inhabilitar computadoras (OSI, 2019).

2.3.21 Vulnerabilidades producidas por usuarios

Para Gómez A. (2022), una de las principales causas de los ataques informáticos es el error o negligencia del usuario. La configuración incorrecta de privilegios o permisos puede hacer que los usuarios accedan a controles o configuraciones para los que no están preparados y cometan errores que amenacen a la empresa. El error humano es una de las principales causas de la ciberseguridad. El usuario siempre corre el riesgo de un error que puede generar inestabilidad, lo que puede generar una vulnerabilidad de seguridad informática. Por lo tanto, la ciberseguridad requiere medidas automatizadas para reducir o eliminar el riesgo de error humano (pág. 15).

Esto concuerda, porque la mayoría de los usuarios que trabajan en algún puesto donde la información es sensible, siempre tratan de recordar la contraseña que les genera el administrador de sistemas de la empresa, igual la mente es volátil y es necesario siempre respaldarlo, el problema es cómo se respalda esa información sensible, la opción que más usan es guardar la clave en un papel, que descuidadamente luego se pierde en el sector de trabajo, cae en manos enemigas que luego proceden a explotar esa falla humana.

Malas prácticas o falta de formación en ciberseguridad, archivos de código abierto, fraude y publicidad engañosa, apertura de correos falsos, etc. También puede dar lugar a vulnerabilidades de seguridad, cuyas acciones dan lugar a ataques como el phishing o amenazas similares donde se ve perjudicada la confidencialidad e integridad de los datos de la institución que se ve afectada por este mal proceder (AMBIT, 2020). Para que esto no suceda siempre existen una solución y es la capacitación a la que se debe someter un trabajador para que no comprometa con una acción involuntaria la seguridad del sistema.

2.3.22 Pilares importantes en la información

Con el auge de los ataques físicos y los delitos cibernéticos, la seguridad de los datos se ha convertido en una prioridad para las organizaciones de tal manera que es un campo con una creciente demanda por parte de las empresas que quieren invertir en seguridad. Por lo tanto, antes de tomar medidas para mejorar la seguridad de sus datos, es importante apoyar los conceptos básicos:

2.3.23 Confidencialidad:

Este principio trata sobre la privacidad de los datos y, por lo tanto, incluye las medidas tomadas para garantizar que la información privada y confidencial esté protegida y no sea robada mediante ataques cibernéticos, espionaje u otros delitos cibernéticos que expondrían datos sensibles que solo le debe pertenecer al propietario siendo esta una personas natural, jurídica o institucional (CEPAL, 2020).

2.3.24 Integridad:

La información íntegra es uno de los parámetros de calidad de los datos, cuya pérdida puede afectar seriamente la confidencialidad; por ejemplo, si una persona ingresa en un caso de fraude por error o debido a un error en la información de la persona, perderá ciertos derechos u oportunidades, como rechazar un préstamo, perder oportunidades laborales o perder beneficios por lo que es necesario cumplir a cabalidad este criterio (Bco. Santander, 2021).

2.3.25 Disponibilidad:

El acceso oportuno a la información significa adoptar sistemas que aseguren que las personas tengan acceso a los documentos necesarios, así como a las actividades, servicios e información con que cuenta la empresa. El acceso también incluye la integración de varios sistemas y técnicas que ayudan a prevenir y repeler ataques cibernéticos que interrumpen los servicios. En la mayoría de los casos, estas intromisiones son realizadas por terceros u organizaciones, dando lugar a la entrada de usuarios no autorizados y no autorizados (Avast, 2022).

2.4 Marco Metodológico

Para el caso de estudio se siguió la investigación de nivel descriptivo, es el primer nivel en taxonomía de la investigación científica, donde permite recopilar, analizar, y poder entablar una relación acorde al tema que es análisis técnico de la seguridad en los sistemas informáticos, donde el lugar en el que se va a realizar este tipo de análisis es en la Unidad Educativa “Eneida Uquillas de Rojas”.

En el proceso de esta investigación se utilizó la investigación de campo que mediante la observación directa permite poner en evidencia si existe vulnerabilidades en los sistemas de cómputo de manera ágil y precisa, en la cual se espera encontrar unidades antiguas, sistemas operativos sin soporte, routers o sistemas de cableado en mal estado, etc. Problemas que son necesario detectar para asegurar una correcta transmisión de información que se confiable, integra y sin errores.

También se utilizó el método bibliográfico este me permite ubicar libros, revistas, artículos, papers, y todo sustento que brinde información de manera confiable para tener la conceptualización del problema clara, y poder ejecutar el razonamiento crítico a la hora de realizar un respectiva conclusión o sugerencia de acuerdo al caso de investigación y que facilite la comprensión a los lectores ubicando términos adecuados.

