UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y La Comunicación (TIC)
Autor:
Guido Alexander Valencia Lomas
Tutor:
Mg. Pablo Recalde

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo Recalde con C.I: 17116850555 en mi calidad de Tutor del proyecto de investigación titulado: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005.

Elaborado por: Guido Alexander Valencia Lomas, de cédula de identidad: 1002177481, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**,, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

Firma

ORCID: 0000-0001-7256-2836

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Guido Alexander Valencia Lomas con cédula de identidad número 1002177481, autor del proyecto de titulación denominado: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
GUIDO ALEXANDER
VALENCIA LOMAS

_____

Firma
Orcid: 0009-0001-7790-3983

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Es crucial salvaguardar la ciberseguridad en el sector educativo, sobre todo cuando se utilizan plataformas tecnológicas para tareas como la calificación y los procedimientos de enseñanza-aprendizaje.

Contextualización

La utilización de Internet para este fin, ayuda a que se desplieguen proyectos de protección en la información que certifiquen la totalidad, disponibilidad y accesibilidad de la información en las Unidades Educativas existe un escaso manejo y resguardo de la integridad de la información y existen patrones de comportamiento que la ponen en riesgo.

Las políticas de seguridad informática son un conjunto de normas y directrices que garantizan la confidencialidad, integridad y disponibilidad de la información, minimizando los riesgos que la afectan. (Kats, 2021)

Para poner en marcha una estrategia de protección de datos, debe realizarse un estudio preliminar de las vulnerabilidades existentes. Este estudio también debe supervisar todos los procesos, el software y el comportamiento dentro de la comunidad educativa. Es igualmente importante que la estrategia sea autorizada por el personal administrativo. En el mundo digital actual, en el que la mayoría de las empresas, hogares e instituciones están interconectados, es crucial proteger la información que generan.

Este análisis compara diferentes sniffers para evaluar las vulnerabilidades en un estudio de caso del centro educativo Unidad Educativa Víctor Mideros Almeida. Los resultados sirven de base para proponer mejoras en la seguridad de otras instituciones educativas bajo el mismo sistema. El proyecto se apega a las normas ISO 27002 y 27005 y analizó las leyes y reglamentos que garantizan la confiabilidad de los datos.

Según Cedeño (2022) es bastante común en Ecuador que las instituciones educativas se enfrenten a problemas de seguridad, por lo que esta propuesta de investigación tiene una importancia significativa. Mediante la adhesión a las normas ISO 27002 para las mejores prácticas de seguridad e ISO 27005 para la gestión de riesgos, se pretende abordar este problema con eficacia.

La investigación reúne los datos necesarios para crear estrategias pertinentes al contexto de la Unidad Educativa Víctor Mideros Almeida, que cuenta con recursos limitados por ser una institución pública.

NORMA ISO 27002: Bloque 5: Reglas de Seguridad en los datos

Es crucial elaborar una guía que describa las reglas de seguridad de los datos en la organización, que tenga principios de seguridad en la información, una agrupación de metas y medidas de seguimiento.

Bloque 6 - Estructura de la Seguridad en los datos

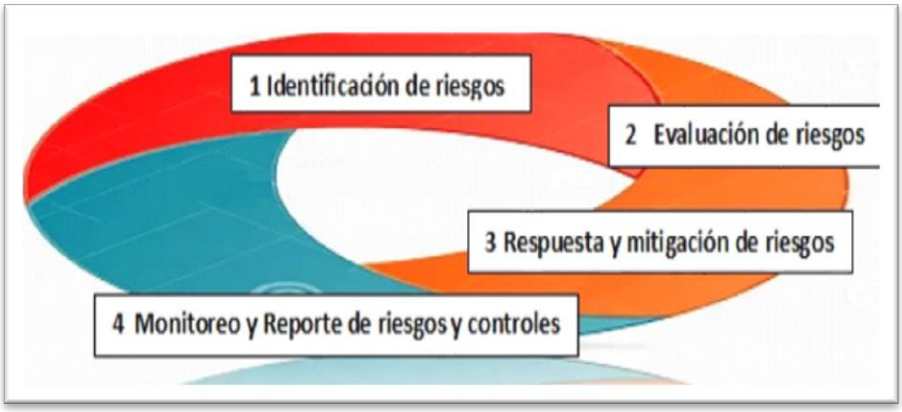
Implantar eficazmente la seguridad en los datos de una organización, es imprescindible instaurar una estructura que la gestione apropiadamente. Esto implica coordinar las acciones de seguridad en los datos a través de representantes designados dentro de la organización que tengan responsabilidades bien definidas, incluida la protección de la información confidencial.

Bloque 7 - Gestión de activos

Según la norma, un activo es cualquier cosa de valor para la organización que necesite protección. Para ello, los activos deben identificarse y clasificarse, lo que permite crear y mantener un inventario. Además, deben cumplir unas normas documentadas que definan el uso permitido de dichos activos. (Chicano, 2023)

Figura 1

ISO 27005 para la administración de riesgos.



Nota. Basado en ISO 27005

La obtención de la certificación ISO/IEC 27005 dotará de la experiencia y los aprendizajes imprescindibles para comenzar la implantación de una forma de gestión de vulnerabilidades para el resguardo de los datos. Esta certificación demuestra tu capacidad para encontrar, identificar, estudiar, validar y abordar diferentes fallos para la gestión de los datos a los que se afrontan las entidades. Además, te capacita para apoyar a las entidades priorizando los riesgos y tomando las medidas adecuadas para reducirlos y mitigarlos. (Chicano, 2023)

Figura 2

ISO 27002 buenas prácticas de seguridad.

