UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

EXTENSIÓN "EL CARMEN"

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

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

PROYECTO INTEGRADOR

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

AUDITORÍA INFORMÁTICA PARA PREVENCIÓN DE ATAQUES NFORMÁTICOS APLICADO A LOS DOCENTES DE LA UNIVERSIDAD "LAICA ELOY ALFARO DE MANABÍ" EXTENSIÓN EL CARMEN

AUTOR

DEMERA ZAMBRANO ANDERSON LINDER

TUTOR

A.S. MARÍA SORAIDA ZAMBRANO QUIROZ, MG.

EL CARMEN, 2023

Certificación del tutor

CERTIFICACIÓN

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

Haber dirigido y revisado el trabajo de Integración Curricular bajo la autoría del estudiante **Demera Zambrano Anderson Linder**, legalmente matriculado/a en la carrera de Ingeniería en Tecnologías de la Información, período académico 2022-2023, cumpliendo el total de 360 horas, cuyo tema del proyecto es "**Auditoría informática para prevención de ataques informáticos aplicado a los docentes de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen**".

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

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

El Carmen, 23 de enero del 2023.

Lo certifico,

A.S. María Soraida Zambrano Quiroz, Mg.
Docente Tutor(a)
Área: Tecnologías de la Información

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

Declaración de autoría

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: **"AUDITORÍA INFORMÁTICA PARA PREVENCIÓN DE ATAQUES INFORMÁTICOS APLICADO A LOS DOCENTES DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN",** corresponde exclusivamente a: **DEMERA ZAMBRANO ANDERSON LINDER** con cédula de ciudadanía número **175094227-6** y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

_____

Autor

Anderson Linder Demera Zambrano
C.C 175094227-6

Dedicatoria

Han sido cinco años de lucha y esfuerzo constante para poder cumplir el objetivo, este proyecto que es uno de los más importantes de mi vida se lo dedico primeramente a mi padre, quien fue la persona que me apoyó para ingresar a la universidad y que hoy desde el lugar que esté se sentirá orgulloso de mí, también a mi madre que es la persona que aún me sigue apoyando y dando ánimos en momentos difíciles.

Anderson

Agradecimiento

Agradezco a mi tutora la Mg. María Soraida Zambrano Quiroz por el apoyo en ese trabajo de titulación, agradecer a mis familiares cercanos que siempre me están brindando buenas vibras y me agradezco a mí por nunca desmayar las ganas de seguir adelante y superarme.

Anderson Zambrano

Índice general

Índice de tablas

Índice gráficos e ilustraciones

Resumen

Con la finalidad de identificar las fallas, peligros o vulnerabilidades que pudieran poner en riesgo el buen funcionamiento de los equipos de cómputo de los docentes, la actividad planificada consiste en realizar una auditoría informática a la planta docente de la Universidad Laica Eloy Alfaro de Manabí extensión en El Carmen.

Previo a la realización de la auditoría, se completó la investigación teórica y bibliográfica correspondiente y su implementación. Los principales hallazgos se utilizaron para desarrollar las directrices basadas en la metodología Magerit y para apoyar el desarrollo de contenidos relacionados con la auditoría informática a nivel de software.

Prosiguió la investigación de enfoques, estrategias y tácticas de recopilación de datos para apoyar la aplicación de la auditoría, como la entrevista y la encuesta para obtener datos verificables sobre el estado de los activos informáticos. Se implementó una tabla de estimación de riesgos para distinguir el nivel de vulnerabilidad en el que se encuentra cada activo estimado. Se tabuló cada activo con su porcentaje de riesgo, donde se pudieron especificar las diferentes eventualidades que presentan, para lo cual se utilizó una metodología basada en el análisis y gestión de riesgos "Magerit".

Se pudo denotar que existen diversas vulnerabilidades dentro de la seguridad informática de los docentes, aunque hay docentes que son capaces de mediar la situación, existe otra parte que ignora mucho sobre la situación, entre los principales resultados obtenidos se notaron las falencias en conocimientos sobre los riesgos que puede causar tener los datos personales expuestos en el internet, así también la peligrosidad de no tener un firewall que ayude a combatir los ataque en la red.

Los principales activos de los docentes que son utilizados como herramienta de trabajos tienden a ser los más vulnerables a infección o ataques informáticos debido todos los usos que se le da como navegar en la web, subida y descargar de archivos que al momento de realizarse interactúan los activos informáticos.

Abstract

In order to identify failures, dangers or vulnerabilities that could jeopardize the proper functioning of teachers' computer equipment, the planned activity consisted of conducting a computer audit of the teaching staff of the Universidad Laica Eloy Alfaro de Manabí extension in El Carmen.

Prior to the audit, the corresponding theoretical and bibliographical research and its implementation were completed. The main findings were used to develop guidelines based on the Magerit methodology and to support the development of content related to computer auditing at the software level.

Research continued on data collection approaches, strategies and tactics to support the implementation of the audit, such as interview and survey to obtain verifiable data on the status of IT assets. A risk estimation table was implemented to distinguish the level of vulnerability each estimated asset is at. Each asset was tabulated with its risk percentage, where it was possible to specify the different eventualities they present, for which a methodology based on "Magerit" risk analysis and management was used.

It could be noted that there are several vulnerabilities within the computer security of teachers, although there are teachers who are able to mediate the situation, there is another part that ignores much about the situation, among the main results obtained were noted the lack of knowledge about the risks that can cause having personal data exposed on the internet, as well as the danger of not having a firewall to help combat attacks on the network.

The main assets of teachers that are used as work tools tend to be the most vulnerable to infection or computer attacks due to all the uses that are given such as surfing the web, uploading and downloading files that interact with computer assets.

CAPÍTULO I

1.1 Introducción

Los equipos informáticos son una herramienta poderosa y esencial en las instituciones de hoy en día, las organizaciones que contribuyen de forma rápida y eficaz a la realización de esta. Sin embargo, junto con sus ventajas, la informática también puede presentar inconvenientes, como los riesgos y la vulnerabilidad de la información en las instituciones, por lo que es necesario establecer medidas para proteger la información.

Para lograrlo, es fundamental gestionar una auditoría informática exhaustiva, que no es más que una inspección técnica realizada por un profesional en auditoría. La persona encargada de llevar a cabo la auditoría utilizará los recursos informáticos a nivel de software, con el fin de evaluar el uso adecuado de los recursos informáticos, lo que se delineará a través de hallazgos donde se identifican los riegos más sobresalientes en los activos, con el fin de efectuar medidas para el uso de buenas prácticas de seguridad informática.

La presente investigación está destinada a evaluar los equipos informáticos a nivel de software en la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen, usando la metodología Magerit que es una metodología para la gestión de riesgos informáticos, y tomando instrumentos necesarios de la normativa ISO 27000.

De forma similar a como se descubrió acreditaciones generalizadas en los libros sobre los elementos lógicos donde se garantiza una estructuración adecuada para la realización de la actual propuesta, existen registros conectados a la auditoría informática en la actualidad donde se garantizan las probabilidades del desarrollo para la investigación.

En el primer capítulo se plantea el problema, también las reseñas históricas sobre el tema de tesis donde se origina o en que tiempos se dieron los primeras auditorías, además da la importancia que tiene dentro de una empresa, se plantea cuál es el motivo por el que se eligió este tema, y qué beneficios aporta la sociedad, también se plantea el lugar donde se va a realizar, y se establece a quienes se le va a aplicar la auditoría informática, se establecen los objetivos específicos y generales.

En el capítulo II se realizó la investigación acerca de la auditoría, solo que implica realizar una auditoría, también acerca de los principales ataques informáticos y principales virus informáticos, información recabada de libros que apoyen una buena investigación, además de lo principal a conocer sobre la metodología Magerit.

En el tercer capítulo, se recurrió a la persona designada como máxima autoridad de la institución en una entrevista y a los docentes en una encuesta como parte del proceso de investigación de los métodos y procedimientos. Por otra parte, en este capítulo se realizó la tabulación de resultados y donde se detectaron las principales vulnerabilidades.

En el cuarto capítulo se plantea la auditoria inicial, los recursos a tomar, se establece la propuesta y se presenta la estructura de la metodología a usar, posteriormente se detectan los principales activos, se plantea su nivel de riesgo basado en la metodología Magerit y se procede con la auditoría.

En el capítulo V, se establecen los criterios de la auditoria, se realiza un análisis interpretativo de los resultados obtenidos, en el capítulo VI de realizan las conclusiones y recomendaciones del tema establecido acompañado de los anexos de evidencia durante la auditoría realizada.

1.2 Presentación del tema

Auditoría informática para prevención de ataques informáticos aplicado a los docentes de la universidad “Laica Eloy Alfaro de Manabí” extensión El Carmen

1.3 Ubicación y contextualización del tema

En la universidad “Laica Eloy Alfaro de Manabí” extensión El Carmen está ubicada en la Av. 3 de Julio, ciudad del El Carmen, provincia de Manabí, Ecuador. Se realizó la investigación sobre las vulnerabilidades de seguridad informática que pueden existir dentro de la institución, se aplicó una auditoria informática a los docentes donde se dio a conocer que tipos de riegos se pueden ser más frecuentes en sus equipos informáticos, como se puede mitigar con ese problema y medidas de seguridad que se deben tomar para reducir al mínimo cualquier tipo de ataque informático.

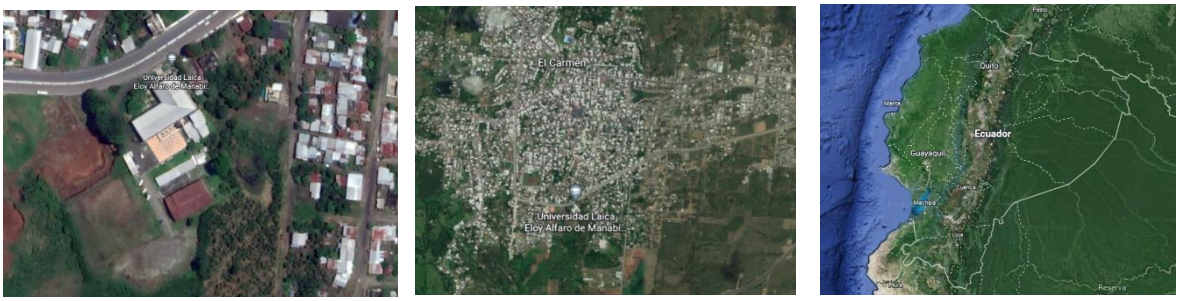


Ilustración 1 Ubicación de la institución

1.4 Planteamiento del problema

1.4.1 Problematización

En la actualidad la tecnología no para de dar sorpresas, cada día se hacen nuevos avances y descubrimientos, pero eso no es del todo bueno ya que así mismo existen una contraparte que es el utilizar cualquier brecha que se genera para hacer mal uso de esta, personas mal intencionadas que siempre tratan de causar daño en los sistemas informáticos y robar información con fines de extorción.

1.4.2 Genesis del problema

El avance de la tecnología es eminente lo que es causa principal que todos los docentes tengan el riesgo de sufrir un ataque cibernético, desde ya más de sietes años se reporta este tipo de problema, describen un docente a quien se cuestionó sobre el tema que sufrió una pérdida

total de su información a causa de intercambiar documentos a través de una USB, así mismo han existido casos donde otros docentes han perdido información valiosa a causa de virus informáticos que se alojan en sus equipos, ya sea en la descarga de algún archivo u otro percance, aunque no es un problema muy frecuente, esto no deja de ser una amenaza, por lo que se da la necesidad de aplicar una auditoria informática para encontrar y mitigar las vulnerabilidades que existen.

1.4.3 Estado actual del problema

Los ataques informáticos hoy en día son una de las principales causas de pérdida de información, por lo que se torna un peligro ante la comunidad universitaria, ya que son muy numerosos y conforme pasan los días se vuelven más sofisticados y peligrosos; entre sus principales consecuencias están la pérdida de información, pérdidas económicas y extorción; aplicando una auditoria informática no se asegura acabar con el problema, pero si se puede generar un manual de usuario para el uso de buenas prácticas de seguridad.

1.4.3.1 Medidas de seguridad ineficiente

Para poder brindad seguridad y mantener los equipos y su información protegida se debe ser estrictamente cuidados, en ocasiones surgen los problemas por el exceso de confianza, sin percatarse de que pueden existir personas mal intencionadas que alteren información o inyecten virus de forma externa.

1.4.3.2 Ataques a equipos informáticos

esto puede producirse por personas mal intencionadas que quieren manipular tu información ya sea por entretenimiento o con fines lucrativos, es importante saber que si sufres un ataque por un hacker puedes llegar a perder toda tu información y quedar expuesto.

1.4.3.3 Poco conocimiento sobre programas maliciosos

maliciosos puede surgir debido al poco interés sobre la seguridad digital o descuido, indirectamente se puede utilizar programas que contengan alguna clase de malware u otro programa dañino por no usar los protocolos de seguridad cuando se instalan programas o se descargan archivos desde la web.

1.4.3.4 Acceso de terceros a los equipos informáticos

Puede ser fácilmente una de las vulnerabilidades más comunes a la que se atribuye la pérdida de información debido a que alguien robó información directamente desde tu ordenador, ya que tuvo acceso al mismo sin ningún tipo de restricción, o en ocasiones por descuido de los propios dueños.

1.4.3.5 Navegar en la web, sin medidas de seguridad

Puede ser la causa que más afecta en la actualidad ya que es desde la web que se infiltran la mayoría de los virus u otros programas maliciosos, esto se debe a que no se tiene cuidado al momento de abrir un sitio web, o descargar un archivo, en ocasiones saltan publicidades que ya contienen algún malware solo con hacerle clic, y así existen múltiples tipos de virus, usar la web de una forma inadecuada puede ser el principal motivo de los ataques informáticos.

1.4.3.6 Uso inadecuado de antivirus

esto puede ser un gran problema ya que el usuario puede desinstalar o desactivar el antivirus y su dispositivo queda totalmente expuesto a cualquier tipo de virus, en ocasiones el uso de los antivirus no adecuados puede generar muchas falencias para proteger un ordenador.

1.5 Diagrama causa efecto

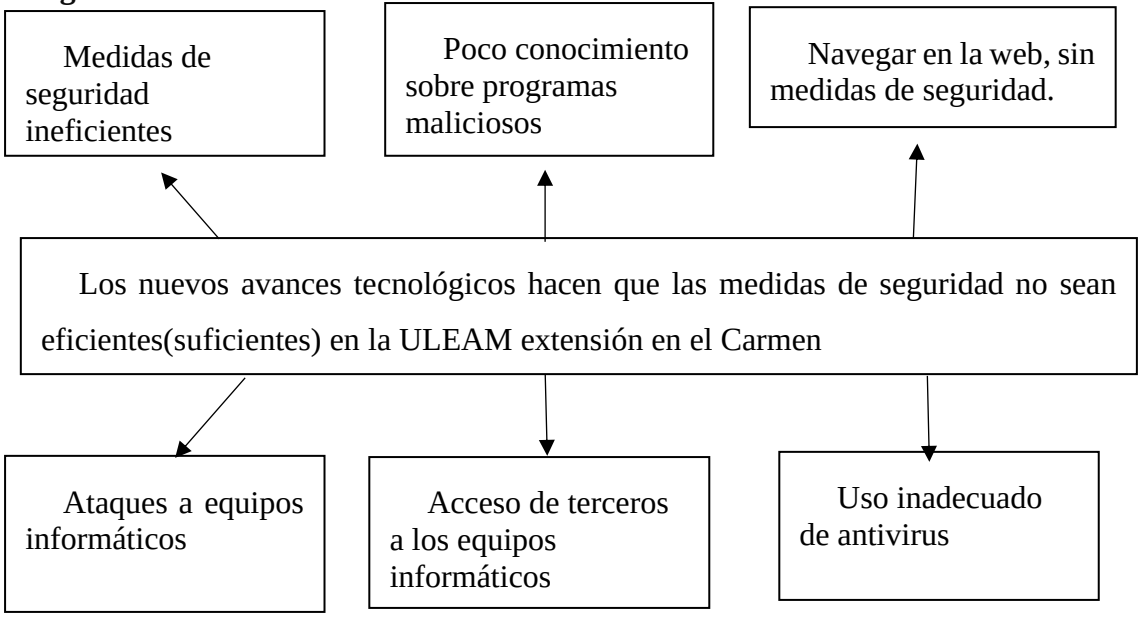


Ilustración 2 Diagrama causa efecto

1.6 Objetivos

1.6.1 Objetivo general

Aplicar una auditoría informática para la prevención de ataque informáticos a los docentes de la universidad Laica Eloy Alfaro de Manabí extensión en El Carmen durante el transcurso del año 2022.

1.6.2 Objetivo especifico

- Recopilar información bibliográfica que permita brindar mayor seguridad a los equipos informáticos.
- Aplicar encuestas y entrevista para obtener la mayor información durante la aplicación de la auditoría a los docentes.
- Evaluar los resultados mediante los hallazgos obtenidos para disminuir las vulnerabilidades de seguridad informática.

1.7 Justificación

Los ataques informáticos se han vuelto un problema persistente en la actualidad, ya que existen muchas formas de ser introducidos a equipos informáticos o servidores, según Maldonado (2017) estos pueden producirse mediante la introducción de virus u otro tipo de malware malicioso, lo que puede causar la pérdida de información confidencial, además de que puede poner en riesgo la integridad de los datos privados de una empresa, así mismo de sus usuarios, esto también puede provocar manipulación o extorción ya que en la actualidad se desconoce aún de múltiples formas de ataques informáticos.