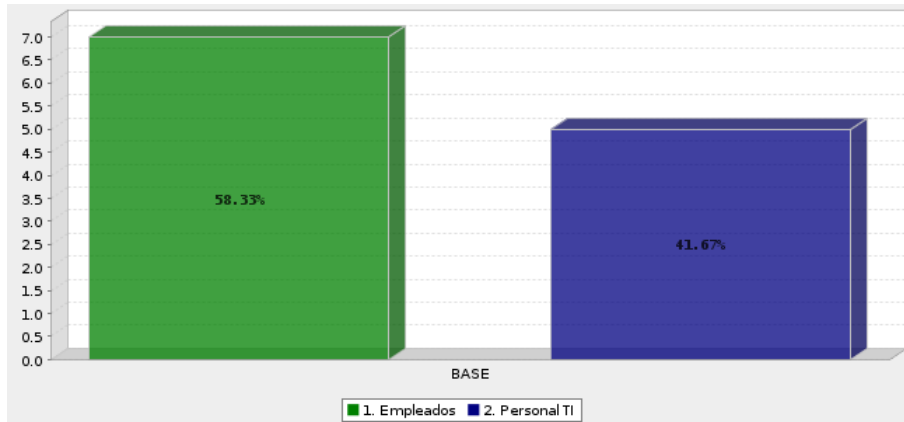
Se uso además el método deductivo, que permite ir de lo general a lo específico, ampliamente usado para generar conocimientos empíricos a la hora de realizar proyectos de investigación, además se empleó una encuesta al personal docente de la institución que consta de 8 preguntas a 12 profesores de la Unidad Educativa Eneida Uquillas de Rojas para tener datos concretos a la hora de realizar la solución respectiva.

2.5 Resultados Obtenidos

La encuesta que se les realizo a los 12 profesores que amablemente participaron como muestra para la investigación arrojó los siguientes resultados:

Q1. ¿Quién es responsable de instalar y mantener el software de seguridad en sus computadoras?

Ilustración 1: El responsable de instalar y mantener el software de seguridad en las computadoras.



Elaborado por: El Autor

Tabla 1: El responsable de instalar y mantener el software de seguridad en las computadoras.

	Answer	Count	Percent
1.	Empleados	7	58.33%
2.	Personal TI	5	41.67%
	Total	12	100%
Mean: 1.417	Confidence Interval @ 95%: [1.125 - 1.708]	Standard Deviation: 0.515	Standard Error: 0.149

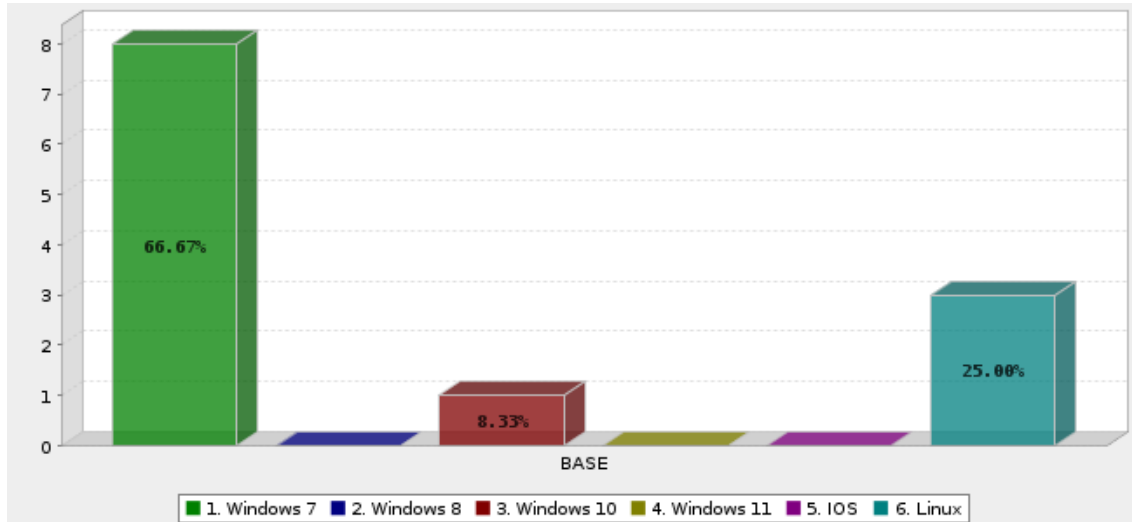
Elaborado por: El Autor

Análisis e Interpretación

7 profesores concuerdan que los empleados de la institución deben hacer estas tareas de instalación y mantenimiento del software lo cual es un error debido que un profesional en TI es más recomendable si se desea dejar en óptimas condiciones los sistemas informáticos.