Nota. Basado en ISO 27002

La finalidad de las reglas de seguridad informática es dar a los miembros de la institución de la misma manera que a usuarios que ingresan a sus recursos tecnológicos, las exigencias y reglas de acción precisas para resguardarlos. Así mismo estas estrategias son eficaces el momento de auditar los procesos de gestión en la información de una institución pública.

Problema de investigación

De las normas en protección de datos en esta unidad educativa son básicas o inexistentes. Se enfrentan a un problema constante con su información en el archivo, ya que tienen documentación tanto física como digital a la que se puede acceder fácilmente y que se puede perder. La unidad ha sufrido varios incidentes de alumnos de la misma unidad educativa que han accedido al sistema de calificaciones y frecuentes pirateos de Internet por parte de alumnos actuales y antiguos.

Los profesores no conocen las estrategias y normas para proteger la información y creen que es responsabilidad exclusiva del profesor encargado de la tecnología. Además, la mayoría de los profesores han sufrido algún tipo de fraude cibernético, lo que supone un mayor riesgo para la fiabilidad de la información. (García, 2019)

El presupuesto asignado a la ciberseguridad es casi inexistente, ya que depende del gobierno, por lo que se necesitan soluciones creativas en este aspecto. Como los servidores son compartidos, no hay presupuesto para uno dedicado, lo que significa que, si otra unidad educativa se infecta, puede contaminar al resto. Se tienen copias de seguridad en Onedrive, y el sitio web está alojado en Siteground, una plataforma de alojamiento web diseñada para un alto rendimiento, mientras que el dominio está en AWS Amazon Web Services. La dirección IP es pública, y las contraseñas se almacenan en un archivo Excel compartido en Google Drive, al que pueden acceder tanto las autoridades como los profesores que tienen acceso a la red Wi-Fi de la Unidad. Esto lleva a una pregunta básica.

¿Qué métodos pueden ayudar a minimizar el nivel de vulnerabilidad de los datos en las Unidades Educativas?

Objetivo general

Comparar métodos de mitigación de la vulnerabilidad vía sniffer, que pueden aplicarse a la Unidad Educativa Víctor Mideros Almeida según las normas ISO 27002 y 27005.

Objetivos específicos

- Reconocer los métodos utilizados para el hackeo de información y el objetivo que persiguen los ataques informáticos en Instituciones de Educación.
- Contextualizar los fundamentos teóricos sobre metodologías sobre sniffers como Wireshark, Ettercap y Nmap.

- Desarrollar estrategias que permitan el control de fugas de información en la Unidad Educativa Víctor Mideros Almeida.
- Identificar el impacto del uso de las actividades sobre la vulnerabilidad de la información en el sistema Webprosistem.

Vinculación con la sociedad y beneficiarios directos:

Los beneficiarios directos de este proyecto de titulación será la comunidad educativa de la Unidad Víctor Mideros Almeida, ya que al generar este documento se proveerá de una serie de estrategias que ayudarán a un mejor manejo de la información.

Además, contribuirá a alcanzar el objetivo de desarrollo sostenible 4, que pide "garantizar una educación de calidad inclusiva y equitativa y promover oportunidades de aprendizaje permanente para todos". (ONU, 2023) al tener una metodología clara para monitoreo de vulnerabilidades en la Unidad Educativa estamos garantizando una educación de calidad ya que sus trabajos y notas serán salvaguardados de ataques cibernéticos.

Adicionalmente, si se tienen en cuenta las sugerencias realizadas sobre registros, alumnos y profesores podrán disfrutar de un sistema educativo más fiable, rápido y seguro.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Se ha producido un avance significativo de la tecnología en el campo de la educación. Sin embargo, con este progreso, el riesgo de robo de información y el acceso ilimitado a los recursos se ha convertido en algo habitual.

1.1. Contextualización general del estado del arte

Los últimos años, las tecnologías de la información y las comunicaciones se han desarrollado rápidamente, beneficiando a las personas, pero también han evolucionado los métodos ilícitos frente al robo de información.

Según Pereira (2019) el objetivo de explicar la Ciberseguridad en un lenguaje sencillo es concienciar y educar individuos sobre la manera de aumentar su protección y confianza cuando utilizan cualquiera de sus equipos tecnológicos.

Cuando navegan en la web, utilizando su email, adquiriendo compras en línea o accediendo a plataformas educativas, es importante comprender las vulnerabilidades y los riesgos asociados a tales actividades. Esta aportación ha hecho reflexionar sobre lo vulnerables que somos al entregar trabajos o registrar calificaciones en la plataforma de la Unidad Educativa.

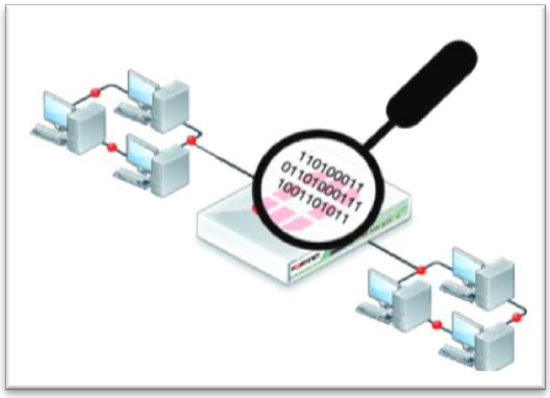
Según Kats(2021), este afirma que el mayor problema está relacionado con los colaboradores descuidados o negligentes que no sólo utilizan redes y dispositivos domésticos potencialmente inseguros, sino que también realizan prácticas de riesgo como hacer clic en enlaces desconocidos, crear contraseñas débiles y caer en tácticas de ingeniería social. Esto les hace vulnerables a las ciberamenazas y crea una importante oportunidad para los actores maliciosos que buscan explotar estos malos hábitos en las organizaciones.