Existe un porcentaje de docentes de la Universidad Laica Eloy Alfaro de Manabí (ULEAM) extensión en El Carmen que no se asocian de la mejor manera con la tecnología lo que los hace el grupo más vulnerable ante cualquier tipo de ataque informático, por lo que la aplicación de una auditoría informática es el proceso de evaluación de la seguridad de una entidad, ya que permite medir y controlar riesgos informáticos a la vez que permite hacer una investigación a fondo de los activos, para ver las vulnerabilidades de las cuales se carece y tomar buenas medidas de prevención ante los problemas que se generan con el avance de la tecnología.

Por otra parte, implementar una auditoría informática es una de las acciones más importantes empleadas dentro de una entidad para mejorar su ciberseguridad y protegerse de los diferentes tipos de ataques informáticos, también existen libros recientes enfocados al tema de ciberseguridad que pueden respaldar la investigación que se va a realizar durante el periodo 2022.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

Una auditoría informática para la prevención de ataques informáticos genera un impacto tecnológico positivo dentro de la universidad, ya que con el uso de buenas prácticas de seguridad se van a disminuir el daño de equipos a causa de virus informático entre otros casos, además de una mejor seguridad para los datos del usuario.

1.8.2 Impacto social

Tras la entrega del manual de usuario los docentes pueden mejorar el índice de seguridad para sus equipos informáticos, generando así mayor confianza y desempeño de los docentes, lo que influye directamente a un mejor aprendizaje para los estudiantes, esto sin hacer de menos que la tecnología avanza cada día y se generan nuevas vulnerabilidades.

1.8.3 Impacto ecológico

La auditoría informática a realizarse culminará con la elaboración de un manual de usuario para el uso de buenas prácticas para la seguridad, éste se realizará digitalmente, lo que disminuye el gasto inapropiado de papel, también evita el uso de otros materiales obtenidos de la naturaleza., la misma que beneficiará al medio ambiente ya que no utilizar el papel disminuye la tala indiscriminada de árboles, también incentiva aprovechar mejor la tecnología, a cuidar el medio ambiente y también hacer uso de este manual digitalmente desde cualquier dispositivo, aunque actualmente cuidar el medio ambiente cuenta con un gran peso, se sigue haciendo el uso excesivo de papel, la finalidad tener el manual de usuario digital es disminuir el impacto ambiental.

CAPITULO II

2 Marco teórico

2.1 Antecedentes históricos

Los importantes avances informáticos de la década de 1940 allanaron el camino para la creación de sistemas de ayuda a la estrategia militar, entre otras cosas. El uso de ordenadores y programas informáticos relacionados aumentó con el tiempo. Se prestaron numerosos tipos de ayuda a los campos de la educación, la sanidad, la industria, la política, la banca, la aviación y el comercio, entre otros.

Para León et al (2016) La auditoría informática se crea utilizando directrices establecidas por institutos a nivel nacional e internacional para las normas, métodos y técnicas. La base para el desarrollo de normas, metodologías y técnicas de auditoría informática la proporcionan los institutos nacionales e internacionales que se han establecido. Se trata de un proceso sistemático dirigido por profesionales de la auditoría y la tecnología de la información que está diseñado para garantizar que se siguen las políticas y los procedimientos.

2.2 Antecedentes relacionados con el tema presentado

En la investigación de Ávila Cevallos Anthony Aldair realizada en 2019, en la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, afirma que la seguridad de la información incluye medidas para proteger los datos del acceso, uso, divulgación, compromiso, alteración o desgracia no autorizados. Los procesos de formación, evaluación, protección, supervisión, reacción y resolución de incidentes son continuos en este proceso interactivo., este es un buen antecedente ya que la presente investigación también está dirigida a los docentes de la Uleam con la finalidad de identificar si cumples con buenas prácticas de seguridad informática.

De acuerdo con la investigación realizada por Muñoz Guillen Derly realizada durante el año 2022 en la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, afirma que a raíz de la pandemia muchas tecnologías y plataformas han tenido un crecimiento exponencial a nivel mundial, lo que ha dado origen al desarrollo de múltiples herramientas relacionadas a la tecnología, las mismas que generan vulnerabilidades, ya que una persona realiza múltiples actividades en un dispositivo electrónico, los delincuentes informáticos busca en cualquier vulnerabilidad para obtener beneficios propios, también afirma que los delincuentes utilizan diferentes técnicas para poder robar tu información, puede ser a través de virus u otro tipo de

malware, este tema se relaciona con la investigación actual ya que también está direccionado a la prevención de ataques informáticos.

Los antecedentes relacionados a esta investigación son investigaciones que particularmente tienen un enfoque a integridad y seguridad de la información, el realce que ha tenido estos últimos años los ciberataques y los problemas de seguridad informática lo que va de la mano con este tema que hace énfasis a la seguridad informática y como disminuir las vulnerabilidades más frecuentes, sin embargo su enfoque es a diferentes ámbitos, esta investigación se proyectó a la seguridad de los equipos informáticos a nivel de software de los docentes.

2.3 Auditoría informática

2.3.1 ¿Qué es auditoria?

Una Auditoría es un curso de confirmación y, además, de aprobación de la satisfacción de un movimiento según las normas dispuestas y especificadas. Tal y como indica la ISO (Organización Internacional de Normalización), un ciclo deliberado libre y archivado permite obtener pruebas de revisión y realizar una evaluación objetiva para decidir hasta qué punto se cumplen las medidas de revisión. Según Comamala (2022) La razón de ser de una revisión es analizar; distinguir qué ejercicios se llevan a cabo de forma adecuada, cuáles no y cuáles pueden pasar al siguiente nivel. Llevar a cabo una revisión empresarial donde a partir de la prueba se pueden identificar las decepciones, avanzar en las mejoras y reunir datos objetivos sobre el estado de la asociación para decidir.

2.3.2 Características de una auditoría

Para Calderón y Ocaña (2014) la actividad de evaluación debe distinguirse generalmente por ser: Ecuánime, lo que implica que debe fundarse en realidades genuinas, sustentables y con pruebas, actuando en su avance con una conducta mental libre y desprejuiciada.

Deliberada, ya que se crea bajo una progresión de pasos y etapas, los cuales deben ser ejecutados en una solicitud sensata para lograr el objetivo final.

Competente y directa, ya que será un ciclo creado por un revisor, un individuo, que debe poder informar de lo que se encuentra en la revisión con casi ningún juicio de estima y libertad.

2.3.3 Auditoria informática

Según Palacios et al (2019)con el ascenso de la digitalización, esencialmente todas las organizaciones trabajan en cierta medida en la web o mantienen una presencia basada en Internet. Por esta razón debemos aceptar una intensa consideración en la seguridad del manejo de la información, así como mantener un control ideal de los sistemas informáticos constantemente.

Una Auditoría de TI es crítica en estos días, ya que la innovación está progresando rápidamente hasta tal punto que podríamos pensar que tenemos esfuerzos de seguridad satisfactorios, y en segundo lugar se existen regiones desprotegidas Imbaquingo et al (2020). Se trata de un ciclo completado por expertos que trabajan en el campo para garantizar la seguridad de cualquier sistema informático ejecutado en la interacción empresarial.

También sigue las directrices de aseguramiento de la información de comparación, así como para comprobar si los esfuerzos de seguridad asumidos son adecuados. En este sentido, resolvemos los posibles episodios que pueda tener un sistema informático y, lo que es más importante, se establecen los distintos modelos que todo el personal debe tener en cuenta para la utilización adecuada del sistema informático.

2.3.4 Cómo puede ayudarle una auditoría informática

En términos generales, podemos decir que una revisión informática se asegurará de que el marco establecido por la organización funciona de forma productiva. En otras palabras, comprueba que la disposición de la red de ordenadores de la organización es ideal. Por lo tanto, Pazmiño (2020) afirma que, a través de una investigación intensiva, evaluaremos los posibles obstáculos que han surgido, suponiendo que se utilizan los activos adecuados, suponiendo que el sistema informático sigue las regulaciones y directrices esperadas por el área.

Suponiendo que lleva a una capacidad de registros fuera de la empresa, suponiendo que hay un déficit de los esfuerzos de seguridad que está siendo atendido por el software, etc. A la luz de este examen, una revisión informática establece los avances que la acompañan:

- Preparar a todo el personal para un tratamiento ideal de los gadgets de sistemas informáticos y, en consecuencia, para mantenerse alejado de usos desaconsejados.
- Actualizar los activos accesibles con el objetivo de que funcionen en su mejor exposición.

- Caracterizar una estrategia de mantenimiento informático preventivo para el correcto soporte y utilización del hardware.
- Trazar una estrategia de seguridad basada en Internet para el servidor del marco, la página web, el conjunto de datos de contacto, las comunidades informales, etc.
- En caso de que surjan posibilidades o episodios potencialmente PC, se realizan líneas de actividad, llevando a cabo las estrategias y técnicas vitales para abordarlos.
- Se establece un inventario con cada uno de los focos que se han explicado para completar una preparación. Esta ordenación se concentrará en cómo cada uno de estos focos puede ofrecer la ejecución más idónea.

Una auditoría de TI es comparable a tener más clientes satisfechos en su negocio, así como limitar los peligros y costos que podría esperar en el equipo debido a la ausencia de mantenimiento. Para decirlo claramente, con esta formación le ayudamos a hacer que su negocio sea beneficioso y a trabajar en la imagen de su organización a través de pequeñas señales. (Saenz Flores, 2019)

2.3.5 Tareas principales de una auditoría informática

- Todos los datos reunidos deben ser probados y reales.
- Las pruebas de revisión son realidades. Deben ser sustanciales, objetivos y probados y fácticos.
- Los modelos de revisión están dirigidos únicamente por la norma con la que los reunimos. Por ejemplo, la ISO 27002. Estas medidas deben ser consideradas y no abordadas.
- Todas las no congruencias y desviaciones deben ser archivadas, independientemente.
- Todo lo que sea coherente se archivará, pero no debería recordarse para el último informe de fines por razones de economía. Esto es así excepto si el cliente tiene un interés particular en que se muestre una conformidad extraordinaria.
- El informe de determinaciones es un resumen de las evaluaciones y en él deben aparecer las no similitudes. Este informe se transmite al cliente y lo refrenda el examinador. (Bravo Indacochea & Barrera Landires, 2020)

2.3.6 Metodología MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos, fue creado como un examen de riesgos y el procedimiento de la junta directiva creado por el Consejo Superior de Administración Electrónica de España, que ofrece una estrategia precisa para investigar los peligros que se derivan de la utilización de los avances en materia de datos y correspondencia para ejecutar las medidas de control más adecuadas para moderar los peligros. Además, cuenta con un archivo completo que reúne estrategias e instancias de cómo realizar el examen de riesgos.

Para Gusmán (2019) MAGERIT se basa en desglosar el efecto que una infracción de seguridad puede tener en la organización, buscando distinguir los peligros que pueden influir en la organización y las debilidades que pueden ser utilizadas por estos peligros, logrando así una prueba razonable reconocible de las medidas preventivas y correctivas más adecuadas.

Lo intrigante de esta técnica es que presenta una guía total poco a poco sobre el método más competente para hacer la investigación de los riesgos. Esta estrategia está dividida en tres libros. De acuerdo con el autor Viveros (2018) el primero alude al Método, donde se describe el diseño que debe tener el modelo de juego del tablero. Este libro se ajusta a lo que la ISO propone para los ejecutivos de riesgo.

El libro siguiente es un Catálogo de Elementos, que es una especie de stock que la organización puede utilizar para concentrar el examen del juego. Contiene una división de los recursos de datos para ser pensado, las calidades que deben considerarse para estimar los recursos distinguidos y además un resumen de los peligros y controles que deben considerarse.

Por último, el tercer libro es una guía de técnicas, lo que lo convierte en un factor de separación de los diferentes enfoques. En esta tercera parte se describen diversas estrategias que se utilizan a menudo en el examen de riesgos. Contiene instancias de examen con tablas, cálculos, árboles de asalto, investigación de ventajas de ahorro de dinero, estrategias realistas y grandes prácticas para completar las reuniones de trabajo para el examen de riesgos.

Esta filosofía es excepcionalmente valiosa para aquellas organizaciones que se inician en la administración de la seguridad de los datos, ya que permite centrar los esfuerzos en los peligros que pueden ser más básicos para una organización, es decir, los relacionados con los marcos de datos. Es interesante que, al estar alineado con las normas ISO, su ejecución se convierte en la etapa inicial para la certificación o para el desarrollo posterior de los marcos de administración (Cabrejos Torres, 2020).

2.3.7 Norma de estandarización ISO 27002

La norma comienza aportando unas orientaciones sobre el uso como finalidad y modo de aplicación de este estándar.

Normas narrativas: recomienda la consulta de ciertos documentos indispensables para la aplicación del ISO 27002.

Contextos de la organización: este es el requisito principal de la norma, el cual recoge indicaciones sobre miento de la organización y su contexto, la comprensión de necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.

liderazgo: este apartado destaca la necesidad de todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha demostrado su liderazgo y compromiso, se debe elaborar una política de seguridad que conozca toda la organización y se anda asignar roles, responsabilidades y autoridades dentro de la misma. (Arguezo Ramirez, 2019)

Planificación: esta es una sección que propone de manifiesto la importancia de la determinación del riesgo y oportunidades al momento de planificar un sistema de gestión de seguridad de la información, es así cómo se establecen los objetivos de seguridad de la información y el modo de lograrlos en esta norma ISO.

Soporte: es en esta cláusula la norma señalada que del buen funcionamiento del SGSI la organización debe contar con los recursos necesarios, competencias, comunicación e información documentada pertinente al caso. Operación: para cumplir con los requerimientos de seguridad de la información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, a hacer una valoración de los riesgos de la seguridad de la información y un tratamiento de ellos.

evaluación de desempeño: en este punto se establece la necesidad y la forma de evaluar o llevar a cabo el seguimiento, la medición como el análisis, la evaluación, la auditoría interna y la revisión por la dirección del sistema de gestión de seguridad de la información, todo esto para asegurar que funciona según lo planificado.

La ISO 27002 para los sistemas gestores de seguridad informática es sencilla de implementar, automatizar y mantener con la plataforma tecnológica de ISO Tools. Con ISO Tools da cumplimiento a todos los requerimientos basados en el ciclo PHVA qué significa planear, hacer, verificar y actuar. para que éste sea establecido se debe establecer, implementar,

mantener y mejorar el sistema gestión de la seguridad de la información Así mismo como el cumplimiento de manera complementaria a las buenas prácticas o controles establecidos en la ISO 27002. (De Santiago Bartolomé, 2019)

La seguridad de la información según ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados por su tratamiento.

- Confidencialidad: la información no se pone a disposición y se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantener la actitud y completitud tú de toda la información y sus métodos durante el proceso.
- Disponibilidad: Acceso y utilización de la información y de los sistemas de tratamiento de esta por parte de los individuos o procesos autorizados siempre y cuando lo requieran.

2.4 Ataques informáticos

2.4.1 Seguridad informática

Se puede caracterizar la seguridad como el método involucrado con la prevención y la distinción de la utilización no aprobada de un sistema informático. Incluye la forma más común de salvaguardar contra los intrusos que utilizan nuestros recursos informáticos con la expectativa maligna o con el objetivo de beneficiarse, o incluso la posibilidad de llegar a ellos por casualidad. Para Suárez (2022) la seguridad informática es realmente una parte del término más no exclusivo de la seguridad de los datos, aunque de vez en cuando los dos términos se utilizan con frecuencia recíprocamente.

La seguridad informática incluye varios esfuerzos de seguridad, por ejemplo, proyectos de programación antivirus, cortafuegos, y diferentes medidas que dependen del cliente, por ejemplo, potenciando o debilitando capacidades de programación específicas, por ejemplo, scripts Java, ActiveX, tratando con la utilización apropiada de, de la organización o de Internet.

Sin embargo para Gómez (2018)el significado de la seguridad de los datos alude a una disciplina que se ocupa de la ejecución especializada de la seguridad de los datos, el envío de avances que establecen un método para garantizar a medias o todas las circunstancias de decepción, cuando los datos son el recurso en peligro, es la disciplina que discute sobre las posibilidades, los peligros, el examen de la situación, las grandes prácticas y los planes

administrativos, que requieren niveles de confirmación del ciclo y la innovación para elevar el grado de confianza en la creación, el uso, la capacidad, la transmisión, la recuperación y la última eliminación de los datos.

2.4.2 Seguridad digital

La seguridad digital o la seguridad de las tecnologías de la información es el ámbito de la información de los datos que se centra en el aseguramiento de la base de las infraestructuras computacionales y de todo lo relacionado con ella, especialmente los datos que contiene o que fluyen. Para Gallegos et al (2019) afirman que existe una progresión de normas, convenciones, técnicas, reglas, instrumentos y reglamentos destinados a limitar los peligros potenciales para el marco o los datos. La seguridad informática incorpora la programación de los equipos y todo lo que la asociación valora y supone una apuesta. En el caso de que estos datos privados queden bajo el control de otros, se convierten en una apuesta para toda la asociación.

Las medidas proactivas y de respuesta incorporan tecnologías, enfoques, controles, preparación y programas de capacitación dirigidos a salvaguardar la privacidad, la fiabilidad y la accesibilidad de los datos contenidos en el entorno informático.