Q2. ¿Qué versión de Windows está instalada en el equipo que normalmente usas para conectarte a Internet en la institución?

Ilustración 2: La versión de Windows en el equipo.



Elaborado por: El Autor

Tabla 2: La versión de Windows en el equipo.

	Answer	Count	Percent
1.	Windows 7	8	66.67%
2.	Windows 8	0	0.00%
3.	Windows 10	1	8.33%
4.	Windows 11	0	0.00%
5.	IOS	0	0.00%
6.	Linux	3	25.00%
	Total	12	100%

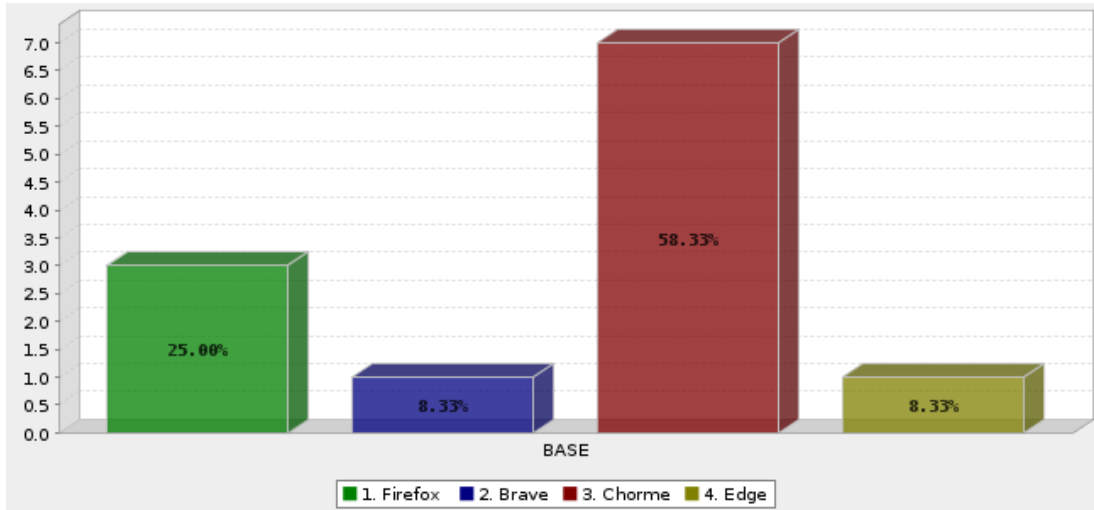
Elaborado por: El Autor

Análisis e Interpretación

Como se puede observar el Windows con el que cuenta la institución es Windows 7, un sistema operativo que ya no tiene soporte y es una coladera hablando en términos informáticos, por lo que esto representa una gran vulnerabilidad en la actualidad.

Q3. ¿Qué navegador web utilizas normalmente?

Ilustración 3: El navegador que usa.



Elaborado por: El Autor

Tabla 3: El navegador que usa.

	Answer	Count	Percent
1.	Firefox	3	25.00%
2.	Brave	1	8.33%
3.	Chrome	7	58.33%
4.	Edge	1	8.33%
	Total	12	100%
Mean: 2.500 Confidence Interval @ 95%: [1.934 - 3.066]		Standard Deviation: 1.000	Standard Error: 0.289

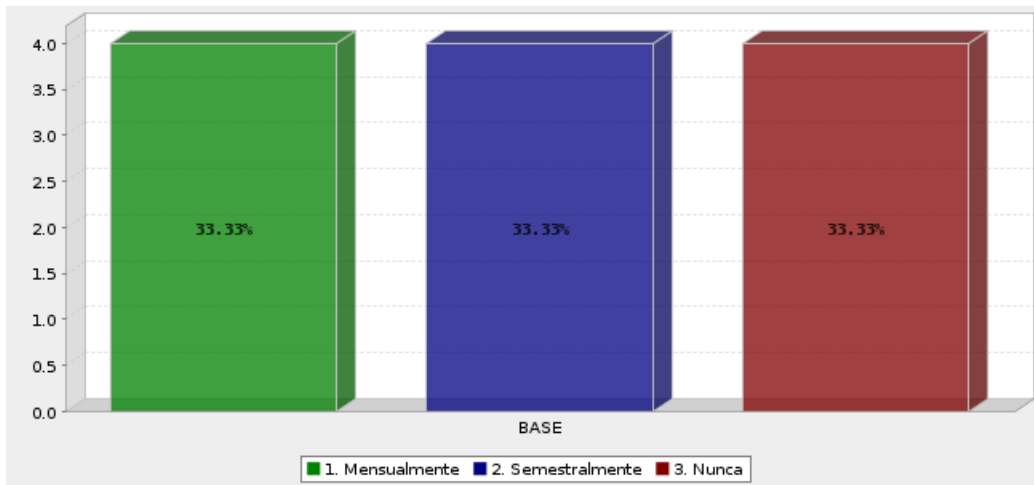
Elaborado por: El Autor

Análisis e Interpretación

El navegador que más usa la institución es Chrome que ciertamente es más seguro, pero de nada vale que un 58.3% afirme esto, si el sistema el elemento principal muestra vulnerabilidad al mantener un software viejo y sin soporte.