En este sentido, es claro que, para encontrar vulnerabilidades como puertos abiertos, es necesario recurrir a Sniffers como Wireshark, Nmap y Ettercap que ayudan a entender las vulnerabilidades de la red de cualquier organización.

Ahora bien, un sniffer es una herramienta o programa informático que puede interceptar datos o información que circulan por una red a la que no está necesariamente destinado, accediendo así a información a la que no debería tener acceso. (Limachi, 2018, p.10)

Figura 3

Esquema de sniffer actuando



Nota. Basado en Internet

1.2. Proceso investigativo metodológico

Esta investigación se basa en los siguientes fundamentos definidos como:

Investigación Bibliográfica

La investigación bibliográfica es cuando se recopila información sobre un tema a partir de libros, artículos y otras fuentes escritas. El objetivo es organizar el conocimiento y conocer las ideas principales sobre ese tema. Existen diferentes nombres para este tipo de investigación, como gabinete, biblioteca o investigación documental. (Méndez, 2018, p.14)

Este documento ha aplicado la investigación bibliográfica para la búsqueda de información, utilizando fuentes confiables sustentando temáticas desarrolladas, la información recopilada fue obtenida de repositorios académicos verificados y constan de fuentes confiables que han apoyado con conocimientos fundamentales para la elaboración de buenos resultados.

Métodos, técnicas e instrumentos

En este trabajo se utilizó la herramienta encuesta que se aplicará a la comunidad educativa Miderista que son alumnos, profesores y administrativos.

Enfoque de la investigación

El enfoque utilizado para este proyecto será un enfoque comparativo, además, mediante una encuesta se identificará los principales métodos de control y acceso a su sistema Webprosistem.

Instrumentos y Técnicas de recolección de datos

Técnicamente y basado en los instrumentos aplicados se han considerado y utilizado en este proceso investigativo para la recopilación de información lo que se muestra a continuación:

Tabla 1

Instrumentos y Técnicas.

Técnica	**Instrumento**	**Aplicar en**
Análisis de documentos	Fuentes bibliográficas	Comparativa de instituciones/procesos
Entrevista	Guía de entrevista	Personas clave de los procesos

Nota: Teoría clásica de técnicas e instrumentos de investigación.

El «Análisis de documentos» es una técnica de investigación utilizada para examinar y analizar documentos escritos, textos, informes, archivos y otros tipos de materiales escritos con el objetivo de obtener información y comprender temas específicos». (Krippendorff, 2019)

«La entrevista es una conversación planificada entre el investigador y el entrevistado para obtener información. Su uso constituye un medio para el conocimiento cualitativo de los fenómenos» (León, 2012)

1.3. Análisis de resultados

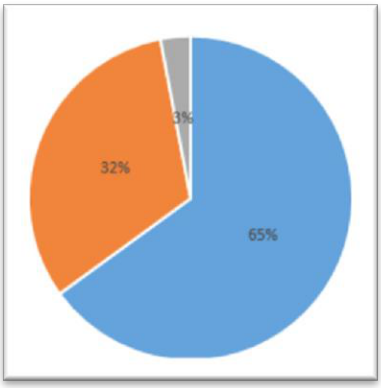
Se ha realizado una encuesta a la comunidad educativa (personal administrativo, docentes y estudiantes a la que beneficia este trabajo obteniendo los siguientes resultados: Este análisis es un resumen de toda la información que se recopilo en la investigación que se muestra prometedora para su implementación general.

Algunos de los resultados de las encuestas se presentan aquí:

Pregunta 1. ¿Cree usted que tiene alguna responsabilidad en la ciberseguridad de la Institución?

Figura 4

Responsabilidad de la ciberseguridad.



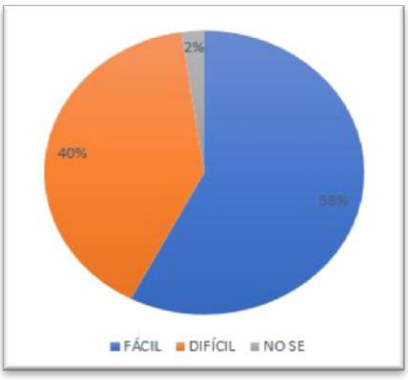
Nota. Basado en la encuesta

La respuesta muestra que el 65% señalaron que no tienen responsabilidad, un 32% señaló que Si y un 3% no sabe que responder; se puede decir que la mayoría no son conscientes de su participación.

Pregunta 2. ¿Qué nivel de dificultad tiene Ud. para averiguar la clave del internet?

Figura 5

Nivel de dificultada.



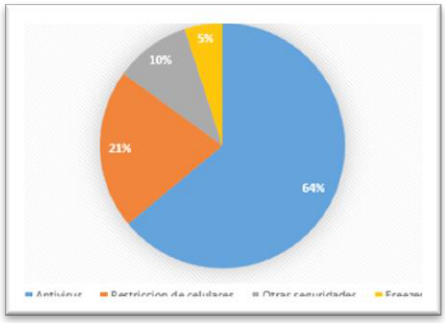
Nota. Basado en la encuesta.

El 58% señalaron que es fácil la contraseña, un 40% señalaron que es difícil y un 2% no sabe que responder; se puede decir que a pesar de que la clave del laboratorio se cambia cada 15 días para ellos no es problema encontrarla.

Pregunta 3. ¿Qué tipo de seguridades ha visto en la Unidad Educativa con respecto a la información?

Figura 6

Tipos de seguridad.