El riesgo en el entorno informático o riesgo de seguridad avanzado es la consecuencia de una mezcla de peligros y debilidades en el entorno informático. El riesgo de seguridad avanzado incluye procesos que garantizan que las actividades o medidas son adecuadas a los peligros y objetivos monetarios y sociales en cuestión.

La prosperidad monetaria y social incorpora la creación de abundancia, el desarrollo, la seriedad, entre otros, así como los puntos de vista relacionados con las oportunidades individuales, el bienestar, la escolarización, la cultura, la cooperación basada en la popularidad, la ciencia, la relajación y diferentes componentes de la prosperidad en los que el clima avanzado está impulsando el avance. (Ferrino, Regueira, & Zapico, 2019)

2.4.3 Estrategias de seguridad

Esta es, sin duda, probablemente la mayor preocupación de cualquier cliente de Internet en el mundo. Es típico, hoy en día los ordenadores y los teléfonos móviles se han convertido en algo tan fundamental que guardamos datos muy personales en ellos. Por suerte, hay un área que practica definitivamente en nuestra seguridad mientras utilizamos cualquier gadget: la protección de la red. Según Postigo (2020) existen firewalls, antivirus y diferentes proyectos para salvaguardar tus equipos contra asaltos de cualquier tipo. En este artículo discutiremos los principales procedimientos utilizados por los expertos para proteger sus equipos, con el

objetivo de que usted pueda seguir su modelo y hacer lo mismo en su PC en un ámbito más modesto o grande.

Los avances en tecnologías de información y comunicación (TIC) son una figura fundamentalmente significativa en el cambio de la nueva economía mundial y en los rápidos cambios que se producen en la opinión pública. Esto ha provocado un desarrollo incesante en el trabajo de la seguridad de los datos, que se considera el recurso más importante del tiempo informático, y ha obligado a que los marcos mecánicos estén suficientemente protegidos contra los peligros legítimos y reales. Cada asociación está indefensa ante los asaltos a los ordenadores y, sorprendentemente, más las instituciones de educación superior que guardan datos sobre el personal regulador, los instructores y los alumnos. (Gordón Revelo & Pacheco Villamar, 2018)

2.4.4 Tipos de ataques

- Carnada

Un gran número de los clientes están interesados por lo que esto es utilizado por los rufianes de PC, por ejemplo, alguien puede dejar un USB desatendida en cualquier lugar para un individuo para tomar y la interfaz a su PC para comprobar lo que contiene, al hacer esto una programación maligna se ha presentado de forma proactiva.

- suplantación de identidad

Es uno de los más utilizados, y consiste en engañar a una persona para que dé datos como clientes, contraseñas, etc., utilizando técnicas, por ejemplo, de manipulación mediante tácticas de miedo. También se utilizan técnicas, por ejemplo, recrear un correo electrónico de una figura de poder, por ejemplo, un jefe, supervisor, jefe, que solicita enviar calificaciones con el objetivo de que el delincuente de informático pueda entrar al sistema informático.

- Engaño

el método de actividad de un ciberdelincuente para este asalto es utilizar el dolor o la miseria que se puede causar en un individuo, utilizando el correo para enviar historias extremadamente desafortunadas como el fallecimiento de un individuo, una enfermedad terminal, entre otras, esto para conseguir que la fuente envíe dinero en efectivo.

- Quid Pro Quo

Con este tipo de truco se envían por correo electrónico adelantos, premios, artículos, para que el beneficiario termine con las estructuras y posteriormente el malhechor pueda obtener la mayor cantidad de información privada para ser utilizada en el fraude al por mayor.

- Spear phishing

Depende de la recolección de datos de los representantes como páginas a las que habitualmente ingresan, para entender lo que les gusta, por ejemplo, les gusta ir de compras, están buscando una tarea, les gusta la comida, cuando el culpable ha recolectado estos datos continuará con el envío de mensajes atrayentes según las inclinaciones de este, todo junto para que el beneficiario lo abra y consecuentemente descargue programación malévola. (López Suarez, 2020)

2.4.5 Tipos de virus

- Gusanos

Castro et al (2018) afirma que esta infección se hace con la capacidad de duplicar entre ordenadores. Con frecuencia causa errores en la red debido a la extraña utilización de la capacidad de transmisión provocada por este malware. Los ciberdelincuentes con frecuencia utilizan nombres atractivos en las conexiones para conseguir esta infección descargada, como las palabras: sexo, apuestas, regalo o premio.

- Adware

El adware también se conoce como programación de promoción. Los creadores de adware incorporan avisos o ayudan a apropiarse de otros programas para ganar dinero. Existen en todos los ordenadores y teléfonos móviles. Mientras que la gran mayoría de ellos están totalmente protegidos y son reales, algunos pueden tener intenciones aburridas, por ejemplo, apropiarse de otras infecciones o abrir accesos indirectos

- Spyware

Se trata de un tipo de malware más particular, ya que es fundamentalmente un programa espía. Su probablemente tomará todos los datos de su ordenador y obtener a su propietario. Es uno de los principales caminos para las violaciones fructíferas de seguridad. Básicamente se utilizan para tomar los datos y almacenar los desarrollos de los clientes en la web y mostrar promociones de primavera a los clientes. Algunos spywares se colocan deliberadamente en los

sistemas informáticos corporativos o públicos para examinar a los clientes. Pueden recopilar información de cualquier tipo, por ejemplo, propensiones a la lectura en la web, contraseñas, datos bancarios, entre otros.

- Ransomwere

Este tipo de malware es mucho más específico que los anteriores. Toma medidas para distribuir la información del afectado o bloquear el acceso a su ordenador de forma perpetua, excepto si se paga un gasto. De ahí que la interpretación del nombre sea captura de información. Los métodos más progresivos son el chantaje criptoviral, que codifica los registros del afectado dificultando su acceso. Suponiendo que se haga bien romper esa clave es impensable. Se completan utilizando troyanos, que parecen ser documentos genuinos.

- Botnet

Para Zambrano (2020) se trata de organizaciones de gadgets manchados que los ciberdelincuentes utilizan para enviar asaltos, por ejemplo, el envío masivo de spam, la denegación de la administración o los asaltos DDoS, el robo de calificaciones, etc. Cuando un gadget está contaminado, resulta esencial para la red de bots cuyo objetivo es extenderse.

- Rootkit

Este se esconde entre los procesos del marco y toma los datos, pero además involucra los activos de su PC para fines vengativos, como el envío de SPAM o infecciones. Son realmente difíciles de distinguir, ya que se disfrazan en el marco de trabajo y pueden pasar desapercibidos incluso por los programas antivirus.

- Troyanos

Un troyano es un tipo de malware que, para contaminar un equipo, se camufla como un programa auténtico. Según Torres (2022) una vez activados, los troyanos pueden permitir a los ciberdelincuentes vigilarle, tomar su información privada y obtener un acceso secundario a su estructura, conocido como acceso indirecto. Asimismo, están equipados para borrar registros, bloquear cuentas, ajustar contraseñas y, en cualquier caso, para interrumpir la exposición de su ordenador.

- Phishing

La principal función del Phishing es la obtención de datos confidenciales de los usuarios, generalmente son datos financieros. La gran familiaridad que este tipo de amenaza tiene con el

sistema y el desconocimiento propio de su operación, es lo que permite que sea tan eficaz al momento de cometer los actos ilícitos. A su forma de operación se suma los pocos mecanismos de defensa que los usuarios tienen con este tipo de amenazas. Haciendo más fácil su operación y el robo de información, lo que constituye una gran pérdida tanto para las empresas como para los diferentes usuarios de la red.

- Spam.

Este tipo de amenaza se manifiesta con el recibido de múltiples correos electrónicos, en los cuales se difunde generalmente anuncios publicitarios. El envío de este tipo de publicidad se ha extendido incluso hasta la telefonía móvil. Sus principales características radican en los envíos masivos y de manera anónima. Es importante tener en cuenta que para considerar un correo como Spam este deberá tener características como imposibilitar al usuario a cancelar su suscripción; que la información que contenga atente contra la moral del usuario o que se realice un envío masivo de mensajes. (Moreno , 2018)

2.4.6 Utilización de programas de antivirus

Según Cañizares y Calazacón (2021) un antivirus es un instrumento de seguridad aparato de seguridad encargado de distinguir, prevenir y eliminar una programación maligna. Estos proyectos de programación se retratan funcionando entre bastidores y filtrando continuamente la máquina en busca de malware. filtrando continuamente la máquina en busca de malware, ofreciendo así seguridad contra la programación maligna continuamente. programación maligna continuamente.

2.4.6.1 ¿Cómo Funciona?

De acuerdo con Salcedo (2022)lo principal es entender lo que un antivirus escanea en las máquinas. Este tipo de software o herramientas de protección se encargan de validar los datos de validar datos de páginas web, descargas, archivos internos del ordenador y programas o software antes y después de ser instalados. y programas o software antes y después de ser instalados. La forma en que se evalúan las amenazas es comparando los archivos o programas con una base de datos de diferentes programas con una base de datos de diferentes tipos de malware o archivos potencialmente peligrosos.

Esta base de datos suele actualizarse a diario, ya que cada vez que se instalan nuevos programas maliciosos o archivos potencialmente peligrosos. Esta base de datos suele actualizarse a diario, ya que cada día se encuentran o crean diferentes amenazas por parte de

los hackers o piratas informáticos. hay varias formas de detectar malwares en la red para actualizar posteriormente la base de datos antivirus. actualizar posteriormente la base de datos antivirus. Dos de las principales y más utilizadas son la reactiva y la proactiva. (Herrero Álvarez, 2018)

2.5 Conclusiones relacionadas con el marco teórico en referencia al tema planteado

Una auditoría informática es un mecanismo mediante el cual se examinan todos los activos a los que se va a auditar, para posteriormente realizar un informe el cual sirve para hacer recomendaciones de mejoras en los sistemas informáticos, o a su vez crear políticas y procedimientos dentro de una empresa u organización,

Los ataques informáticos son una amenaza constante hoy en día, por lo que se debe tener mucha precaución, no solo son archivos mal intencionados o maliciosos, existen personas detrás de estos que buscan beneficiarse de alguna manera, los ataques informáticos han existido durante mucho tiempo y en la actualidad son más sofisticados y difíciles de detectar, sin embargo, son muy dañinos tanto para un dispositivo como para la integridad de una persona.

La investigación realizada permite al lector tener unos conocimientos más adentrados a lo que son los ataques informáticos y métodos para prevención de estos, siempre se debe tener en cuenta que donde exista la tecnología se tiene el riesgo de un percance como este, por esta razón se realizan las auditorías a las empresas para mitigar los problemas de diferentes tipos, en estos casos sobre prevención de ataques informáticos.

CAPITULO III

3 Marco investigativo

3.1 Introducción

En este capítulo se describirán tanto los tipos como métodos de investigación que se aplicaron para la obtención y estudio de datos, posteriormente estos fueron tabulados para obtener indicadores que permitan establecer nuevos parámetros que ayuden a mejorar la seguridad informática dentro de la institución.

Las estrategias para la aplicación y recolección de datos son muy importantes, ya que debido a esas se puede reducir el problema en general y enfocarse realmente al área de estudio al que se desea aplicar la auditoría, esos ayudan a realizar el estudio desde lo general de problema e irlo desglosando hasta llegar a los especifico, así tomando las mejores decisiones al momento de desarrollar un manual de usuario para las buenas prácticas de seguridad informática.

Dentro de los instrumentos aplicados para la recolección de datos se tomó en cuenta la aplicación de entrevistas y encuestas, la entrevista fue aplicada al decano de la extensión por lo que él cuenta con el conocimiento de los acontecimientos dentro de la universidad y su información sería de gran ayuda para obtener un resultado que ayudase, por otra parte las encuesta fueron aplicadas a los docentes de la institución quien son el objetivo de la auditoría, son ellos los que aportan más información.

3.2 Tipo de investigación

3.2.1 Bibliográfica

La revisión de la literatura actual sobre el tema en estudio constituye la investigación bibliográfica. Este es uno de los pasos fundamentales de todo proyecto de investigación, junto con la elección de las fuentes de información (Matos, 2020).

Con el objetivo de reunir información fidedigna de libros y artículos sobre auditoría informática y otros componentes físicos y lógicos que beneficien el tema de investigación tanto para la fundamentación teórica de las variables como para las hipótesis propuestas, se utilizó este tipo de investigación para revisar el material bibliográfico que abarca el tema de investigación.

3.3 Métodos de investigación

3.3.1 Deductivo - Inductivo

Utilizando la información estadística procedente de la observación, el registro y el análisis comparativo que se produce durante la investigación, se emplea la técnica inductiva en el proceso en el que se establece una relación universal de situaciones específicas. Según con Westrecher (2020), el método deductivo se asemeja más al uso de la lógica para llegar a un resultado porque la veracidad de la conclusión alcanzada dependerá de la exactitud de las premisas que se hayan utilizado como base o referencia. Este método puede aplicarse directa o indirectamente y supone extraer una conclusión a partir de premisas que se suponen ciertas.

Método aplicado en la recolección de datos ya que hace una investigación en general a la información para que esta pueda ser analizada desde un punto de vista generalizado y así de deduce a información más específica sobre los ataques informáticos lo que antes fue un problema en general.

3.3.2 Analítico - sintético

El método analítico, en cambio, se basa en el examen, descomposición y estudio muy detallado de una cosa, por lo que este método comienza con el análisis en general y descompone la información en partes más pequeñas para observar las causas y efectos del estudio que se está desarrollando. A continuación, este método relaciona cada acción realizando una síntesis general del caso o fenómeno estudiado. (Sosa, 2018)

Método aplicado a la auditoría estudiando y analizando a detalle los temas investigados y la recolección de información que fue de gran importancia, este permite encontrar detalles mas a fondo sobre las vulnerabilidades informáticas debido que gracias a este método se desglosa de una manera minuciosa la información obtenida, de esta manera se sintetiza la información en únicamente lo más importante.

3.4 Fuente de información de datos

3.4.1 Fuentes primarias

Para el desarrollo del presente trabajo, se requirió emplear fuentes primarias de información, como la entrevista y la encuesta. Estas herramientas se distinguen por el hecho de que su mecanismo es oral permitiendo al entrevistador tener una mejor obtención de datos ya que no se omiten detalles o escrito dándole al encuestador la facilidad de no tener respuestas ambiguas, y la misma se recopila directamente, sin intermediarios.

3.5 Estrategia operacional para relector datos

3.5.1 Población – segmentación

La población a la que se tomó para la aplicación de los instrumentos es de 65 docentes de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen.

3.5.2 Técnica de muestreo

La técnica de muestreo se realizó mediante la aplicación de entrevista al decano de la universidad y encuestas realizadas a los docentes ya que permite obtener información específica sobre la investigación que se realiza.

3.5.3 Tamaño de muestra

La aplicación de los instrumentos fue aplicada a 41 docentes de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen que fueron la muestra final, con la finalidad de obtener información que posteriormente se utilizó para la aplicación de la auditoría.

3.5.4 Análisis de las herramientas de recolección de datos a utilizar

Las herramientas para la recolección de datos son piezas cruciales que permiten recopilar información muy importante sobre un tema que se presenta durante su creación e implementación, para la aplicación de la auditoría informática se aplicaron las siguientes herramientas:

3.5.4.1 Encuesta

La encuesta suele ser considerada como una entrevista mediante un cuestionario en el cual el encuestado deberá responder a las preguntas antes planteadas que por lo general suelen ser preguntas cerradas para tener más exactitud en las estadísticas de los resultados obtenidos por el encuestador, esta se lleva a cabo a través de un formulario ya sea impreso o de manera digital enfocado a la obtención de información del problema del estudio, según Ahamah (2019) afirma que la encuesta tienes una mejor ventaja que las entrevista que permite una mejor tabulación de datos debido a la precisión que posee.

3.5.4.2 Entrevista

Dentro de toda entrevista existe don roles uno que es el entrevistador y el otro que es el entrevistado, el entrevistador es quien formula las preguntas de acuerdo a sus intereses mientras el entrevistado las responde, dentro de una entrevista el entrevistado puede brindar la

información necesaria, explique o argumente información, en ocasiones puede que simplemente brinde su opinión o testimonios relacionados (Seid, 2016)

Se le realizó una entrevista al decano de la ULEAM extensión en El Carmen para recabar información importante sobre temas de seguridad o falencias que tenga la institución.

3.5.4.3 Estructura de lo(s) instrumento(s) de recolección de datos aplicados

Entrevista

¿Ha existido algún tipo de incidente informático dentro de la institución, qué procedimientos se realizaron para solucionar el problema?

_____

_____

la tecnología avanza día a día así mismo los ciberdelincuentes, ¿cree usted que la seguridad de los docentes dentro de la institución puede ser violentada, y que medidas de seguridad se deberían tomar?

_____

_____

¿Existen procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de que uno que este en uso, se le esté dando mantenimiento?

_____

_____

¿Existen políticas relacionadas al ingreso y salida de Hardware dentro de la institución, que aseguren la seguridad informática de los docentes?

_____

_____

¿Brindas cursos de capacitación a los docentes sobre seguridad informática?

_____

_____

Cree usted que sería de beneficio realizar un estudio sobre vulnerabilidades que puedan existir dentro de la institución y realizar un manual para mejorar la seguridad informática ¿Por qué?

_____

_____

¿Como considera usted el nivel de seguridad informática que existe actualmente dentro de la institución?

_____

_____

¿Existe una persona responsable de la seguridad informática dentro de la institución?