Q4. ¿Con qué frecuencia utilizas actualiza sus sistemas?

Ilustración 4: Frecuencia con que se actualiza el sistema.



Elaborado por: El Autor

Tabla 4: Frecuencia con la que se actualiza el sistema.

	Answer	Count	Percent
1.	Mensualmente	4	33.33%
2.	Semestralmente	4	33.33%
3.	Nunca	4	33.33%
	Total	12	100%
Mean: 2.000		Confidence Interval @ 95%: [1.517 - 2.483]	Standard Deviation: 0.853 Standard Error: 0.246

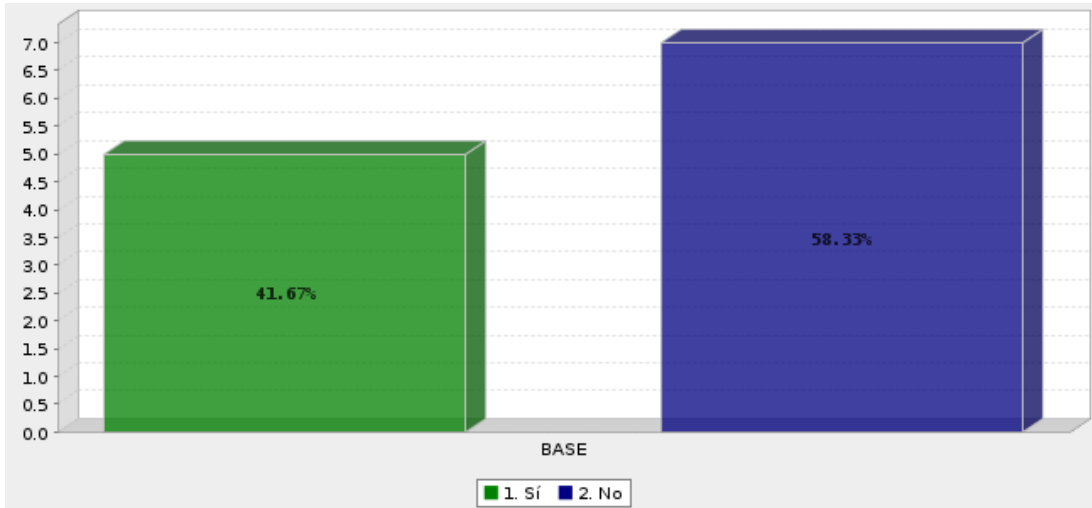
Elaborado por: El Autor

Análisis e Interpretación

Esta pregunta muestra un conflicto en el conocimiento dado que no hay una posición clara en las cifras que arroja la respuesta, se podría decir que hay 4 profesores que creen que el sistema se actualiza o debe cada me, y otros cada seis meses, pero esto se contrapone al tener Windows 7 un sistema que no tiene soporte ni actualizaciones.

Q5. ¿Tiene software antivirus instalado en tu computadora?

Ilustración 5: La máquina tiene antivirus.



Elaborado por: El Autor

Tabla 5: La máquina tiene antivirus.

	Answer	Count	Percent
1.	Sí	5	41.67%
2.	No	7	58.33%
	Total	12	100%
Mean: 1.583	Confidence Interval @ 95%: [1.292 - 1.875]	Standard Deviation: 0.515	Standard Error: 0.149