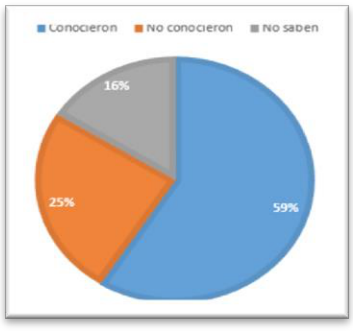
Nota. Basado en la encuesta.

El resultado muestra que el 64% señalaron que los antivirus son la mayor seguridad que han visto, un 21% señalaron que es la restricción de celulares, un 10% señaló que hay otras seguridades y un 5% señala que los freezer.

Pregunta 4. ¿Ha conocido Ud. ¿Algún incidente dónde se hayan adulterado notas en el sistema académico Webprosistem de la Unidad Educativa?

Figura 7

Incidentes en Webprosistem.



Nota. Basado en la encuesta.

Los resultados señalan que el 59% si han conocido incidentes de adulteración de notas, un 25% señalaron que no conocen y un 16% no lo saben.

CAPÍTULO II: PROPUESTA

La propuesta pretende mitigar varias vulnerabilidades que se dan en la plataforma educativa de la Unidad Víctor Mideros Almeida, empleando los mejores sniffers.

2.1. Fundamentos teóricos aplicados

ESTRUCTURA DE LA NORMA ISO 27001

La norma comienza delineando algunas pautas para su uso, intención y método de aplicación.

Referencias: A los efectos de aplicar la norma ISO 27001, se recomienda que los usuarios consulten algunos documentos clave.

En su contexto organizacional este es el primer requisito del estándar e incluye detalles sobre cómo determinar el alcance del SGSI y cómo comprender cómo encaja la organización en su entorno.

Como referencias normativas recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO 27001.

Figura 8

Norma ISO 27001.

PARAMETRO	DETALLE
Contexto de la organization:	Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.
Liderazgo:	Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
Planificación:	Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.
Soporte:	En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.

Nota. Parámetros de la norma ISO 27001

LEY ORGÁNICA DE TELECOMUNICACIONES

El sistema educativo Webprosistem por medio de su administrador está sujeto a la ley Orgánica de Comunicaciones que protegen los datos de los estudiantes, docentes, padres de

Figura 9

Protección de los datos personales.

Artículo 78.- Derecho a la intimidad. Para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley. Dichas medidas incluirán, como mínimo:

1. La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley.

2. La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.

3. La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

4. La garantía de que la información suministrada por los clientes, abonados o usuarios no será utilizada para fines comerciales ni de publicidad, ni para cualquier otro fin, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario. El consentimiento deberá constar registrado de forma clara, de tal manera que se prohíbe la utilización de cualquier estrategia que induzca al error para la emisión de dicho consentimiento. ›› (Ley Orgánica de Telecomunicaciones, 2016, p.24)

Nota. La figura fue extraída de la Ley Orgánica de telecomunicaciones

2.2. Descripción de la propuesta

En primer lugar, se realizó un levantamiento de la situación actual de las Unidades Educativas referente a la normativa que poseen para el manejo y resguardo de la información y los patrones de comportamiento que la ponen en riesgo, luego se estudió a la Unidad Educativa Víctor Mideros Almeida y su manejo de la información. Finalmente se aplicó el uso de sniffers como Wireshark, Ettercap y Nmap para comparar su efectividad al momento de encontrar vulnerabilidades.

El resultado de este proceso proporcionó los fundamentos para poder realizar el análisis de las políticas que se necesitan para la propuesta en la Institución. Se realizó un análisis de riesgos, amenazas y vulnerabilidades a los que están expuestos los datos que se acceden a través de los dispositivos que se conectan a las redes, en donde se obtuvieron puntos clave para la creación de las políticas de seguridad, se analiza patrones de seguridad de los directivos, docentes, estudiantes y sus comportamientos de navegación a través de los routers o switches.

a. Estructura general

En el análisis de los parámetros necesarios para la seguridad de datos se realiza una tabla comparativa entre características de cada sniffer, sus ventajas y desventajas para una optimización del análisis.

Figura 8

Comparativa de Ventajas y Desventajas entre los Sniffers.

SNIFFER	VENTAJAS	DESVENTAJAS
NMap	Herramienta utilizada descubrimiento de seguridad. Este programa y la versión gráfica tiene mucho potencial, lo que dificulta ser perjudicados en la web. Analiza el rango de puertos deseado y revela sus movimientos, como consecuencia impide que el intruso pueda ingresar al dispositivo remoto.	Mientras mayor complejidad tenga la clase de escaneo que se requiere ejecutar, el escaneo suele ser demorado y tomar minutos antes de concluir, la rapidez del análisis de basa esencialmente en 3 factores, rapidez del equipo del intruso, latencia en la red dependiendo de su velocidad, y el tiempo de respuesta además de las políticas de seguridad de la computadora escaneada del perjudicado.
WIRESHARK	Analizador de protocolos open source que actualmente está disponible para plataformas Windows y Unix. Wireshark como analizador de redes que le brinda una vista microscópica de lo que sucede dentro de los paquetes de red y proporciona información detallada sobre paquetes individualizados. Se sigue actualizando frecuencia. Esto no incluye funcionalidades, si también recibe parches de seguridad.	Cuanto más complejo sea el tipo de análisis que intenta ejecutar, más tiempo llevará el proceso de análisis, que puede tardar varios minutos en completarse. La velocidad de escaneo depende básicamente de los 3 factores.
ETTERCAP	Ettercap es un rastreador/interceptor/registrador de redes LAN de switchs que admite el análisis activo y pasivo de muchos protocolos (incluidos los cifrados) y tiene muchas funciones para el análisis de hosts y redes. Admite direcciones activas y pasivas para varios protocolos, incluidos protocolos cifrados como SSH y HTTPS. Interceptar tráfico remoto a través de túneles GRE: conectarse a un enrutador Cisco, a través de un túnel GRE puede interceptar el tráfico y lanzar ataques de intermediario.	Existen también los rpm, pero no te los recomiendo, porque no traen todos los plugins que trae el archivo tar. No trae actualizaciones. Debe estar en la misma red para que Funcione correctamente