_____

_____

¿Considera que los docentes de la institución están listos para enfrentar un ataque informático?

_____

_____

¿Se ha aplicado antes una auditoria informática dentro de la institución?

_____

Ilustración 3 Estructura instrumento entrevista

Encuesta.

1. ¿Conoce usted acerca de ataques informáticos

Si

No

2.Malware, es un término general para cualquier tipo de software con intenciones maliciosas. ¿Usted es capaz de identificar un malware?

Si

No

3. ¿Ha sido víctima de algún ataque informático?

Si

No

4. ¿Cuál de los siguientes ataques informáticos considera más común?

Phishing

Malware

Ataques Web

Ransomware

Troyano

Otros

5. ¿Usa antivirus en su equipo?

Si

No

6. ¿Brinda mantenimiento periódico a su equipo informático?

Si

No

7. ¿Cambia su contraseña periódicamente?

Si

No

Ilustración 4 Estructura instrumento encuesta

3.5.5 Plan de recolección de datos

Cronograma	17 días?	lun 10/10/22	mar 1/11/22
Inicio	12 días?	lun 10/10/22	mar 25/10/2
Prepar entrevista	1 día?	lun 10/10/22	lun 10/10/22
Preparar encuestas	1 día?	mar 11/10/2	mar 11/10/2
Revisión de instrumentos	1 día?	lun 17/10/22	lun 17/10/22
Corrección de instrumentos	5 días	mar 18/10/22	lun 24/10/22
Revisión de correción	1 día?	mar 25/10/2	mar 25/10/2
Aplicación de instrumento	4 días?	mié 26/10/2	lun 31/10/22
Entrevista Al decano	1 día?	mié 26/10/2	mié 26/10/2
Encuesta a docentes	1 día?	jue 27/10/22	jue 27/10/22
Tabulación y análisis de los datos	1 día?	vie 28/10/22	vie 28/10/22
Presentación y descripción de los resultados	1 día	lun 31/10/22	lun 31/10/22
Fin	1 día	mar 1/11/22	mar 1/11/22
Informe final del análisis de los datos	1 día	mar 1/11/22	mar 1/11/22

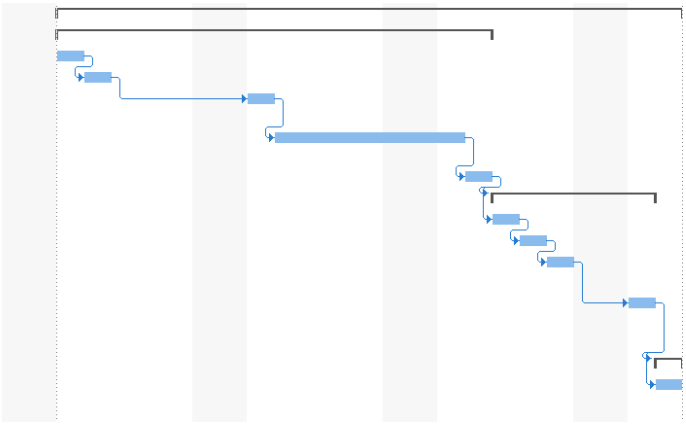


Ilustración 5 Plan de recolección de datos

3.6 Análisis y presentación de los resultados

3.6.1 Tabulación y análisis de los datos

3.6.1.1 Entrevista

N°	Pregunta	Respuesta
1	Cree usted que sería de beneficio realizar un estudio sobre vulnerabilidades que puedan existir dentro de la institución y realizar un manual para mejorar la seguridad informática ¿Por qué?	Los avances en la tecnología no pueden atrasarse los beneficios pues tampoco pueden quedar de lado, por lo que considero que si es una buena opción aplicar una auditoría para mejorar la seguridad de la institución.
2	¿Como considera usted el nivel de seguridad informática que existe actualmente dentro de la institución?	Sí, hay falencias, no hay la seguridad suficiente y actualmente todo lo que sea relacionado a internet puede ser hackeado.
3	¿Existe una persona responsable de la seguridad informática dentro de la institución?	Si, el ingeniero Jean Carlos Cedeño es el encargado de la seguridad y de los programas que se utilizan.

N°	Pregunta	Respuesta
4	¿Considera que los docentes de la institución están listos para enfrentar un ataque informático?	Existe un docente experto en el tema, claro que no todos los docentes pueden defenderse ante un ataque informático, pero pueden acudir a él para solucionar problemas mayores.
5	¿Se ha aplicado antes una auditoria informática dentro de la institución?	Que yo recuerde auditorías de este tipo no se habían implementado.
6	¿Ha existido algún tipo de incidente informático dentro de la institución, qué procedimientos se realizaron para solucionar el problema?	Que yo recuerde no, no tengo conocimientos de algún problema informático dentro de la institución.
7	La tecnología avanza día a día así mismo los ciberdelincuentes, ¿cree usted que la seguridad de los docentes dentro de la institución puede ser violentada, y que medidas de seguridad se deberían tomar?	Sí pude ser violentada hoy en día nada es seguro en especial si hablamos de informática, como bien se dijo la tecnología avanza, pero así mismo se encuentras nuevas formas de violentar la seguridad.
8	¿Existen procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de que uno que este en uso, se le esté dando mantenimiento?	Sí, existen procedimientos de mantenimiento, si un equipo informático falla se le da el respectivo mantenimiento y luego vuelve a su trabajo.
9	• ¿Existen políticas relacionadas al ingreso y salida de Hardware dentro de la institución, que aseguren la seguridad informática de los docentes?	Cuando toca hacer mantenimiento a los equipos informáticos, se brinda la confianza al técnico Ya que los equipos informáticos se hacen su respectivo mantenimiento en el mismo lugar, ya es un lugar de confianza.

N°	Pregunta	Respuesta
10	¿Brindas cursos de capacitación a los docentes sobre seguridad informática?	Sí, se brindan capacitaciones cada seis meses para seguir preparando a los docentes.

Tabla 1Tabulación de entrevista

3.6.1.2 Presentación y descripción de los resultados obtenidos en entrevistas

Entrevista: La entrevista está dirigida al decano de la institución, el cual ha sido considerado parte del trabajo de titulación debido a que tiene control sobre todo lo que pasa dentro de la universidad y los acontecimientos respecto a la seguridad informática. Por otra parte, las encuestas están dirigidas a los docentes que son el objetivo principal para mitigar los riesgos informáticos.

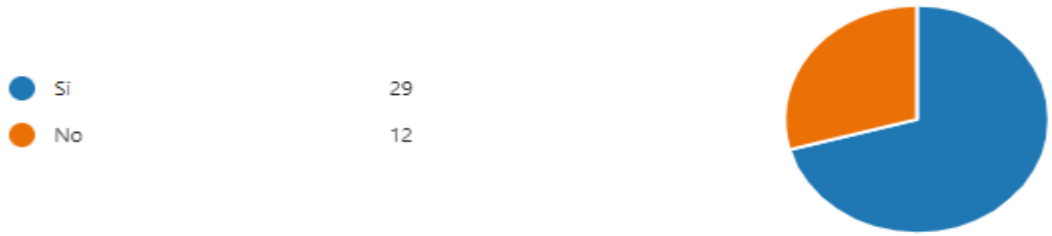
Se determina que la vulnerabilidad de los equipos informáticos de los docentes siempre está en constante riesgos ya que en la actualidad nada relacionado al internet es seguro, y aunque existe personal el cual capacita a los docentes, no es suficiente ya cada día existen nuevas vulnerabilidades, también se manifiesta que ha existido anteriormente incidentes informáticos dentro de la institución. Sin embargo, es probable que exista riesgos por descuidos en los usos de los equipos informáticos.

3.6.2 Presentación y descripción de los resultados obtenidos en encuestas

A continuación, se exponen los resultados de las encuestas y entrevistas, se ha utilizado herramientas informáticas de google forms, lo cual ha permitido realizar las respectivas gráficas para evaluar y determinar las variables.

3.6.3 Informe final del análisis de los datos

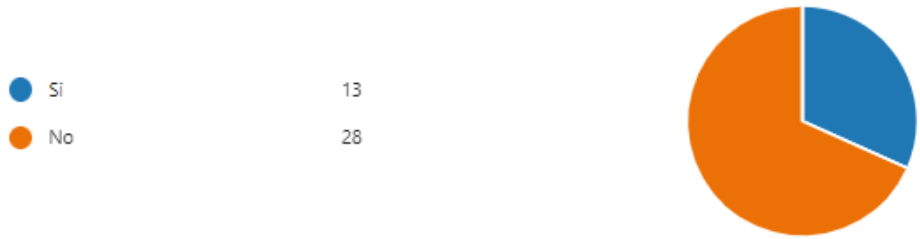
Pregunta 1: ¿Conoce usted acerca de ataques informáticos?



Análisis: De los docentes encuestados 70.23% de ellos si conocen acerca de los ataques informáticos, sin embargo, existe un 29,27% que desconoce sobre los ataques informáticos.

Interpretación: Se determina que, de la muestra a la que se encuestó, la gran mayoría tiene conocimientos sobre los ataques informáticos y los riegos que pueden generar, sin embargo, existe un pequeño margen el cual no tiene conocimientos sobre este tema lo que los hace aún más vulnerable a los riesgos de seguridad.

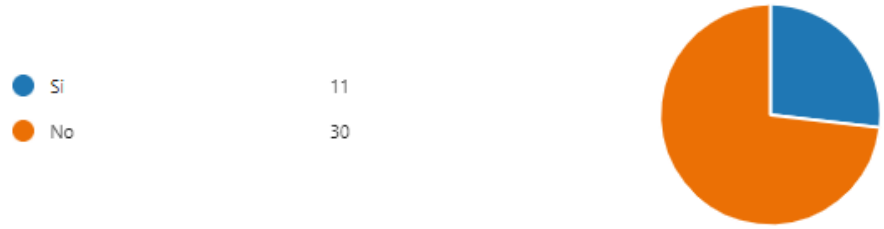
Pregunta 2: Malware, es un término general para cualquier tipo de software con intenciones maliciosas. ¿Usted es capaz de identificar un malware?



Análisis: El 68,29% de los encuestados no son capaces de reconocer un malware mientras que un 31,71 si pueden identificar un malware.

Interpretación: Se determina que la mayoría de las docentes no podrían prevenir algún malware en su equipo informático ya que no es capaz de reconocerlo, por otra parte, un pequeño margen de docentes puede tomar acciones en caso de un malware.

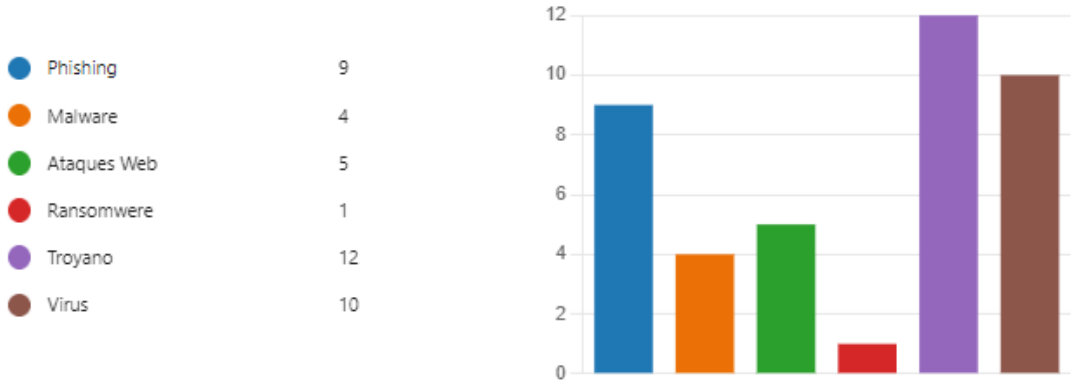
Pregunta 3: ¿Ha sido víctima de algún ataque informático?



Análisis: Un 26,83% de los docentes encuestados afirma haber sido víctima de un ataque informático, el otro 73,17% no tienen incidentes con ataques informáticos.

Interpretación: Existe una pequeña minoría de docentes afirma que han sufrido de ataques informáticos, aunque es menos de un 35% es un índice de peligro, ya que puede afectar directamente a las actividades académicas de los docentes, por otra parte, a pesar de no de que una gran mayoría no identifica un malware, afirman que no han sufrido de ataques de virus informáticos.

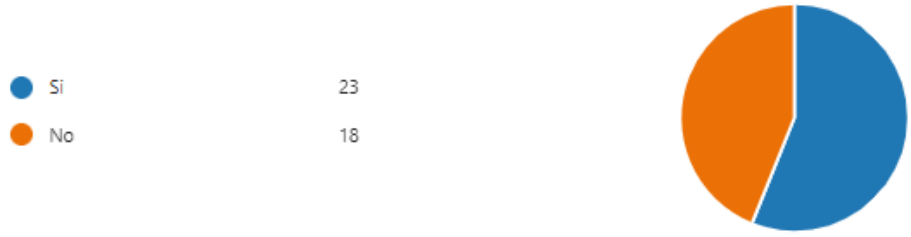
Pregunta 4: ¿Cuál de los siguientes ataques informáticos considera más común?



Análisis: De los encuestados el 29, 27% opinaron que los ataques informáticos más comunes en los equipos suelen ser los troyanos, mientras 21,95% opinan que sola más frecuentes son los phishing.

Interpretación: Todos los ataques informáticos son peligrosos, según el análisis de los encuestados, los virus informáticos son unos de los más comunes, juntos a los troyanos y phishing, que por lo general todos estos tipos de ataques maliciosos son para perjudicar a un usuario determinado.

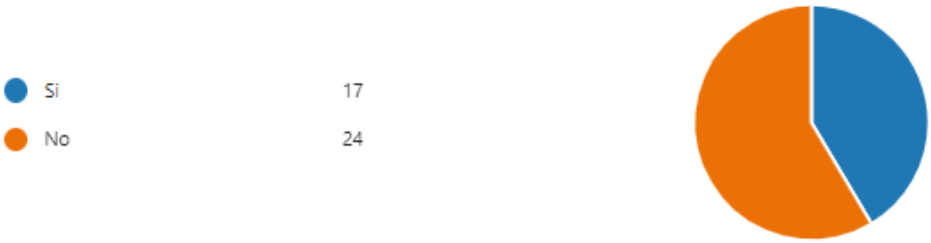
Pregunta 5: ¿Brinda mantenimiento periódico a su equipo informático?



Análisis: El 56,10% de los encuestados afirma que, si brinda mantenimiento periódico a su equipo, mientras que un 43,90 no lo hacen.

Interpretación: La mayor parte de los encuestados sabe que a un equipo informático se le debe brindar un mantenimiento correctivo, esto con la finalidad de mitigar problemas en el equipo ya sea de hardware o software, por otra parte, un pequeño porcentaje no hace mantenimiento a los equipos informáticos, lo que implica que puedan ser vulnerable ataques informáticos.

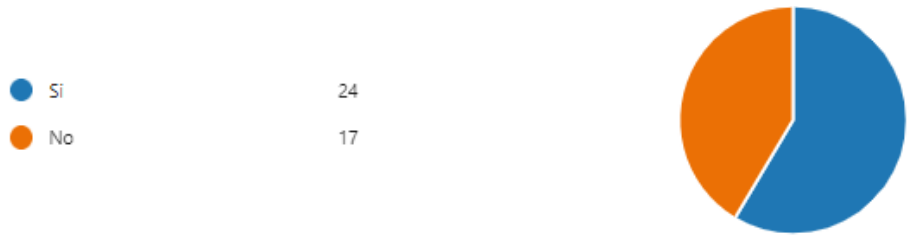
Pregunta 6: ¿Cambia su contraseña periódicamente?



Análisis: El 41,46% de los docentes que fueron encuestados si cambian contantemente sus contraseñas, el 58,54% no cambia su contraseña.

Interpretación: Esto indica que más del 50% de los docentes permanece con la misma contraseña por tiempos prolongados, lo que los hace muy vulnerable a la pérdida de información, ya que usar la misma contraseña durante mucho tiempo es uno de los principales motivos por los que se pueden hackear los equipos informáticos.

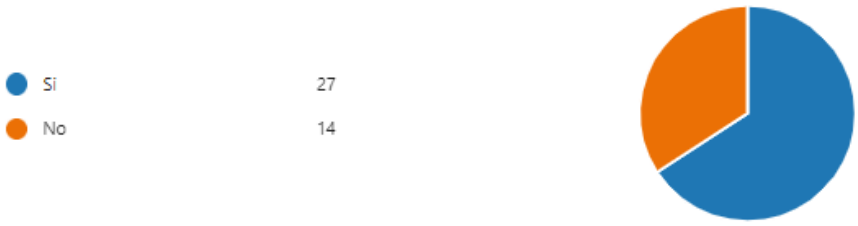
Pregunta 7: ¿Evita usar datos personales para la contraseña de sus equipos informáticos como: número de cedula, nombres, fechas de nacimientos, ¿entre otros?



Análisis: El 58,54% de los encuestados evita el uso de datos personales en sus contraseñas, sin embargo, un 41,46% si usas esos datos referenciales en sus contraseñas.

Interpretación: Se determina que, los docentes que usan datos personales en sus contraseñas son más propensos a sufrir un ataque informático ya que es una de las principales causas de ataque maliciosos y pérdida de información, pero existe una gran mayoría que conoce los riesgos que esto implica y usan otras referencias para sus contraseñas por precaución.