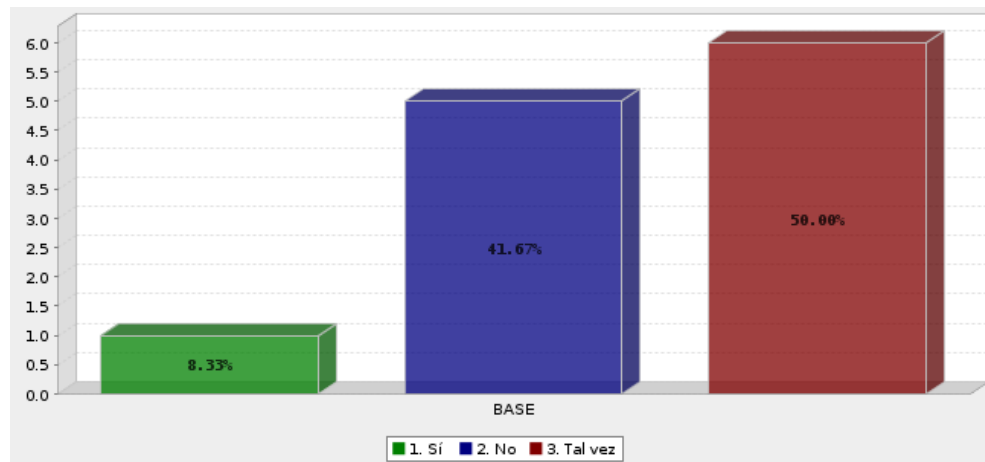
Elaborado por: El Autor

Análisis e Interpretación

El 58.33% indica que el software que posee no es un antivirus lo que mantiene al sistema aún más desprotegido, se encuentra vulnerable a malware, troyanos, virus, etc. Cabe recalcar que son solo los puntos antes descritos es para otorgar un nivel de criticidad alto al sistema que maneja la Unidad Educativa “Eneida Uquillas de Roja”.

Q6. ¿Utilizas un software de firewall en tu ordenador?

Ilustración 6: La máquina posee firewall.



Elaborado por: El Autor

Tabla 6: La máquina posee firewall.

	Answer	Count	Percent
1.	Sí	1	8.33%
2.	No	5	41.67%
3.	Tal vez	6	50.00%
	Total	12	100%
Mean: 2.417	Confidence Interval @ 95%: [2.038 - 2.795]	Standard Deviation: 0.669	Standard Error: 0.193

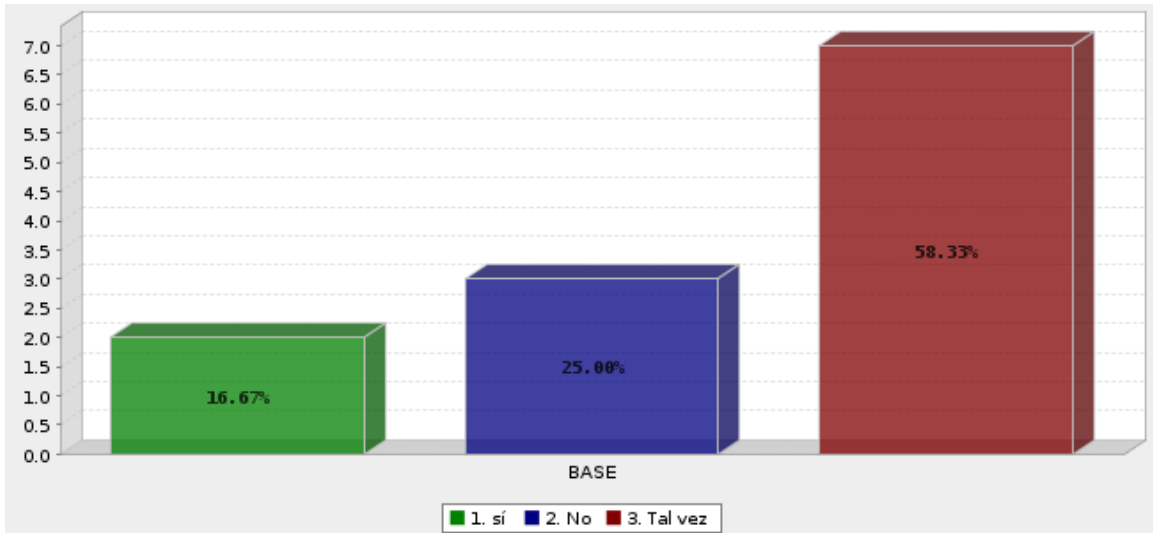
Elaborado por: El Autor

Análisis e Interpretación

El firewall es considerado la primera protección que impide que una gran parte de programas maliciosos infecten el ordenador, es prioridad que todo sistema de información use este corta fuego para minimizar la cantidad de paquetes nocivos que entran en la red.

Q7. ¿La administración está monitoreando tu computadora todo el tiempo?

Ilustración 7: La administración monitorea la computadora.



Elaborado por: El Autor

Tabla 7: La administración monitorea la computadora.