Nota. Basado en análisis propios

b. Explicación del aporte

Para desarrollar esta propuesta se realizaron varios pasos, los cuales incluyen la observación, la entrevista a grupos específicos de interés, la investigación bibliográfica, la comparativa. Y se establecen los siguientes aportes. Se establece que se deben cumplir: NORMAS PARA EL RESGUARDO DE LA INFORMACIÓN DE ARCHIVO

- ✓ No compartir claves con personal no autorizado
- ✓ Acceso restringido al lugar de archivo.
- ✓ Escaneo de documentos físicos para mantener un archivo digital.
- ✓ Mantener el lugar ventilado para evitar el deterioro de los documentos.
- ✓ Crear un documento donde se clasifique cada proceso de resguardo de la información y se clasifique la información por grado de sensibilidad.

Se establece que se deben cumplir: NORMAS PARA EL PERSONAL DOCENTE Y AUTORIDADES

- ✓ Capacitación sobre los riesgos y vulnerabilidades a las que son expuestos en donde se haga hincapié en los siguientes temas:
  - Phishing
  - Actualización de claves en las plataformas educativas Ingeniería social.

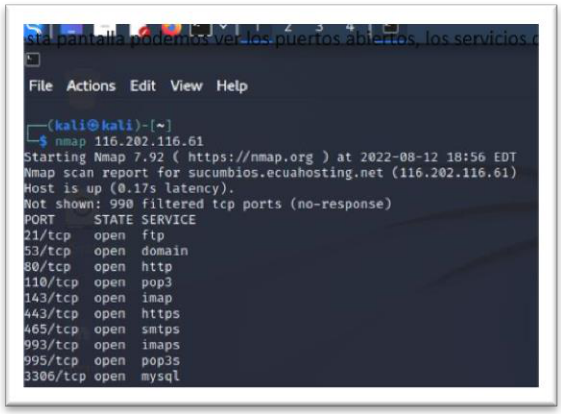
c. Estrategias o técnicas

A continuación, la revisión de modelos o técnicas empleadas revisar la viabilidad de la implementación de la propuesta.

Mediante el uso de los sniffer analizados, se establecen puertos en los que es muy fácil vulnerarlos y de esa forma entrar en la red de forma ilícita.

Figura 9

NMap al site webprosistem.com.

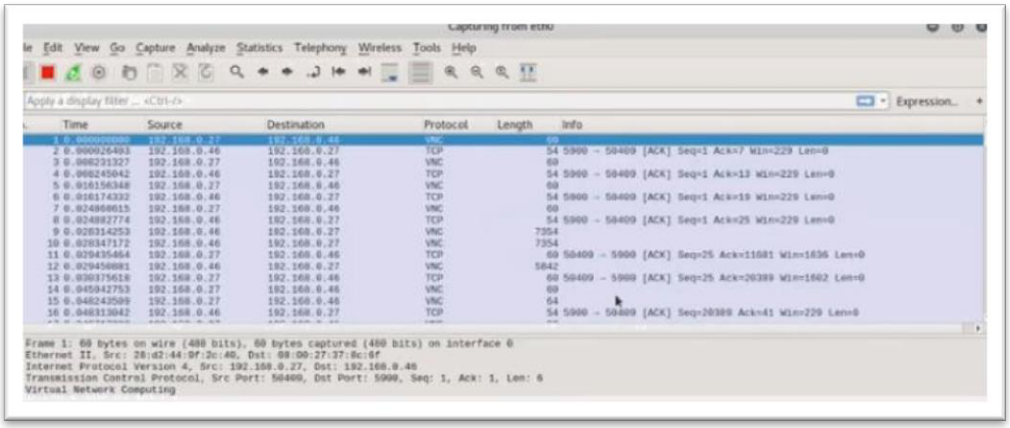


Nota. Se obtiene puertos de servicios a proteger

Para analizar posibles ataques de *man in the midle*, se usa Wireshark.