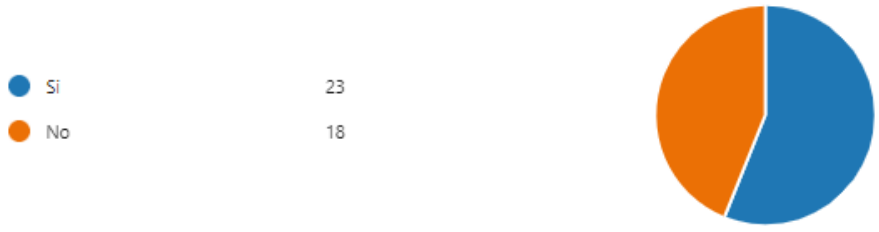
Pregunta 8: ¿Usa antivirus en su equipo?



Análisis: El 65,85 % de los docentes encuestados si usan un antivirus en sus equipos informáticos y un 34,15% no posee o no usa un antivirus en su equipo informático.

Interpretación: Es un problema bastante común que no se use antivirus en los dispositivos informáticos, sin embargo, es un gran problema ya que los antivirus ayudan a proteger de archivos maliciosos u otros tipos de virus a los equipos, los que si usan un antivirus pueden tener mejor seguridad sin embargo no se debe de confiar solo en el antivirus.

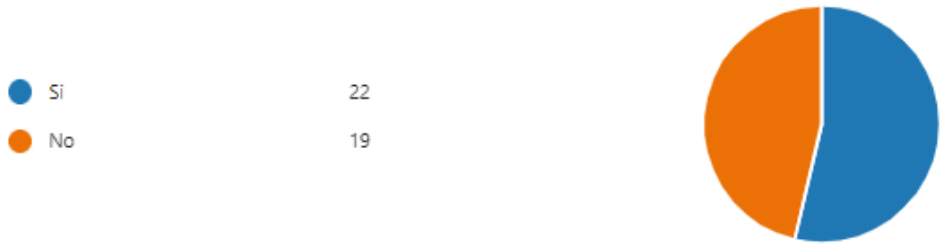
Pregunta 9: Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. ¿Tiene usted implementado un firewall en su equipo informático?



Análisis: De los docentes encuestados el 56,10% si usan un firewall en sus equipos informáticos para ayudar a protegerlos, pero un 43,90 de los encuestados no usan ningún tipo de firewall.

Interpretación: Un margen de docentes son muy vulnerables a ataques informáticos mediante la red a la que se conectan ya que no poseen un firewall de protección, teniendo en cuenta que hoy en día los ciberdelincuentes atacan desde cualquier vulnerabilidad detectada, no proteger la red a la que se conecta su computador puede ser un grave peligro.

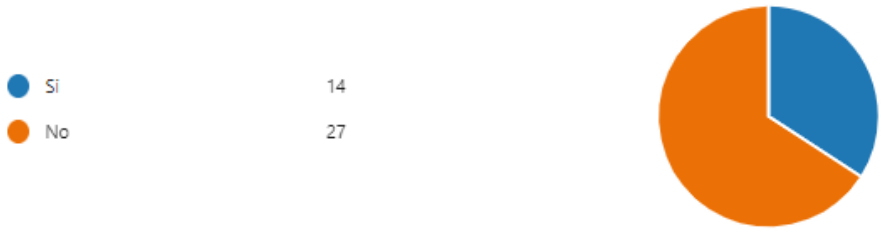
Pregunta 10: ¿Reconoce cuando un sitio web confiable y seguro?



Análisis: El 53,66% de los encuestados puede identificar si un sitio web es seguro y confiable, sin embargo, un 46,34% no son capaces de identificar si es seguro.

Interpretación: Se determina que, no reconocer si un sitio web es seguro o no acarrea un sinnúmero de peligros, ya que puedes acceder a links llenos de virus, que se ejecuten automáticamente en su ordenador o pueden descargarse archivos automáticamente que llenen de virus tu equipo informático.

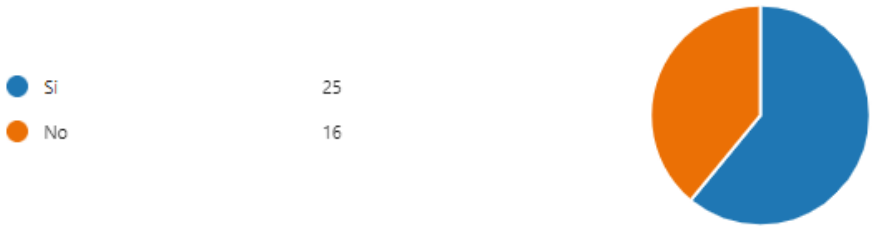
Pregunta 11: ¿Usted guarda información personal en alguna página web del navegador?



Análisis: El 65, 85% de los encuestados evita guardar sus datos personales en sitios web, sin embargo, un 34,15% si dejan guardados sus datos en los sitios webs.

Interpretación: Dejar guardado los datos en los sitios webs es peligroso ya que si su equipo tiene un virus que robe información puedes ser muy vulnerable a un ataque informático.

Pregunta 12: ¿Revisa detenidamente un correo electrónico antes a abrir o descargar cualquier archivo?



Análisis: 60,98% de los encuestados hacen una revisión delicada al descargar cualquier tipo de archivo desde sus correos, un 39,02 no revisa nada.

Interpretación: Es Muy importante realizar una revisión cuidadosa en los correos que se recibe, además puedes ser víctimas de un ataque informático si no se tiene cuidado, esto implica que se infecte de virus su computador y pierdas información o se dañen sus archivos.

3.6.4 Triangulación general

Basado en los resultados que se obtuvieron a partir de los instrumentos realizados se logró evidenciar que dentro de la universidad existen muchas falencias de seguridad de la información, se puede determinar que la seguridad informática es un riesgo al cual se debe poner mayor énfasis ya que está presente en los equipos informáticos, esa información se da a conocer en la pregunta 2 de la encuesta tanto como en la pregunta 7 de la entrevista relacionada a los ataques informáticos.

En la pregunta 3 de las encuestas se determina que una parte de los encuestados han sufrido algún ataque informático, mientas en la pregunta 10 se da a conocer que no todos son capaces de identificas sitios web seguros, información que se relaciona con la pregunta 3 de la entrevista donde afirmo que existe un personal capaz de hacer frente a ese problema, sin embargo, no todos pueden hacerlo.

Dentro de la encuesta en la pregunta 11 también se puede evidenciar que muchos de los docentes, suelen dejar sus datos guardados en los navegadores webs, para cuando se hace usos de ciertas páginas que se utilizan recurrentemente sea mucho más fácil acceder, sin embargo, esto implica un problema grave, porque dentro de la internet es donde mayo cantidad de peligros informáticos se encuentran alojados y causar perdida de información delicada, mientras que en de la entrevista se dio a conocer que los docentes se capacitan todos los semestre lo que implica que no todos lo hacen de la manera correcta.

CAPITULO IV

4 Marco propositivo

4.1 Introducción

Se realizó una minuciosa investigación para detectar las vulnerabilidades de seguridad informática en la Uleam, donde después de la tabulación de datos se procedió a la aplicación de la auditoría, en esta parte de la investigación se describen los recursos que se implican durante el proyecto, la metodología con la cual se trabaja, dentro de la metodología se describen sus fases.

Dentro de la auditoría se evalúan los activos informáticos, los niveles de inseguridad que encuentras, esto para determinar las amenazas vulnerabilidades de cada activo, para posteriormente realizar el manual de usuario que es donde se describe las técnicas para hacer buen uso de prácticas de seguridad informáticas.

De acuerdo con la investigación realizada, se tomaron los activos que se consideraron más importantes para la investigación realizada, se tomó la escala de vulnerabilidad descrita en la metodología Magerit, para la evaluación de los activos, y los criterios son tomados en base a la norma ISO 27002, que es una norma basada en el uso de buenas prácticas de seguridad informática.

4.2 Descripción de la propuesta

En base a la problemática de la investigación, se procedió a proponer la solución más acertada que permita alcanzar los objetivos planteados, para la prevención de ataques informáticos; dentro de la institución se necesitó recopilar información bibliográfica, que fue de vital importancia para una buena investigación, asimismo se aplicaron encuestas y entrevistas, estos son instrumentos para obtener información precisa sobre el problema que se necesita resolver.

Una vez hecho el análisis de las vulnerabilidades y aplicando los controles de la norma que se va a utilizar, el siguiente paso a realizar es un manual de usuario, éste describe las vulnerabilidades que se encontraron, también se determina el peligro que implica cada una de ellas, posteriormente se describen cuáles serían los pasos para seguir para hacer el uso de buenas prácticas de la seguridad informática.

Para el presente trabajo se hizo uso de la metodología MAGERIT, que es una metodología que está enfocada al análisis y gestión de riesgos informáticos, esta metodología se ofrece como marco y guía y para determinar los riesgos informáticos y definir el uso de buenas prácticas de seguridad informática se hizo uso de los controles de la norma ISO 27002.

4.3 Determinación de recursos

4.3.1 Humanos

A continuación, se presenta un resumen de los recursos humanos comprometidos con el desarrollo del presente proyecto de titulación.

Recurso humano	Función
A.S. María Soraida Zambrano Quiroz, Mg.	Tutor del Proyecto de Titulación
Anderson Linder Demera Zambrano	Autor del Proyecto de Titulación.

Tabla 2 Recursos humanos

4.3.2 Tecnológicos

Los recursos tecnológicos que fueron necesarios para el desarrollo del proyecto de titulación se describen de la siguiente manera:

Recursos tecnológicos	Función
1 computadora Asus, Intel Pentium(R), 8g de RAM.	De uso importante para el desarrollo de proyecto.
Internet	Es importante para realizar la investigación planteada.

Tabla 3 Recursos tecnológico

4.3.3 Económicos

En este trabajo no se hizo uso de recursos económicos por lo que el proyecto es una investigación sobre seguridad informática y requiere más de análisis e investigación que en invertir capital económico.

4.4 Etapas de acción para el desarrollo de la propuesta

En esta investigación examina la metodología Magerit, porque permite analizar y gestionar los riesgos de los sistemas de información de organizaciones o entidades públicas y privadas teniendo en cuenta la ubicación de la empresa. Las organizaciones construidas en zonas bajas, cerca de ríos o del mar se enfrentan a un mayor riesgo debido a las frecuentes inundaciones provocadas por las fuertes lluvias, el desbordamiento de ríos, etc.

Estas organizaciones son especialmente vulnerables al robo de información o equipos, un riesgo al que se enfrentan la mayoría de las empresas. Existe una alta probabilidad de pérdidas potenciales o interrupciones inesperadas de los recursos informáticos dadas estas situaciones, combinadas con las de catástrofes naturales importantes, de ahí que sea importante elaborar y aplicar un plan de contingencia informática que permite a la empresa prepararse para los retos haciendo una lista de los riesgos potenciales que podrían afectarle y qué hacer en caso de que se produzca alguno (Molina Miranda, 2017)

Magerit persigue los siguientes objetivos

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de gestionarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

4.4.1 Ventajas de la metodología

- Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.
- Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla.
- Permitirá saber cuánto valor tiene la información o los servicios que maneja la empresa y ayudará a protegerlos.
- Conocer el riesgo al que están sometidos los elementos de trabajo para poder gestionarlos.

- Tener una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

4.4.2 Análisis de Riesgos

En el análisis de riesgos se identifican y valoran los diversos elementos componentes del riesgo, obteniendo una estimación de los umbrales de riesgo deseables.

El análisis del riesgo contempla lo siguiente:

- Identificación de activos de información.
- Identificación de requerimientos legales y comerciales que son relevantes para los activos identificados.
- Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
- Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
- Cálculo de la posibilidad de que las amenazas y vulnerabilidades ocurran.

4.4.3 Inventario de activos

Los activos deben protegerse para mantener el buen funcionamiento de la empresa y la continuación de las actividades, ya que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Para llevar a cabo un análisis y una evaluación de riesgos precisos, es crucial tener claridad conceptual en las definiciones de los activos de información, dado su amplio alcance. Un grupo multidisciplinar formado por personas que participen en los procesos y subprocesos cubiertos por el alcance del modelo debe llevar a cabo el procedimiento de identificación y evaluación de activos. (Gómez, Duchimaza, Ramos, & Alejandro, 2019)

Los principales propietarios de los activos deben reunirse en un equipo multidisciplinar. La persona encargada de supervisar el mantenimiento, la utilización y la seguridad de los activos se denomina propietario de activos. Los activos importantes que entran en el ámbito del SGSI deben identificarse con precisión y luego analizarse para ver cómo podrían afectar a la empresa en caso de que perdieran su disponibilidad, confidencialidad o integridad.

4.4.4 Identificación de amenazas y vulnerabilidades

Los activos de información de las organizaciones son vulnerables a muchos peligros. Un incidente inoportuno que perjudique a la organización y a sus activos puede ser provocado por una amenaza. Es aconsejable clasificar las amenazas según su naturaleza cuando una empresa empieza a reconocer riesgos que podrían dañar sus activos. Esto facilitará la localización de los peligros más adelante. Las amenazas pueden clasificarse en las seis categorías siguientes:

- Amenazas naturales: inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales.
- Amenazas a instalaciones: fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas.
- Amenazas humanas: huelgas, robos, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave.
- Amenazas tecnológicas: virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallasen la red, fallas en las líneas telefónicas.
- Amenazas operacionales: crisis financieras, pérdida de proveedores, fallas en equipos, aspectos regulatorios, mala publicidad.
- Amenazas sociales: motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo.

Las amenazas pueden provenir de causas o circunstancias no intencionadas. Una amenaza tendría que aprovecharse de uno o más puntos débiles en el sistema, las aplicaciones o los servicios que utiliza la empresa para dañar un activo de información. Una vez identificados los numerosos riesgos que pueden dañar un activo, es necesario determinar la probabilidad de que se produzcan. Se aconseja utilizar una escala de Likert, como la del ejemplo siguiente, para calificar la probabilidad de materialización de cada amenaza.

Tabla 1. Escala de Likert

1	2	3	4	5
Muy Bajo	Bajo	Medio	Alto	Muy alto

Ilustración 6 Escala de likert

4.5 Fase I: Planificación de la auditoria.

4.5.1 Dirigido a

El presente documento está dirigido a la Universidad Laica Eloy Alfaro de Manabí Extensión “El Carmen” en donde se realizará una auditoría para prevención de ataques informáticos aplicado a los docentes, con la finalidad de alcanzar los objetivos establecidos y brindar una mayor seguridad informática.

4.5.2 Alcance

Llevar a cabo una auditoría para para prevención de ataques informáticos aplicado a los docentes de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen, como lo son, las aplicaciones que usan en sus equipos informáticos, protección de equipos informático, seguridad en contraseñas, a través de un análisis basado en las normas de estandarización ISO para los SGDI que se maneja dentro de cada uno de sus componentes, proceso que será llevado a cabo en mes de Diciembre del 2022.

4.5.3 Designación de equipo de trabajo

Para la ejecución de la Auditoría será de mucha importancia el trabajo que realizan las personas involucradas, como parte principal está, Demera Anderson que encargara en ejecutar la auditoría, también la Ingeniera Zambrano Soraida quien es la docente a cargo del proyecto designado a prevención de ataques informáticos aplicado a los docentes de la “Universidad Laica Eloy Alfaro de Manabí extensión “El Carmen".