	Answer	Count	Percent
1.	sí	2	16.67%
2.	No	3	25.00%
3.	Tal vez	7	58.33%
	Total	12	100%
Mean: 2.417		Confidence Interval @ 95%: [1.968 - 2.865]	
		Standard Deviation: 0.793	
		Standard Error: 0.229	

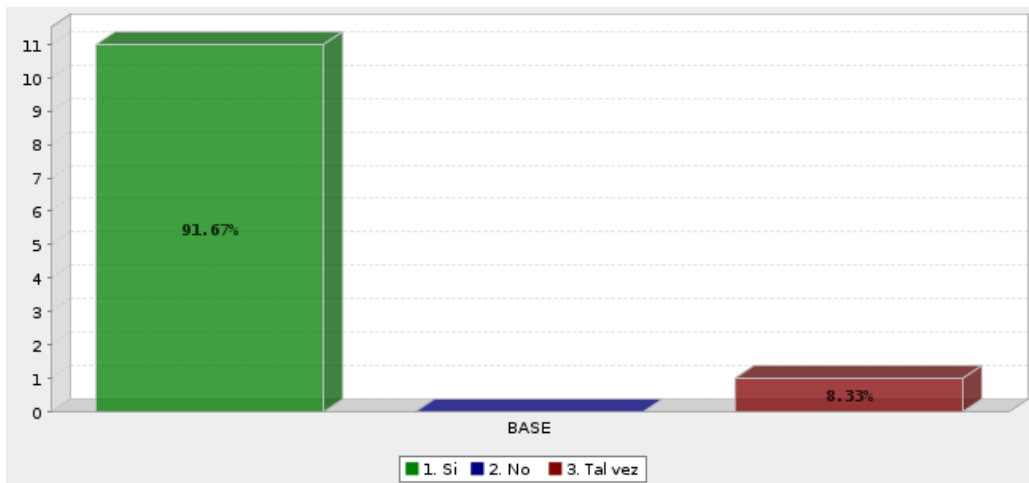
Elaborado por: El Autor

Análisis e Interpretación

Los encuestados están en dudas no saben si existe un control por parte de la administración de la institución, y de momento si no es así es el motivo de que nadie le haya indicado la vida útil que muchas computadoras poseen mucho más en el sistema operativo que es el corazón que maneja todo el hardware.

Q8. ¿Cree usted que le gustaría recibir una asesoría en seguridad de la información?

Ilustración 8: La docencia quiere asesoría en seguridad informática.



Elaborado por: El Autor

Tabla 8: La docencia quiere asesoría en seguridad informática.

	Answer	Count	Percent
1.	Si	11	91.67%
2.	No	0	0.00%
3.	Tal vez	1	8.33%
	Total	12	100%
Mean: 1.167		Confidence Interval @ 95%: [0.840 - 1.493]	
		Standard Deviation: 0.577	
		Standard Error: 0.167	

Elaborado por: El Autor

Análisis e Interpretación

Esta pregunta es para conocer las preferencias de los docentes con respecto a este problema donde el 91.67% está de acuerdo en que se debe concientizar y dar charlas sobre seguridad informática tanto para la seguridad de la información en la escuela como para ellos mismo tener siempre la confianza de que sus equipos están siempre protegidos.

2.6 Discusión de Resultados

Una vez desarrollado la encuesta a los docentes en la Unidad Educativa Eneida Uquillas de Rojas y realizado las observaciones pertinentes al tema de investigación se plantean las siguientes discusiones:

- La Unidad Educativa mediante las observaciones preliminares demuestra serios agujeros de seguridad, al poseer un sistema operativo sin soporte, a esto se le suma que los principales escudos para protección como antivirus, el firewall, analizadores de malware y otras políticas de seguridad son inexistente en la escuela.
- La encuesta arroja un fallo de conocimiento al creer los docentes mediante un 58,33% que un empleado normal puede supervisare y hacer labores de seguridad en vez de un profesional en sistemas o Ti.
- Los docentes mediante la encuesta corroboran en un 66,67% lo que la observación preliminar arrojó, el sistema operativo es un sistema obsoleto Windows 7, y sin soporte por Microsoft, lo que permite que un atacante especializado pueda robar los datos.
- Un 58,33% indica que se usa Chrome en la institución, a pesar que el navegador es seguro ya muestra advertencias al estar en un sistema operativo viejo, y al no tener antivirus como lo indica el 58,33% está todo el sistema expuesto, eso a la suma que no posee firewall muchos paquetes pueden atacar los diferentes servicios que posee la escuela y dañar la integridad de la información.