Figura 10

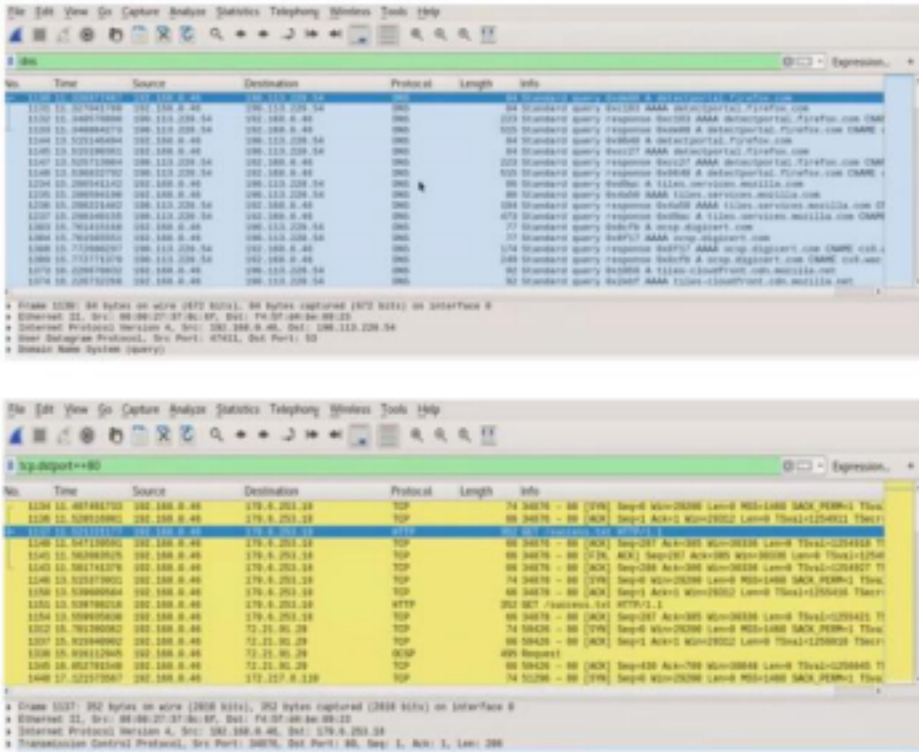
Análisis de interceptación.



Nota. Se obtiene indicios de Hackeo sobre los puertos anteriores

Figura 11

Filtrados de DNS y Web.

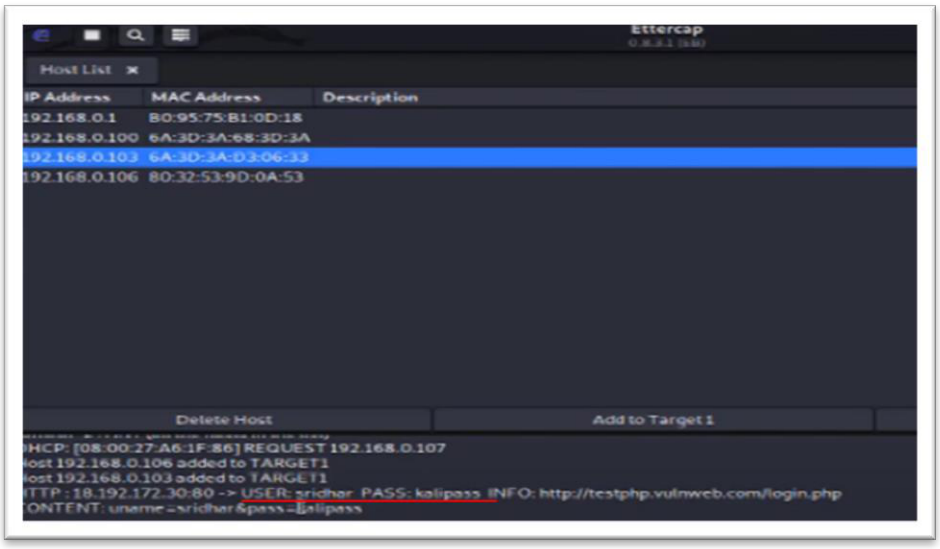


Nota. Captura de filtrados para defensa del site.

Para confirmar el proceso de usuario contraseña, mediante ettercap.

Figura 12

Uso de Ettercap para texto no cifrado.



Nota. Captura de texto no cifrado, para confirmar el uso de herramientas de cifrado del site.

2.3. Valoración de la propuesta

Se presentan documentos de responsables de áreas que por su trabajo manejan varios procesos y que pueden valorar el impacto del trabajo. (Ver anexos)

Se validará la propuesta a través del método de criterios del especialista:

Tabla 3

Especialistas que valoran este trabajo.

ESPECIALISTA	PUESTO	EMPRESA
Msc. Juan Carlos Figueroa	Coordinador TICs	Distrito de Educación Zona 1
Msc. Cristina Cervantes	Coordinador del Área de Informática	U.E. Vítor Mideros Almeida
Msc. Edwin Pilataxi	Miembro del departamento de TICs	Distrito de Educación Zona 1

Nota. Personas que han analizado el trabajo y dan su criterio.

A decir de los especialistas que valoraron este trabajo, es adecuado y da pistas de cómo debe protegerse la Unidad Educativa.

2.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 4

Matriz de articulación.

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Estándares y políticas de seguridad de la información.	Es un estándar que permite la seguridad, confidencialidad e integridad de los datos y la información y los sistemas que los procesan. Se basa principalmente en la identificación y el análisis. delas principales amenazas de Seguridad de la Información.	El método de investigación fue bibliográfico y me permitió desarrollar conceptos sobre una variedad de estrategias.	Fuentes bibliográficas	Características de seguridad que debe poseer un laboratorio de computación.	Libros digitales, artículos
Protocolos de red y uso	Wireshark es un analizador de protocolos open source que actualmente está disponible para plataformas Windows y Unix.	Protocolos y manejo de paquetes de red	Fuentes bibliográficas y Experimentación	Puertos bloqueados y sugerencias de protección de datos al sistema y red.	Analizador de protocolos.

Nota. Análisis detallado de cada sniffer

CONCLUSIONES

Se han encontrado varios conceptos en la línea de investigación de Sistemas de Información, del manejo de procesos y métodos de mitigación en vulnerabilidades vía sniffers, que pueden aplicarse en Unidades educativas según las normas ISO 27002 y 27005.

En la mayoría de instituciones de educación media que mantienen sus plataformas educativas disponibles al público, no se ha identificado una metodología clara que permita proteger la información de estudiantes, docentes, padres de familia, personal administrativo y de servicio; se concluye que esto se debe a la falta de conocimiento de los riesgos informáticos a los que están expuestos.