4.6 Programa de auditoría

<table>
<tr><td colspan="3">Programa de auditoría para prevención de ataques informáticos aplicado a los docentes de la “Universidad Laica Eloy Alfaro de Manabí extensión “El Carmen"</td></tr>
<tr><td colspan="3">Objetivos:
Recopilar información bibliográfica de la investigación realizada.
Aplicar instrumentos para obtener la mayor información durante la aplicación de la auditoría a los docentes.
Identificar y valorar activos para determinar los más vulnerables.
Elaborar un manual de usuario que especifique las vulnerabilidades de seguridad informática.</td></tr>
<tr><td>Técnicas y procedimientos</td><td>Referencia</td><td>Fecha</td></tr>
<tr><td>1 Objetivo</td><td></td><td></td></tr>
</table>

Programa de auditoría para prevención de ataques informáticos aplicado a los docentes de la “Universidad Laica Eloy Alfaro de Manabí extensión “El Carmen"		
1.1 Aplicar una auditoria para prevención de ataques informáticos aplicado a los docentes de la “Universidad Laica Eloy Alfaro de Manabí extensión “El Carmen".	------	19/12/2022
1.2 Seleccionar la norma y dominios con mayor enfoque a la seguridad de la información.	Pt1	23/12/2022
1.3 Elaborar instrumentos en base a los controles de la norma seleccionada.	F1	25/12/2022
1.4 resultados de auditoría.	F1	25/12/2022
Elaborado por: Demera Zambrano Anderson	**Revisado por:**	
Fecha: 18/12/2022		
Observaciones:		

Tabla 4Programa de auditoría

4.6.1 Levantamiento de información básica

La Universidad Laica “Eloy Alfaro” de Manabí, creada mediante Ley No. 10 publicada en el Registro Oficial No. 313 de noviembre 13 de 1985, es una institución de Educación Superior, con personería jurídica de derecho público sin fines de lucro, de carácter laico, autónoma, democrática, pluralista, crítica y científica. La Universidad Laica “Eloy Alfaro” de Manabí tiene su sede en Manta, una de las cinco principales ciudades del Ecuador, ciudad ribereña al mar, centro pesquero de los más importantes del Pacifico Sur y ciudad de gran potencialidad en cuanto a desarrollo turístico, es además una ciudad que se proyecta a futuro como posible puerto de transferencia internacional. La Universidad fundamentalmente sirve a la juventud de la tercera provincia del Ecuador que tiene una población que supera el millón doscientos mil habitantes. (ULEAM, 2020)

4.6.2 Misión

“Formar profesionales competentes y emprendedores desde lo académico, la investigación, y la vinculación, que contribuyan a mejorar la calidad de vida de la sociedad”. (ULEAM, 2020)

4.6.3 Visión

"Ser un referente nacional e internacional de Institución de Educación Superior que contribuye al desarrollo social, cultural y productivo con profesionales éticos, creativos, cualificados y con sentido de pertinencia". (ULEAM, 2020)

4.6.4 Organigrama

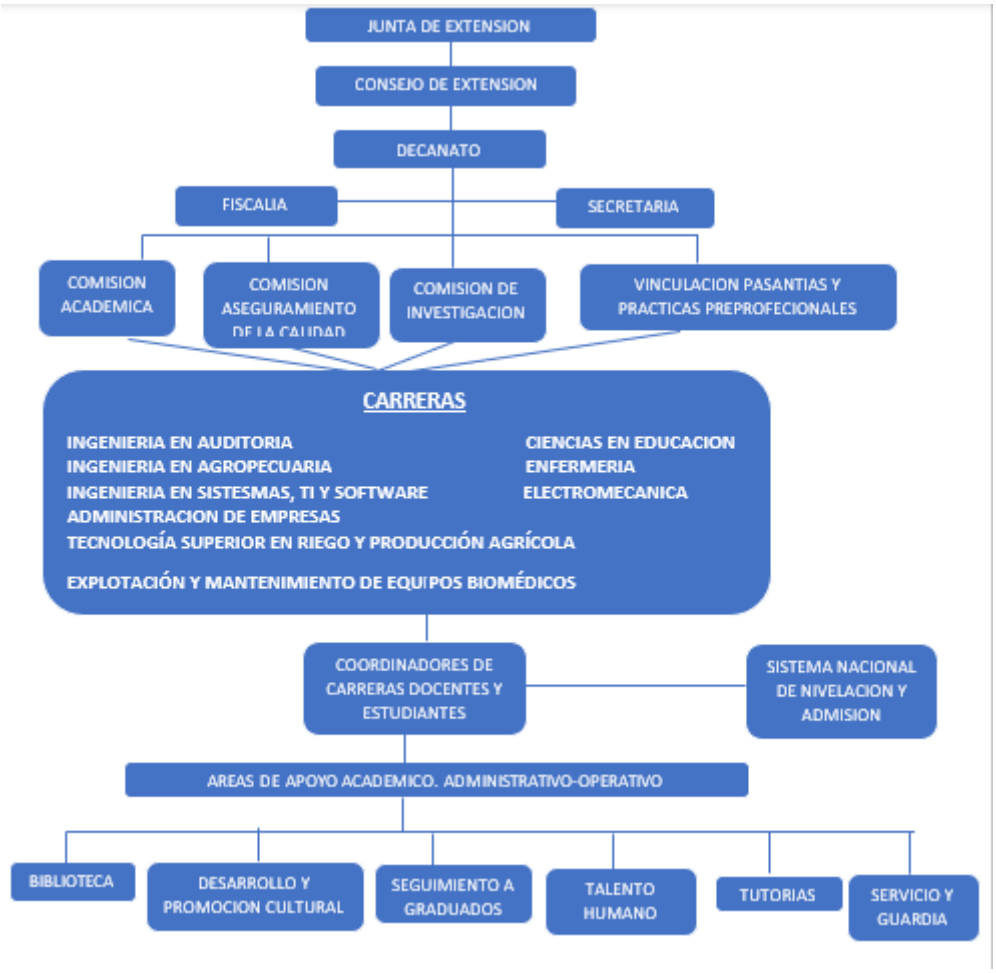


Ilustración 7 Organigrama Uleam

4.7 Fase II: análisis de requerimiento.

4.7.1 Identificación de activos

Identificación de activos de información			Ref. A
No.	Nombre	Descripción del activo	Tipo de activo

A1	Pc´s	Equipo informático para gestión de documentos educativos	Equipo informático
A2	Smartphone	dispositivo móvil que sirve para navegar en internet.	Dispositivo móvil
A3	Sistema operativo	Windows 10	Software
A4	Paquete office	Paquete de herramientas de ofimática office 365.	
A5	Antivirus	Software que permite detectar y eliminar virus.	
A6	Navegador web	Software, aplicación o programa que permite el acceso a la web.	
A7	Servicio de correo electrónico	Información de mensajes por correo electrónico institucional.	Servicio
A8	Servicio de red cableada	ayudan a la red local a funcionar sin problemas y eficientemente.	
A10	Router	Dispositivo que provee de internet	
A11	Servicio web	Servicio diseñado para la interacción entre maquinas a través de una red.	

A12	Servicio de internet	Servicio que brinda un proveedor externo.	

Tabla 5Identificacion de activos

4.7.2 Evaluación de los procesos del negocio

Pc's herramienta informática para realizar tareas, instalar programas y conectarse a clases de manera virtual. También para revisar todos los procesos académicos dentro el aula virtual como hacer consultas, participar en debates, subir tareas entre otros.

Smartphone dispositivo móvil que se utiliza para conectarse a clases virtuales, así como realizar ciertas tareas, revisar calificaciones, acceder a aula virtual y conectarse en llamadas.

Sistema operativo, conjunto de programas mediante el cual funciona la computadora o dispositivo móvil, ocupándose de gestionar la memoria de nuestro sistema y la carga de los distintos programas de software y hardware.

Paquete Office 365 permite crear, acceder y compartir documentos online entre distintos usuarios ya sea en Word, Excel, PowerPoint entre otros, esto permite la realización de las actividades de los docentes.

Antivirus es un software que permite proteger los dispositivos de múltiples ataques cibernéticos, y a la vez brinda mayor seguridad al ordenador de basuras y softwares maliciosos, ya que este permite liberar espacio en los dispositivos para que tengan una mejor funcionalidad.

Navegador web es un programa que permite acceder a la información que contiene una página, en este caso permitirá ver todos los procesos llevados dentro del aula virtual, permitiendo al usuario interactuar con el contenido y navegar además de otros procesos para la enseñanza académica.

Servicio de internet permite al usuario el acceso al contenido de los navegadores web, como es de gran utilidad para el proceso educación virtual, ya que este permite compartir recursos, comunicarse y acceder a una gran cantidad de información de cualquier parte del mundo.

Correo electrónico permite enviar y recibir mensajes de correo, además es posible de incluir archivos multimedia o documentos, y es posible recuperar la información desde cualquier dispositivo conectado a internet.

Internet por cable, a menudo conocido como el uso de un cable Ethernet para conectarse a un router o módem, es un método de acceso a Internet.

Corta fuegos, es una solución de seguridad que permite a su ordenador comunicarse con otros servicios autorizados al tiempo que bloquea el acceso no autorizado al ordenador.

Router dispositivo que provee de conexión a internet tanto para computadoras como teléfonos para establecer una ruta por el cual viajan los datos de información en la red.

Servicio web, es una tecnología que transfiere datos entre aplicaciones utilizando un conjunto de protocolos y estándares. Los servicios web permiten que distintos programas de software creados en varios lenguajes de programación y ejecutados en cualquier plataforma intercambien datos a través de redes informáticas como Internet.

Servicio de internet, es una tecnología que transfiere datos entre aplicaciones utilizando un conjunto de protocolos y estándares. Los servicios web permiten que distintos programas de software creados en varios lenguajes de programación y ejecutados en cualquier plataforma intercambien datos a través de redes informáticas como Internet.

4.7.3 Valoración de activos

4.7.3.1 Definición de la escala

Integridad		Criterio
Alto	**3**	La pérdida o modificación de la información tiene un impacto negativo en los equipos informáticos.
Medio	**2**	La pérdida o modificación de la información tiene un impacto tolerable en los equipos informáticos.
Bajo	**1**	La pérdida o modificación de la información tiene un impacto mínimo en los equipos informáticos.

Confidencialidad		Criterio
Alto	**3**	La difusión de la información no autorizada tiene un impacto muy alto los equipos informáticos.
Medio	**2**	La difusión no autorizada de la información tiene un impacto considerable para los equipos informáticos.
Bajo	**1**	La difusión de la información no tiene ningún impacto para el aula virtual.

Disponibilidad		Criterio
Alto	**3**	La falta del activo de información tiene un impacto negativo para los equipos informáticos.
Medio	**2**	La falta del activo de información tiene un impacto tolerable para los equipos informáticos.
Bajo	**1**	La falta del activo de información tiene un impacto mínimo para los equipos informáticos.

Tabla 6 Valoración de activos

4.7.3.2 Valoración de activos

$$VA = \frac{C + I + D}{3}$$

Tabla 7 Formula valoración de activo

Valoración de activos de información					**Ref. B**
No. activo	**Nombre del activo**	**Valoración de impacto**			
		C: Confiabilidad **I: Integridad** **D: Disponibilidad**			
		C	**I**	**D**	**VA**
A1	Pc´s	3	3	3	3,00
A2	Smartphone	2	2	3	2,33
A3	Sistema operativo	1	**2**	3	2,00
A4	Router	1	3	3	2,33
A5	Paquete office	1	2	2	1,67
A6	Antivirus	1	2	2	1,67
A7	Navegador web	**3**	**3**	**3**	3,00
A8	Servicio de correo electrónico	**3**	**3**	**3**	3,00
A9	Servicio de red cableada	**2**	**2**	2	2,00
A10	Servicio web	**2**	2	3	2,33
A11	Servicio de internet	**2**	2	3	2,33

Tabla 8 Valoración de activos

4.8 Fase III: evaluación de riesgos

4.8.1 Análisis de amenazas y vulnerabilidades

Identificación de riesgos			**Ref. C**
No. activo	**Nombre del activo**	**Amenazas**	**Vulnerabilidades**
A1	Pc´s	• Pérdida o robo de equipos. • Fallas del equipo. • Ataque de virus.	• Seguridad deficiente para inicio de sesión. • Falta de mantenimiento. • Poco almacenamiento.
A2	Smartphone	• Pérdida o robo del dispositivo. • Mala manipulación. • Fuga de datos.	• Perdida de información confidencial. • Contraseñas poco seguras. • Falta de protocolo para la instalación de aplicaciones o conexión a redes inalámbricas.
A3	Sistema operativo.	• Caída del sistema. • Infección de virus. • Robo de información clasificado.	• Capacidad del equipo no es compatible con el sistema. • Realizar actividades ilegales. • Errores de configuración.
A4	Router	• Fallas del equipo. • Fácil de hackear.	• Puede ser interferido por hackers. • Estar al alcance de cualquier persona. • Contraseñas débiles.

Identificación de riesgos			**Ref. C**
No. activo	**Nombre del activo**	**Amenazas**	**Vulnerabilidades**
		• Debilidad en configuración del router.	
A5	Paquete office.	• Error de activación. • Eliminación del usuario agregado. • Mal uso del paquete office. •	• Paquete office no oficial. • No tener licencia de activación. • Daño del paquete office.
A6	Antivirus.	• Eliminación del antivirus. • Ataque mediante el uso de ingeniería social. • Eliminación de ficheros importantes para el S.O.	• Falta de actualización del antivirus. • Licencia caducada. • Borrar archivos accidentalmente.
A7	Navegador web	• Infección de virus. • Actualizaciones falsas. • Suplantación	• Perdida de información. • Enlaces maliciosos. • Navegación lenta
A8	Servicio de correo electrónico	• Ataque de hackers.	• Perdida de velocidad de navegación. • Navegación lenta

Identificación de riesgos			**Ref. C**
No. activo	**Nombre del activo**	**Amenazas**	**Vulnerabilidades**
		• Eliminación del correo electrónico. • Robo de información confidencial.	• Enlaces maliciosos
A9	Red cableada	• Daño intencionado en el cable • Mal estado del cable.	• Descarga eléctrica. • Desastres naturales. • Cables de red averiados.
A10	Servicio web	• Anuncios automáticos • Paginas no seguras • Navegador no configurado	• Puede ser hackeado • Datos personales en la web • Se ejecutan archivos maliciosos automáticamente.
A11	Servicio de internet	• Corte del servicio. • Divulgación de información. • Fallo de los enlaces de comunicación.	• Falla eléctrica. • Desastres naturales. • Equipos de bajo rendimiento.

Tabla 9 Identificación de riesgos

4.8.2 Instrumentos de evaluación de vulnerabilidades

Indicadores para valorar las vulnerabilidades de los activos		
Activo 1: PC`S		**Demera Anderson**
Vulnerabilidad	**Indicador**	**Auditor**
Seguridad deficiente para inicio de sesión	¿Tiene creado un usuario de acceso para su uso personal y otro para el uso de su familia?	**Si**
	¿Su contraseña tiene caracteres como: mayúsculas, minúsculas, números, ¿un mínimo 8 caracteres y máximo 16?	**No**
	¿Cambia su contraseña constantemente?	**No**
Falta de mantenimiento	¿Brinda manteniendo a su PC?	**Si**
	¿Tiene instalado algún tipo firewall para protección de su equipo?	**no**
	¿Tiene antivirus?	**Si**
	¿Desinstala las aplicaciones que ya no utilice para liberar espacio?	**No**
Poco almacenamiento	¿Libera espacio de la papelera constantemente?	**No**
	¿Almacena archivos en algún tipo de nube online?	**Si**

Tabla 10 Instrumentos de evaluación de vulnerabilidades PC´s

Indicadores para valorar las vulnerabilidades de los activos		
Activo 2: Smartphone		
Vulnerabilidad	**Indicador**	**Auditor**
Sobrecalentamiento del dispositivo	¿Realiza mantenimiento de su dispositivo?	**Si**
	¿Deja de usar su dispositivo móvil mientras está cargando?	**No**
	¿Cierra aplicaciones que se ejecutan en segundo plano, para ejecutar una nueva?	**No**
Contraseñas poco seguras	¿Su contraseña tiene caracteres como: mayúsculas, minúsculas, números, ¿un mínimo 8 caracteres y máximo 16?	**No**
	¿Hace uso de la huella digital para desbloquear su dispositivo?	**Si**
	¿Evita usar datos personales para la contraseña de su smartphone?	**No**
Falta de protocolo para la instalación de aplicaciones o conexión a redes inalámbricas	¿Analiza la red a la cual quiere acceder?	**No**
	¿Evita instalar aplicaciones no confiables que puedan afectar a su dispositivo?	**No**
	¿Evita conectarse a redes públicas (acceso libre)?	**Si**

Tabla 11 Instrumentos de evaluación de vulnerabilidades Smartphone

Indicadores para valorar las vulnerabilidades de los activos		
Activo 3: Sistema Operativo		
Vulnerabilidad	**Indicador**	**Auditor**
Capacidad del equipo no es compatible con el sistema	¿Realizo una correcta descarga del sistema operativo?	**Si**
	¿El sistema operativo cumple con el tipo de procesador de su pc?	**Si**
	¿Realiza actualizaciones al sistema operativo para obtener la versión actual?	**Si**
Realizar actividades ilegales	¿Evita la instalación de Sistemas operativos pirateados?	**Si**
	¿Tiene conocimiento de los problemas que puede presentar su sistema operativo por no descargar e instalar de la página oficial?	**No**
	¿Evita instalar un SO modificado por falta de una licencia?	**Si**
	¿Evita usar terceras aplicaciones para actualizar el SO?	**Si**
Errores de configuración	¿Tuvo en cuenta los requerimientos necesarios para la configuración del sistema operativo?	**No**
	¿Realizo una partición del disco duro?	**No**
	¿Cuenta con licencia de activación para el sistema operativo?	**Si**

Tabla 12 Instrumentos de evaluación de vulnerabilidades SO

Indicadores para valorar las vulnerabilidades de los activos		
Activo 4: Router		
Vulnerabilidad	**Indicador**	**Auditor**
Puede ser interferido por hackers	¿Cree que la configuración de su router es suficiente para evitar ataques cibernéticos?	**No**
	¿Usa el método de seguridad en la red WPA2?	**Si**
	¿Activa el Firewall de Windows, para impedir que un programa maligno pueda robar información?	**Si**
	¿Realiza la limpieza del router cada mes?	**No**
	¿Reinicia su equipo frecuentemente?	**Si**
Estar al alcance de cualquier persona	¿El router se encuentra en un lugar seguro?	**Si**
	¿Evita que el router sea manipulado por otras personas?	**Si**
	¿Mantiene su red oculta?	**No**
Contraseñas débiles	¿Su contraseña tiene caracteres como: mayúsculas, minúsculas, números, ¿un mínimo 8 caracteres y máximo 16?	**Si**
	¿Usted cambia su contraseña constantemente?	**No**
	¿Establece direcciones IP para cada dispositivo que se conectan a la red de su router?	**No**
	¿Cumple con un estándar de contraseñas seguras para la red?	**No**

Tabla 13 Instrumentos de evaluación de vulnerabilidades Router

Indicadores para valorar las vulnerabilidades de los activos		
Activo 5: Paquete Office		
Vulnerabilidad	**Indicador**	**Auditor**
Paquete office no oficial	¿Evita Instalar paquetes de office crackeado?	**Si**
	¿Descarga el paquete office de sitios confiables?	**Si**
	¿La versión gratuita le permite acceder a todas las funciones del paquete?	**No**
	¿Activa correctamente el paquete office?	**Si**
No tener licencia de activación	¿Compró la licencia del paquete office?	**No**
	¿Evita usar versión gratuita de licencia para activar office?	**Si**
	¿Los programas se ejecutan correctamente y rápido?	**No**
	¿Identifica usted que el software instalado necesita una licencia qué es de pago?	**No**
Daño del paquete office	¿Sabe si su office está infectado por virus?	**No**
	¿Se instaló el paquete office siguiendo los pasos de instalación?	**Si**
	¿Identifica usted cuando un archivo está infectado?	**No**
	¿Le muestra un mensaje de error cuando office deja de responder?	**Si**