3. Conclusiones

Una vez elaborado la encuesta y posteriormente obtenida información que se analizó se procede a desarrollar las conclusiones pertinentes del caso de investigación que son presentadas a continuación:

- Se concluye que no hay un personal adecuado que de mantenimiento de software y de sistemas, este personal es un TI, apto para dar seguridad a los equipos de cómputos que existen en la unidad educativa en la que se realizó la posterior evaluación, este personal es importante en la consecución de equipos más seguros.
- Se encontró evidencia que el Windows con el que cuenta la institución es Windows 7, un sistema operativo que ya no tiene soporte y es una coladera hablando en términos informáticos, por lo que esto representa una gran vulnerabilidad en la actualidad, a pesar que el navegador que más usa la institución es Chrome, esto no impide que un atacante pueda sustraer información sensible o dejar inutilizada la institución, por tener sistemas operativos obsoletos.
- No existe política de actualización del software a pesar de contar con un SO inutilizable, es necesario tener metodologías que puedan mitigar un accidente, esto también es fácilmente verificable porque el 58.33% de los encuestados indican que el software que posee no es un antivirus lo que mantiene al sistema aún más desprotegido, se encuentra vulnerable a malware, troyanos, virus, etc.
- No existe firewall por lo que nada impide que una gran parte de programas maliciosos infecten el ordenador, también existe dudas en tener un control por parte de la administración de la institución en estos asuntos informáticos, lo que crea desconcierto y duda en sus empleados.

4. Referencias

- AMBIT. (10 de Noviembre de 2020). *Building Solution Together*. Tipos de Vulnerabilidades y Amenazas informáticas: <https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas>
- Avast. (14 de Julio de 2022). *Avast*. Troyano: <https://www.avast.com/es-es/c-trojan>
- Bco. Santander. (1 de Enero de 2021). *Banco Santander*. ¿Qué es la integridad de los datos?: <https://www.bancosantander.es/glosario/integridad-seguridad-online>
- CEPAL. (18 de Diciembre de 2020). *Nacione Unidas*. Gestión de datos de investigación: <https://biblioguias.cepal.org/c.php?g=495473&p=4398114>
- CISCO. (14 de Julio de 2022). *Cisco*. ¿Qué es la seguridad de red?: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html
- Estruga, N. (28 de Octubre de 2020). *Ealde Bussines School*. CIBERSEGURIDAD Y RIESGOS DIGITALES: <https://www.ealde.es/importancia-seguridad-informatica-empresas/>
- Eulises Ortiz, A. (13 de Julio de 2020). *Hostdime*. ¿Qué es una amenaza informática? ¿Cómo contenerla?: <https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/>
- Gómez, A. (2022). *Auditoría de seguridad informática*. Ediciones de la U. https://books.google.com.ec/books?hl=es&lr=lang_es&id=No5dEAAAQBAJ&oi=fnd&pg=PA41&dq=seguridad+inform%C3%A1tica&ots=RfAM6AJyn4&sig=OfOza28SQg3SdYtLbwDspI_9Aq8&redir_esc=y#v=onepage&q=seguridad%20inform%C3%A1tica&f=false
- INTEL. (14 de Junio de 2022). *Intel*. Funciones de seguridad de hardware para ordenadores de empresa: <https://www.intel.es/content/www/es/es/business/enterprise-computers/resources/hardware-security-features.html>
- Karsperky . (14 de Julio de 2022). *Karsperky*. ¿Qué son los ataques DDoS?: <https://latam.kaspersky.com/resource-center/threats/ddos-attacks>
- Malwarebytes. (14 de Julio de 2022). *Malwarebytes*. Spyware: <https://es.malwarebytes.com/spyware>
- Matachana, Y. L. (2020). *Los virus informáticos: una amenaza para la sociedad*. Editorial Universitaria (Cuba).
- Oracle. (14 de Julio de 2022). *Oracle*. ¿Qué es el malware?: <https://www.oracle.com/es/database/security/que-es-el-malware.html>

- OSI. (6 de Febrero de 2019). *Oficina de Seguridad del Internauta* . ¿Sabías que el 90% de las contraseñas son vulnerables?: <https://www.osi.es/es/actualidad/blog/2019/02/06/sabias-que-el-90-de-las-contrasenas-son-vulnerables>
- Red Seguridad . (12 de Julio de 2021). *Red Seguridad* . ‘Rootkit’: definición, tipos y protección ante este ‘malware’: https://www.redseguridad.com/actualidad/cibercrimen/rootkit-definicion-tipos-y-proteccion-ante-este-malware_20210712.html
- Tibor , M. (1 de Enero de 2020). *Software Lab*. ¿Qué es una vulnerabilidad informática? La definición y ejemplos: <https://softwarelab.org/es/que-es-una-vulnerabilidad-informatica/>
- Torres López, N. I. (2022). *Estudio comparativo de tecnologías de la seguridad informática phishing y spoofing para la detección de un ataque informático*. Bachelor's thesis, Babahoyo: UTB-FAFI. 2022.
- UNIR. (15 de Junio de 2021). *Universidad de Internet*. ¿Qué es la seguridad informática y cuáles son sus tipos?: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>
- UNIR. (15 de Junio de 2021). *Universidad del Internet*. ¿Qué es la seguridad informática y cuáles son sus tipos?: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>

5. Anexos

Análisis Técnico De La Seguridad En Los Sistemas Informáticos

De La Unidad Educativa Eneida Uquillas De Rojas.