La Unidad educativa Víctor Mideros Almeida maneja de forma empírica los procesos, tanto para la secretaría como para el área académica y que se entrelazan para entregar solamente resultados.

Por simplicidad se pudo presentar propuestas de procesos generales basadas en el uso de Sniffers como Wireshark, Ettercap y Nmap, no obstante, deben ser desarrollados por profesionales del área de Tics en las Instituciones educativas, para su implementación.

La valoración de expertos de este tipo de procesos, indican la aceptación del uso de Sniffers en el control de tráfico de la red educativa, pero señalan que la implementación debe ser progresiva y que se capacite a la comunidad educativa sobre el tema, principalmente de aquellas que no están actualizadas con el uso de la tecnología.

El desconocimiento de estas herramientas puede llevar a prácticas inseguras que expongan la red y los datos sensibles a amenazas de seguridad. Los estudiantes y el personal pueden no ser conscientes de los riesgos asociados con la fuga de información, lo que podría resultar en la exposición de información confidencial o en la manipulación de la red.

RECOMENDACIONES

- Ofrecer capacitación a docentes, personal de Tics y personal administrativo sobre cómo utilizar los Sniffers de manera efectiva.
- Establecer métricas para evaluar el impacto de la utilización de Sniffers y reglas de seguridad en las Unidades Educativas y realizar evaluaciones periódicas.
- Escuchar la retroalimentación de estudiantes, docentes y administrativos para realizar mejoras continuas en la implementación de metodologías para la mitigación de vulnerabilidades.
- Dialogar con expertos en el área informática y de educación para orientar la implementación y aprovechar las mejores prácticas.
- Comunicar los avances y logros en la implementación de normas de uso de laboratorios y áreas compartidas tanto dentro como fuera de las unidades educativas para atraer estudiantes y fortalecer la reputación.
- Establece claramente los límites sobre qué está permitido y qué no lo está al utilizar analizadores de red. Evita que los estudiantes utilicen estas herramientas con fines maliciosos.
- Antes de llevar a cabo cualquier actividad de análisis de red, asegurarse de obtener el consentimiento explícito de todas las partes involucradas, incluidos los estudiantes, el personal y los administradores de la red.
- Evitar capturas o analizar información de tráfico que pueda contener datos sensibles o privados, como contraseñas o información personal.
- Supervisa de cerca las actividades de los estudiantes que involucren el uso de estas herramientas para garantizar que se adhieran a las políticas establecidas y no causen daño a la red ni a otros usuarios.
- Recuerda que el uso de analizadores de red y sniffers debe ser coherente con las políticas y regulaciones locales, y siempre debe enfocarse en fines educativos legítimos. La seguridad y la privacidad deben ser prioritarias en cualquier actividad relacionada con la seguridad informática en una unidad educativa.

BIBLIOGRAFÍA

Abad Parrales, W. M., Cañarte Rodríguez, T. C., Villamarín Cevallos, M. E., Mezones Santana, H. L., Delgado Pilozo, Á. R., Toala Arias, F. J., Figueroa Suárez, J. A., & Romero Castro, V. F. (2019). *La ciberseguridad práctica aplicada a las redes, servidores y navegadores web*. Editorial Científica 3Ciencias.

Aldaz, W. (2019). VULNERABILIDADES DE SEGURIDAD INFORMÁTICA EN LA ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO" A TRAVÉS DEL PHISHING. Universidad Tecnológica Israel.

Armijo, V., & Alexander, E. (2022). *Análisis de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador*. Universidad Católica de Santiago de Guayaquil.

Canfranc, P. R. (2019). *Ciberseguridad: Protegiendo la información vulnerable*. Fundación Telefónica.

Carrión Jumbo, I., Luis, J., Luis, P., & Vivanco, J. (s/f). Edu.ec. Recuperado el 22 de junio de 2022, de http://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242-2019-033.pdf

Cedeño Villacís R. P. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. *Revista Tecnológica Ciencia Y Educación Edwards Deming*, *6*(1). https://doi.org/10.37957/rfd.v6i1.88

Ciberseguridad, C. I. S. (2017). *Política Nacional de Ciberseguridad*. http://biblioteca.digital.gob.cl/handle/123456789/738

García, A. A. (2019). *Ciberseguridad: ¿Por qué es importante para todos?* Siglo XXI Editores México.

Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Pérez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. *Revista de pensamiento estratégico y seguridad CISDE*, *7*(1), 69–79. http://uajournals.com/ojs/index.php/cisdejournal/article/view/1126

Julia, V., Lcdo, E., Emiro, J. R., Autoridades, M., Miguel, G.-C., René Cortijo -Rector, M., Patricia, A.-V., & Editora, E. (s/f). Edu.ec. Recuperado el 22 de junio de 2022, de https://uisrael.edu.ec/wp-content/uploads/2018/01/Revista-2-2016.pdf

Macías, A. D. E., & Galarza, M. D. Á. (2022). Análisis de ciberataques sobre el uso de redes sociales en relación a la protección de datos personales en Ecuador. *Dominio de las Ciencias*, *8*(1), 1070–1079. https://dialnet.unirioja.es/servlet/articulo?codigo=838337

Muñoz, S., (2021) *Everis revela que el ciberataque de finales de 2019 le costó 15 millones de euros*. El País. https://bit.ly/2YCuShV.

ONTSI. *Informe Anual del sector de las TIC, los medios y los servicios audiovisuales 2020. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información*. https://bit.ly/3uZBX8k

Ortega, S. (2022). ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE. Universidad Tecnológica Israel.

Pereira, D. F. (2019). *Ciberseguridad al alcance de todos: Guía práctica para evitar ser víctima del ciberdelincuente*. Cámara Colombiana del Libro.