Tabla 14 Instrumentos de evaluación de vulnerabilidades Paquete Office

Indicadores para valorar las vulnerabilidades de los activos		
Activo 6: Antivirus		
Vulnerabilidad	**Indicador**	**Auditor**
Falta de actualización del antivirus	¿Actualiza constantemente su antivirus?	**Si**
	¿Un antivirus desactualizado puede inmunizar su computador?	**No**
	¿Evita descargar antivirus de cualquier sitio web?	**Si**
	¿Revisa si existe una nueva versión del antivirus?	**No**
Licencia caducada	¿Cree es necesario e importante renovar la licencia de antivirus?	**Si**
	¿Las características que ofrecen siguen funcionando sin estar activado?	**No**
	¿Cree que su antivirus realiza un correcto análisis general?	**Si**
Borrar archivos accidentalmente	¿Evita eliminar archivos del ordenador mediante el antivirus?	**Si**
	¿Revisa el análisis que hace el antivirus antes de eliminar los archivos que cree una amenaza?	**No**

Tabla 15 Instrumentos de evaluación de vulnerabilidades Antivirus

Indicadores para valorar las vulnerabilidades de los activos		
Activo 7: Navegador Web		
Vulnerabilidad	**Indicador**	**Auditor**
Perdida de información.	¿Evita guardar información personal en alguna página web del navegador?	**No**
	¿Ha usado el navegador en modo incognito?	**Si**
	¿Identifica cuando está accediendo a un sitio web confiable y seguro?	**No**
	¿Conoce los pasos necesarios para proteger su red y evitar alguna filtración?	**No**
Enlaces maliciosos.	¿Evita ingresar a sitios poco confiables que no posean el protocolo https?	**Si**
	¿Evita abrir anuncios que le muestra las páginas a las que accede?	**Si**
	¿Cuándo comparte un enlace de descarga, revisa si es seguro?	**Si**
Navegación lenta	¿Realiza usted un mantenimiento a su red?	**No**
	¿Tiene constancia acerca del plan de velocidades del internet?	**Si**
	¿El acceso al internet es rápido?	**No**
	¿Es consiente que el navegador Google Chrome usa mucho recurso?	**Si**
	¿Ha instalado algún navegador web más optimizado que los que viene por defecto?	**Si**

Tabla 16 Instrumentos de evaluación de vulnerabilidades Navegador web

Indicadores para valorar las vulnerabilidades de los activos		
Activo 8: Servicio de Correo Electrónico		
Vulnerabilidad	**Indicador**	**Auditor**
Enlaces maliciosos	¿Considera peligroso abrir enlaces desconocidos?	**Si**
	¿Sabe usted si al abrir enlaces sin remitente puede conllevar a que sus equipos informáticos se infecten de virus?	**Si**
	¿Evita abrir cualquier correo y aceptar cualquier petición que le hacen?	**Si**
Contraseñas vulnerables	¿Su contraseña tiene caracteres como: mayúsculas, minúsculas, números, ¿un mínimo 8 caracteres y máximo 16?	**Si**
	¿Cambia su contraseña frecuentemente?	**No**
	¿Evita compartir la contraseña de su correo con otros usuarios?	**Si**
	¿Usa la verificación de dos pasos?	**No**
Envío de mensajes masivos no deseados	¿Tiene conocimiento del spam?	**Si**
	¿Elimina con frecuencia los mensajes no deseados?	**No**
	¿Cree que está expuesto a ser extorsionado por ciberdelincuentes?	**Si**
	¿Analiza los correos no deseados antes de abrirlos?	**No**

Tabla 17 Instrumentos de evaluación de vulnerabilidades Correo electrónico

Indicadores para valorar las vulnerabilidades de los activos		
Activo 9: Red cableada		
Vulnerabilidad	**Indicador**	**Auditor**
Descarga eléctrica	¿Cuenta con un sistema de Alimentación ininterrumpida?	**Si**
	¿Usted revisa si la conexión eléctrica se encuentra en buen estado?	**Si**
	¿El servicio de internet se reestablece rápidamente después de un corte eléctrico?	**Si**
Desastres naturales	¿Después de una tormenta eléctrica la conexión a internet sigue siendo de buen rendimiento?	**Si**
	¿Revisa el cable de internet después de una tormenta eléctrica?	**No**
Cables de red averiados	¿La red se distribuye en toda la institución?	**Si**
	¿El cableado de red que posee funciona con normalidad?	**Si**
	¿Cuneta con conexión a fibra óptica?	**Si**

Tabla 18 Instrumentos de evaluación de vulnerabilidades Red cableada

Indicadores para valorar las vulnerabilidades de los activos		
Activo 10: Servicio web		
Vulnerabilidad	**Indicador**	**Auditor**
Puede ser hackeado	¿Considera peligroso abrir enlaces desconocidos?	**Si**
	¿Sabe usted identificar si una página es segura para navegar?	**No**
	¿utiliza modo incognito para reducir un poco la filtración de su información?	**No**
Datos personales en la web	¿Guarda sus datos personales como: correo, contraseña, fechas de nacimiento entre otros datos en los navegadores webs?	**Si**
	¿Cambia su contraseña frecuentemente?	**No**
	¿Evita compartir sus contraseñas con terceras personas?	**Si**
	¿Usa la verificación de dos pasos?	**No**
Se ejecutan archivos maliciosos automáticamente.	¿Tiene conocimiento de la publicidad engañosa?	**Si**
	¿alguna vez le han descargado archivos de manera automática?	**Si**
	¿Cree que está expuesto a ser extorsionado por ciberdelincuentes?	**Si**
	¿Analiza las páginas webs a las que antes de seguir navegando en ellas?	**No**

Tabla 19 Instrumentos de evaluación de vulnerabilidades Servicio web

INDICADORES PARA VALORAR LAS VULNERABILIDADES DE LOS ACTIVOS		
Activo 11: Servicio de Internet		
Vulnerabilidad	**Indicador**	**Auditor**
Falla eléctrica	¿Cuenta con un sistema de Alimentación ininterrumpida?	**Si**
	¿Usted revisa si la conexión eléctrica se encuentra en buen estado?	**Si**
	¿El servicio de internet se reestablece rápidamente después de un corte eléctrico?	**Si**
Desastres naturales	¿La conexión a internet se ve afectado por una tormenta eléctrica?	**Si**
	¿Revisa los equipos de internet después de una tormenta eléctrica?	**No**
Equipos de bajo rendimiento	¿Posee usted un equipo que abastece a toda la institución?	**Si**
	¿El equipo que posee funciona con normalidad?	**No**
	¿Cuenta con conexión a fibra óptica?	**Si**
	¿Está satisfecho con el rendimiento del equipo que le provee internet?	**No**

Tabla 20 Instrumentos de evaluación de vulnerabilidades Servicio de internet

4.8.3 Tabulación de resultados de vulnerabilidades y amenazas

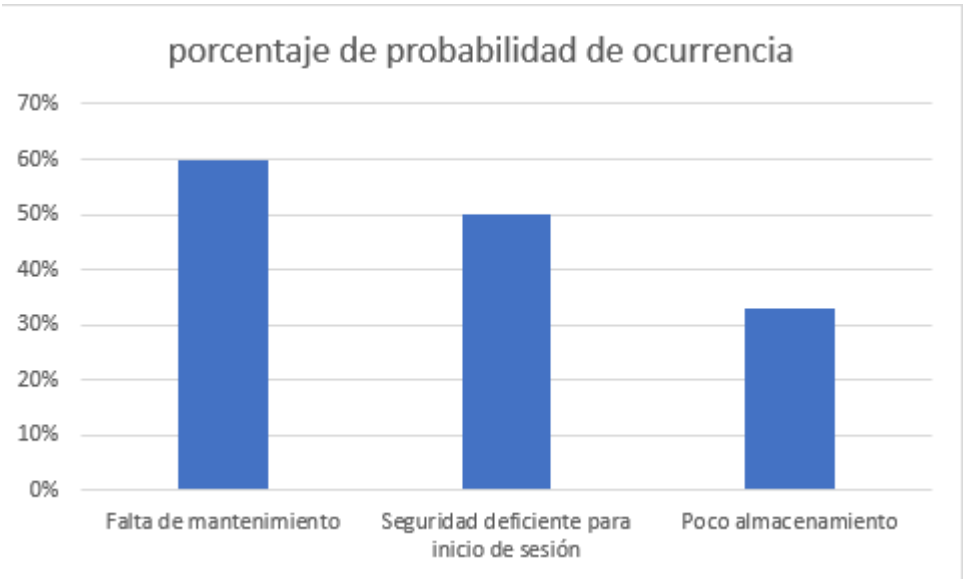
TABULACIÓN DE LOS INSTRUMENTOS APLICADOS PARA EVALUAR LOS RIESGOS EN LOS ACTIVOS			
Activos	**Vulnerabilidad**	**Auditor "Si"**	**Promedio %**
PC	V1	2 de 4	**50%**
	V2	3 de 5	**60%**
	V3	1 de 3	**33%**
Smartphone	V1	1 de 3	**33%**
	V2	2 de 4	**50%**
	V3	1 de 3	**33%**
Sistema Operativo	V1	3 de 3	**100%**
	V2	3 de 4	**75%**
	V3	1 de 3	**33%**
Router	V1	3 de 5	**60%**
	V2	2 de 3	**67%**
	V3	1 de 4	**25%**
Paquete Office	V1	3 de 4	**75%**
	V2	1 de 4	**25%**
	V3	2 de 4	**50%**
Antivirus	V1	2 de 4	**50%**
	V2	2 de 3	**67%**
	V3	1 de 2	**50%**
Navegador Web	V1	1 de 4	**25%**
	V2	3 de 3	**100%**

	V3	3 de 5	**60%**
Servicio de correo electrónico	V1	3 de 3	**100%**
	V2	2 de 4	**100%**
	V3	2 de 4	**50%**
Red cableada	V1	3 de 3	**100%**
	V2	1 de 2	**50%**
	V3	3 de 3	**100%**
Servicio web	V1	1 de 3	**33%**
	V2	2 de 4	**50%**
	V3	3 de 4	**75%**
Servicio de Internet	V1	3 de 3	**100%**
	V2	1 de 2	**50%**
	V3	2 de 4	**50%**

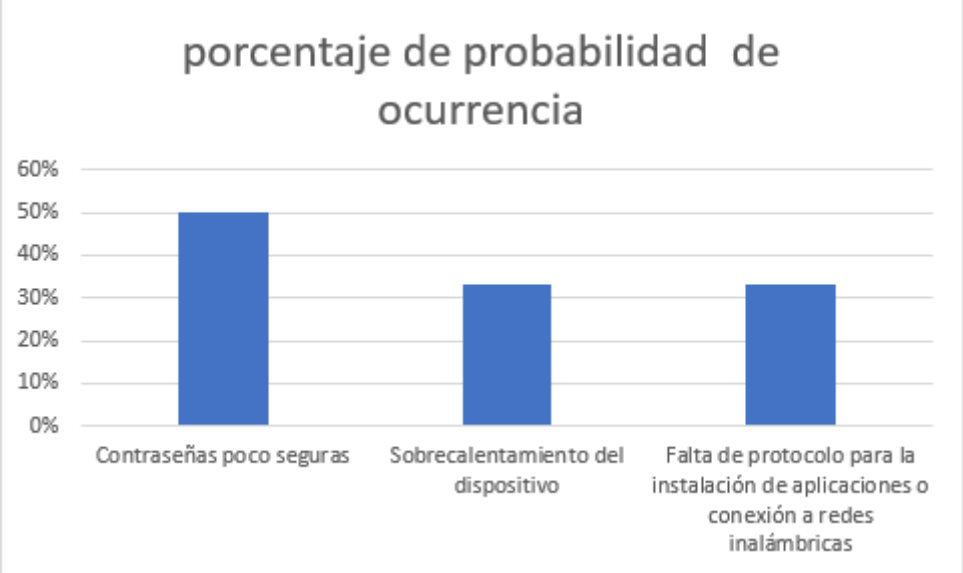
Tabla 21 Tabulación de resultados de vulnerabilidades y amenazas

Tabulación de resultados Auditoría

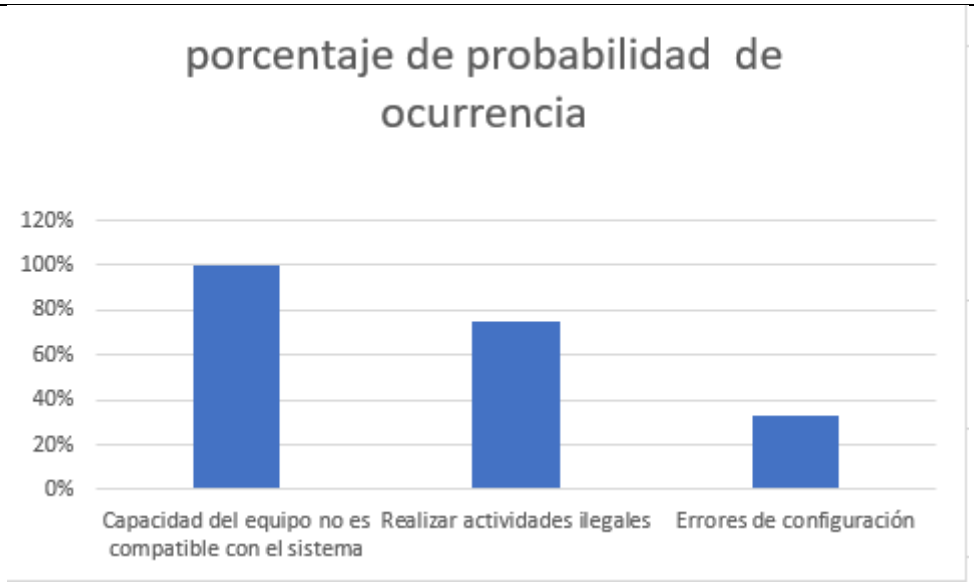
Activo Pc's			
Vulnerabilidades			**Orden %**
1	Falta de mantenimiento	**V2**	**60%**
3	Seguridad deficiente para inicio de sesión	**V1**	**50%**
2	Poco almacenamiento	**V2**	**33%**



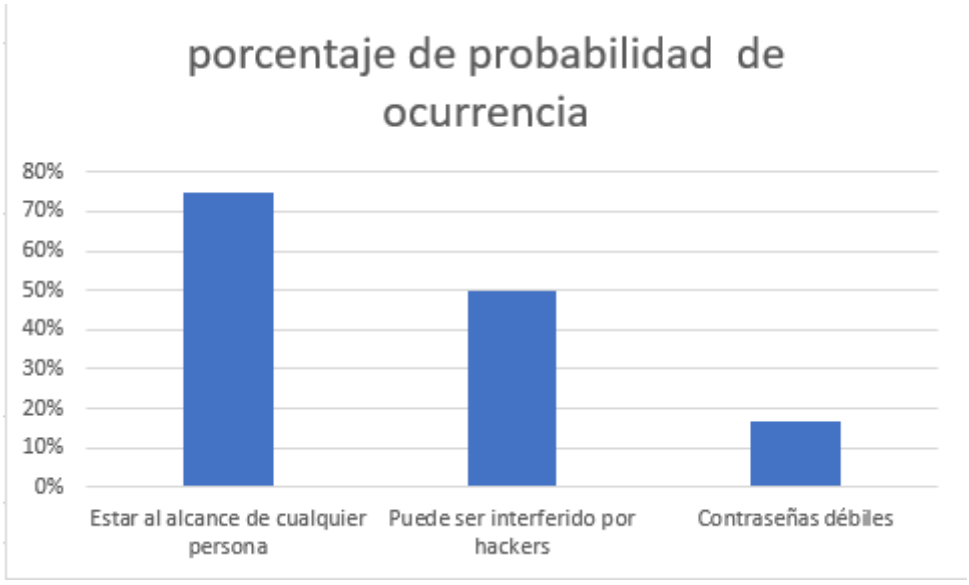
Activo Smartphone			
Vulnerabilidades			**Orden %**
1	Contraseñas poco seguras probabilidad	**V2**	**50%**
2	Sobrecalentamiento del dispositivo	**V3**	**33%**
3	Falta de protocolo para la instalación de aplicaciones o conexión a redes inalámbricas	**V1**	**33%**