Técnica: Encuesta

Instrumento: Cuestionario

Cargo laboral: Docentes/administrativos

Nombre:

¿Quién es responsable de instalar y mantener el software de seguridad en sus computadoras?

1. Empleados
2. Personal TI

2. ¿Qué versión de Windows está instalada en el equipo que normalmente usas para conectarte a Internet en la institución?

1. Windows 7
2. Windows 8
3. Windows 10
4. Windows 11
5. IOS
6. Linux

3. ¿Qué navegador web utilizas normalmente?

1. Firefox
2. Brave
3. Chrome
4. Edge

4. ¿Con qué frecuencia utilizas actualiza sus sistemas?

1. Mensualmente
2. Semestralmente
3. Nunca

5. ¿Tiene software antivirus instalado en tu computadora?

1. Sí
2. No

6. ¿Utilizas un software de firewall en tu ordenador?

1. Sí
2. No
3. Tal vez

7. ¿La administración está monitoreando tu computadora todo el tiempo?

1. sí
2. No
3. Tal vez

8. ¿Cree usted que le gustaría recibir una asesoría en seguridad de la información?

1. Si
2. No
3. Tal vez



UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, 30 de junio de 2022
D-FAFI-UTB-0311-2022

Lcda.

Mercedes Agustina Julio Macias

DIRECTORA DE LA UNIDAD EDUCATIVA ENEIDA UQUILLAS DE ROJAS

La Teresa.-

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El Señor **CASTILLO LEON EDDER SANTIAGO**, con cédula de identidad No. 120749138-0, Estudiante de la Carrera de Ingeniería en Sistemas, matriculado en el proceso de titulación en el periodo Abril 2022 – Septiembre 2022, trabajo de titulación modalidad Caso de Estudio, previo a la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS** solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar el Caso de Estudio en la institución de su digna dirección, el cual titula: **ANÁLISIS TÉCNICO DE LA SEGURIDAD EN LOS SISTEMAS INFORMATICOS DE LA UNIDAD EDUCATIVA ENEIDA UQUILLAS DE ROJAS.**

De la señora directora,

Atentamente.


Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO



C/c: Archivo

Realizado

Mercedes Julio M.



Babahoyo, 30 de junio del 2022

Magister

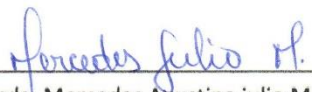
Eduardo Galeas Guijarro

**DECANO DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E
INFORMÁTICA**

De mis consideraciones:

Por medio de la presente autorizo que el Sr. **CASTILLO LEON EDDER SANTIAGO** con cédula de identidad **120749138-0**, estudiante de la carrera de **INGENIERÍA EN SISTEMAS** realice el estudio de caso en la **UNIDAD EDUCATIVA ENEIDA UQUILLAS DE ROJAS** ubicada en Babahoyo – La Teresa, previa a la obtención del título universitario de tercer nivel como **INGENIERO EN SISTEMAS**. El estudio de caso es: **ANÁLISIS TÉCNICO DE LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA UNIDAD EDUCATIVA ENEIDA UQUILLAS ROJAS.**

Atentamente.


Lcda. Mercedes Agustina julio Macias
(Rectora de la Unidad Educativa)





Babahoyo, 12 de agosto del 2022

**CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES
EN EL SISTEMA DE ANTIPLAGIO**

En mi calidad de Tutor del Trabajo de la Investigación del Sr. **CASTILLO LEON EDDER SANTIAGO**, cuyo tema es: **ANÁLISIS TÉCNICO DE LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA UNIDAD EDUCATIVA ENEIDA UQUILLAS DE ROJAS**, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de [**8%**], resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.

The screenshot shows the 'CERTIFICADO DE ANÁLISIS' from the 'compilatio' system. The title is 'CASO EDDER CASTILLO'. The main result is '8% Similitudes'. A breakdown of the similarity includes: '< 1% Texto entre comillas', '1% similitudes entre comillas', and '2% Idioma no reconocido'. Metadata includes: 'Nombre del documento: CASO EDDER CASTILLO LEON.docx', 'Depositante: EDDER CASTILLO', 'Fecha de depósito: 4/8/2022', 'Tamaño del documento original: 34 ko', 'Tipo de carga: url_submission', 'Autor: EDDER CASTILLO', 'Número de palabras: 4726', and 'Número de caracteres: 30.970'.

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

ING. LEÓN ACURIO JOFFRE VICENTE.
DOCENTE DE LA FAFI.