Sánchez-Vallejo, M.A. (2021). *Uno de los mayores oleoductos de Estados Unidos suspende sus operaciones tras sufrir un ciberataque*. El País. https://bit.ly/3Dxz29Y

Silva, E. (2022). Modelo de seguridad informática en los aspectos organizativos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NITS. http://repositorio.uisrael.edu.ec/handle/47000/3365

Vega Briceño, E. (2020). *Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking*. Editorial Científica 3Ciencias.

Villacís, R. P. C. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador.

ANEXOS

FORMATO DE ENCUESTA

Pregunta 1. ¿Cree usted que tiene alguna responsabilidad en la ciberseguridad de la Institución?

SI

NO

NO SABE

Pregunta 2. ¿Qué nivel de dificultad tiene Ud. para averiguar la clave del internet del laboratorio de computación?

FÁCIL

DIFÍCIL

NO SE

Pregunta 3. ¿Qué tipo de seguridades ha visto en el laboratorio de computación?

Pregunta 4. ¿Ha conocido usted algún incidente donde se hayan adulterado notas en el sistema académico de la Unidad Educativa?

Pregunta 5. ¿Conoce las aplicaciones y dispositivos extraíbles que utilizan los usuarios del laboratorio dentro y fuera de él?

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLOGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Msc. Cristina Cervantes

Título obtenido
MAGÍSTER EN EDUCACIÓN **INGENIERA INFORMÁTICA EN REDES DE INFORMACIÓN**
Cédula de Identidad
1002168605
E- mail
rosana.cervantes@educacion.gob.ec
Institución de Trabajo
Unidad Educativa "Víctor Mideros Almeida"
Cargo
Coordinadora del área de Informática
Años de experiencia en el área
21 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*5*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	***5***				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***5***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***5***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***5***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***5***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*5*				
Total		*35*				

Observaciones:

Este proyecto marca una diferencia en la seguridad de nuestra Unidad Educativa, ya que se ha demostrado que estas herramientas son potencialmente valiosas. Con una metodología basada en la capacitación, concientización y uso de sniffers de software libre se logrará mitigar las vulnerabilidades que hay en la red.

Recomendaciones

Los sniffers pueden tener importancia en el ámbito educativo en términos de seguridad de la red, enseñanza de ciberseguridad, investigación y monitoreo de recursos. Sin embargo, su uso debe ser cuidadosamente gestionado para proteger la privacidad y los derechos de las personas en la comunidad educativa.

Lugar, fecha de validación: Ibarra, 08 de septiembre de 2023

Firmado electrónicamente por:
ROSANA CRISTINA CERVANTES ALBAN

Msc. Cristina Cervantes

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLOGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Msc. Carlos Ramiro Bedoya

Título obtenido
MAGISTER EN TECNOLOGíAS PARA LA GESTIÓN Y PRÁCTICA DOCENTE
Cédula de Identidad
1001829777
E- mail
ramiro.bedoya@educacion.gob.ec
Institución de Trabajo
Unidad Educativa "Víctor Mideros Almeida"
Cargo
Rector
Años de experiencia en el área
25 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*5*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	***5***				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		***4***			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***5***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***5***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***5***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*5*				
Total		*34*				

Observaciones:

La seguridad informática en las unidades educativas es esencial para proteger datos sensibles, garantizar la continuidad del aprendizaje, cumplir con regulaciones, fomentar la confianza y preparar a los estudiantes para un mundo digitalizado. No solo es una medida de protección, sino también una parte integral de la gestión educativa moderna.

Recomendaciones

RAMIRO BEDOYA

En programas de educación en ciberseguridad, los sniffers pueden ser herramientas útiles para enseñar a los estudiantes cómo funcionan las amenazas cibernéticas y cómo se pueden detectar y mitigar. Esto ayuda a preparar a los futuros profesionales de la ciberseguridad.

Lugar, fecha de validación: Ibarra, 08 de septiembre de 2023

Msc. Carlos Bedoya

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLOGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Msc. Susana Enríquez

Título obtenido
MAGÍSTER EN EDUCACIÓN **INGENIERA INFORMÁTICA EN REDES DE INFORMACIÓN**
Cédula de Identidad
0401383351
E- mail
Susana.enriquez@educacion.gob.ec
Institución de Trabajo
Unidad Educativa "Valle del Chota"
Cargo
Coordinadora del área de Informática
Años de experiencia en el área
19 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: ANÁLISIS COMPARATIVO DE SNIFFERS PARA APLICARLOS EN LAS UNIDADES EDUCATIVAS APEGADO A LAS NORMATIVA ISO 27002 Y 27005

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*		*4*			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	***5***				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***5***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***5***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***5***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***5***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*5*				
Total		*34*				

Observaciones:

Este proyecto contribuye a la ciberseguridad utilizando sniffers de código abierto, lo que evita costos y daños reputacionales. Un ciberataque exitoso puede tener gastos financieros significativos y dañar la reputación de la institución. La inversión en seguridad informática puede ayudar a prevenir estos costos y proteger la imagen de la unidad educativa.

Recomendaciones

Sugiero difundir esta metodología en otras plataformas educativa, ya que la seguridad informática adecuada en las unidades educativas genera confianza entre estudiantes, padres, personal y otros stakeholders. Saber que sus datos están protegidos y que la institución se preocupa por la seguridad informática crea un ambiente de confianza y credibilidad.

Lugar, fecha de validación: Ibarra, 08 de septiembre de 2023

Firmado electrónicamente por:
PATRICIA SUSANA ENRIQUEZ ESTACIO

_____

Msc. Susana Enriquez