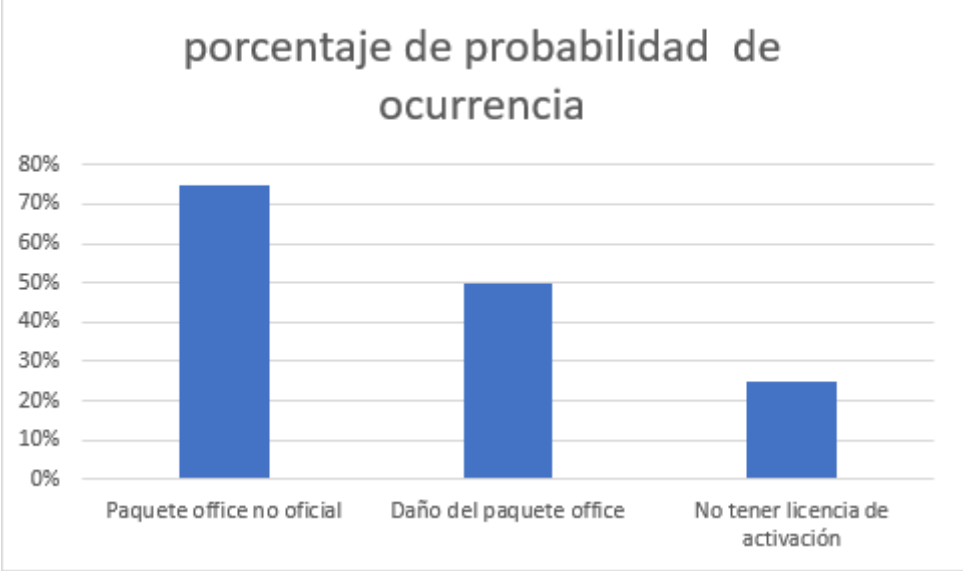
Activo Sistema Operativo			
Vulnerabilidades			**Orden %**
1	Capacidad del equipo no es compatible con el sistema	**V1**	**100%**
2	Realizar actividades ilegales	**V2**	**75%**
3	Errores de configuración	**V3**	**33%**



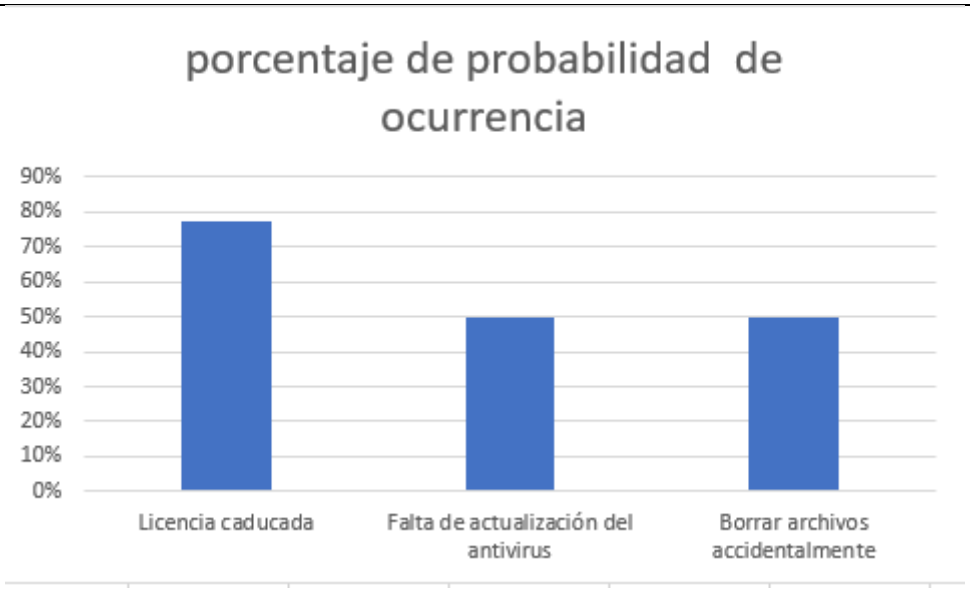
Activo Router			
Vulnerabilidades			**Orden %**
1	Estar al alcance de cualquier persona	**V2**	**75%**
2	Puede ser interferido por hackers	**V1**	**50%**
3	Contraseñas débiles	**V3**	**17%**



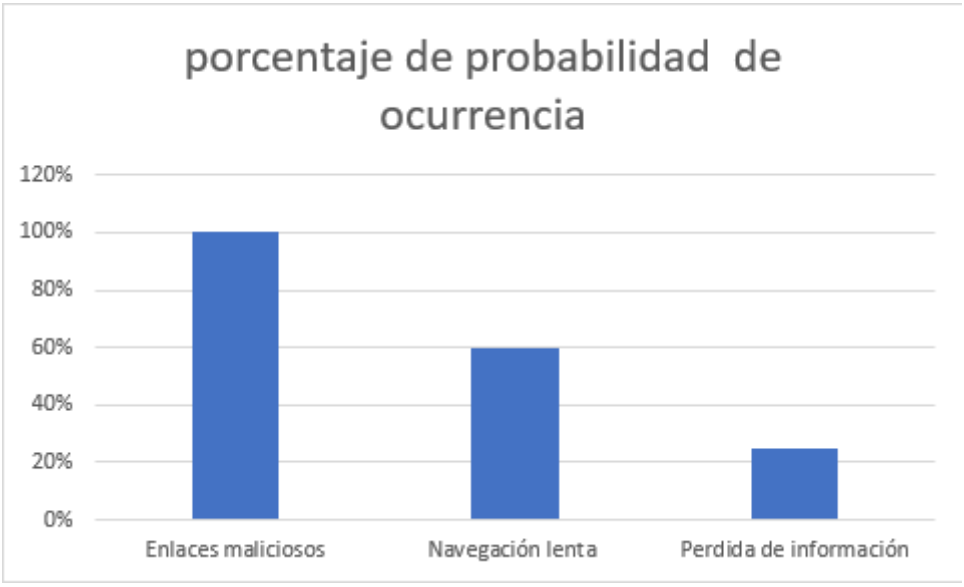
Activo Paquete Office			
Vulnerabilidades			**Orden %**
1	Paquete office no oficial	**V1**	**75%**
2	Daño del paquete office	**V3**	**50%**
3	No tener licencia de activación	**V2**	**25%**



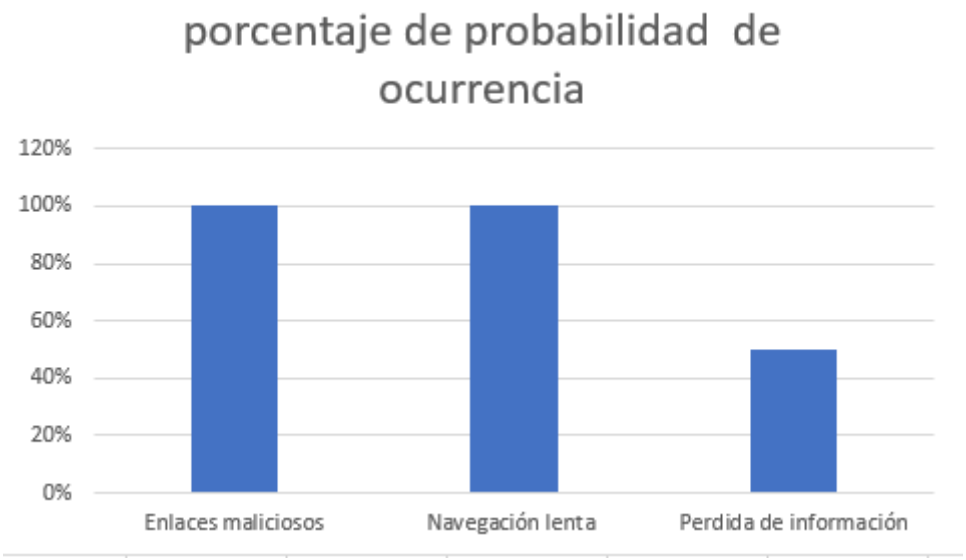
Activo Antivirus			
Vulnerabilidades			**Orden %**
1	Licencia caducada	**V2**	**77%**
2	Falta de actualización del antivirus	**V1**	**50%**
3	Borrar archivos accidentalmente	**V3**	**50%**



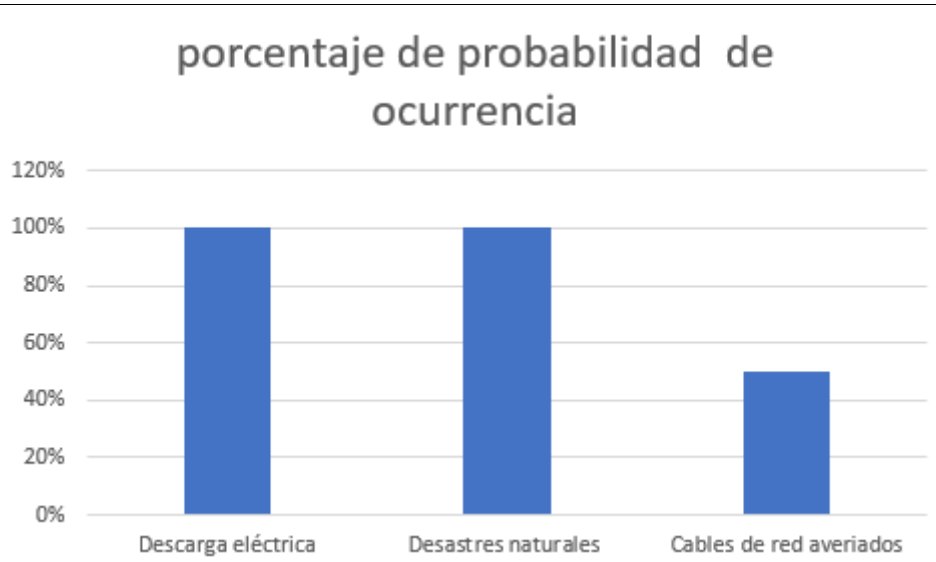
Activo Navegador Web			
Vulnerabilidades			**Orden %**
1	Enlaces maliciosos	**V2**	**100%**
3	Navegación lenta	**V3**	**60%**
2	Perdida de información	**V1**	**25%**



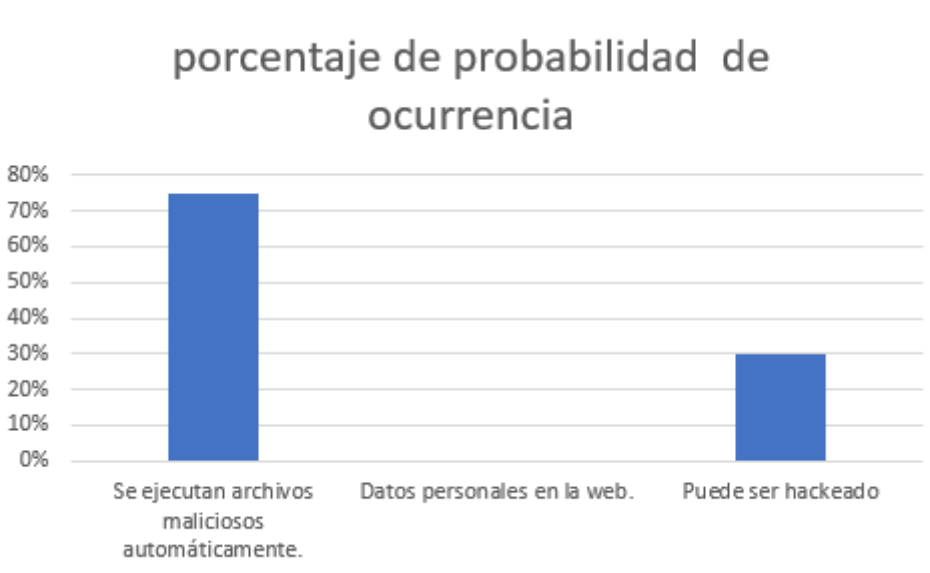
Activo Servicio de correo electrónico			
Vulnerabilidades			**Orden %**
1	Enlaces maliciosos	**V1**	**100%**
3	Navegación lenta	**V2**	**100%**
2	Perdida de información	**V3**	**50%**



Activo Red Cableada			
Vulnerabilidades			**Orden %**
1	Descarga eléctrica	**V1**	**100%**
3	Desastres naturales	**V3**	**100%**
2	Cables de red averiados	**V2**	**50%**



Activo Servicio Web			
Vulnerabilidades			**Orden %**
1	Se ejecutan archivos maliciosos automáticamente.	**V3**	**75%**
3	Datos personales en la web.	**V2**	**66.67%**
2	Puede ser hackeado	**V1**	**30%**



Activo Servicio de Internet			
Vulnerabilidades			**Orden %**
1	Falla eléctrica	**V1**	**100%**
2	Desastres naturales	**V2**	**100%**
3	Equipos de bajo rendimiento	**V3**	**63%**

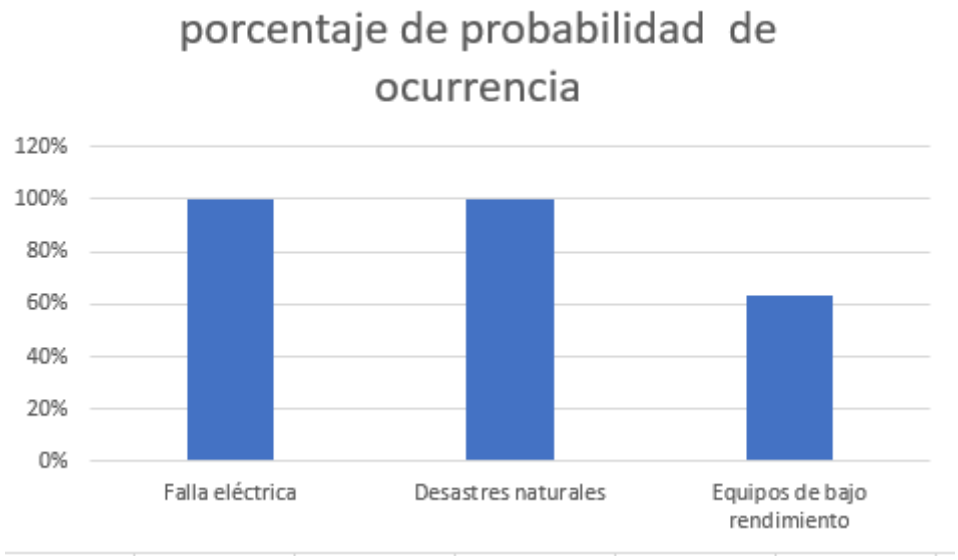
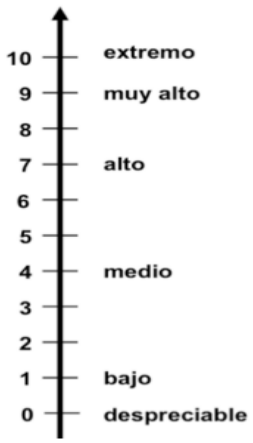


Tabla 22Tabulación de resultados Auditoría

4.8.4 Identificación de riesgos



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Ilustración 8 Valoración de riesgos

0-3	El riesgo es BAJO	El riesgo debe ser estudiado e implementar medidas de seguridad de la información para evitar su desarrollo e impacto.
4-8	El riesgo es MEDIO	El riesgo es tolerable, debe ser monitorizado y requiere medidas de seguridad de la información para evitar un impacto negativo.
➢ 9	El riesgo es ALTO	El riesgo es grave, requiere medidas de seguridad de la información urgentes.

Tabla 23 Medida de riesgos

La Fórmula que se aplicó para el cálculo de evaluación de riegos es:

Nivel de riesgo= VA(CID)*Nivel de amenaza (NA)*Nivel de vulnerabilidad (NV)

Evaluación de riesgos					**Ref. C**	
No. activo	**Amenazas**	**Vulnerabilidades**	**Evaluación de riesgo**			
			Probabilidad		**Cálculo de evaluación**	**Nivel de riesgo**
			NA	**NV**		
A1	Pérdida o robo de equipos.	Seguridad deficiente para inicio de sesión.	2	2	12	Alto
	Fallas del equipo.	Falta de mantenimiento.	2	2	12	Alto
	Ataque de virus.	Poco almacenamiento.	2	1	6	Medio
A2	Pérdida o robo del dispositivo.	Sobrecalentamiento del dispositivo.	2	2	9,32	Alto
	Mala manipulación.	Contraseñas poco seguras.	2	2	9,32	Alto

Evaluación de riesgos				Ref. C		
No. activo	**Amenazas**	**Vulnerabilidades**	**Evaluación de riesgo**			
			Probabilidad		**Cálculo de evaluación**	**Nivel de riesgo**
			NA	**NV**		
	Fuga de datos.	Falta de protocolo para la instalación de aplicaciones o conexión a redes inalámbricas.	3	3	20,97	Alto
A3	Caída del sistema.	Capacidad del equipo no es compatible con el sistema.	1	1	2	Bajo
	Infección de virus.	Realizar actividades ilegales.	2	1	4	Medio
	Robo de información clasificado.	Errores de configuración.	1	2	4	Medio
A4	Fallas del equipo.	Puede ser interferido por hackers.	1	2	4,66	Medio
	Fácil de hackear.	Estar al alcance de cualquier persona.	2	1	4,66	Medio
	Debilidad en configuración del router.	Contraseñas débiles.	2	3	13,98	Alto
A5	Error de activación.	Paquete office no oficial.	1	1	1,67	Bajo
	Eliminación del usuario agregado.	No tener licencia de activación.	1	2	3,34	Bajo

Evaluación de riesgos					Ref. C	
No. activo	**Amenazas**	**Vulnerabilidades**	**Evaluación de riesgo**			
			Probabilidad		**Cálculo de evaluación**	**Nivel de riesgo**
			NA	**NV**		
	Mal uso del paquete office.	Daño del paquete office.	1	2	3,34	Bajo
A6	Eliminación del antivirus.	Falta de actualización del antivirus.	1	3	5,01	Medio
	Ataque mediante el uso de ingeniería social.	Licencia caducada.	1	3	5,01	Medio
	Eliminación de ficheros importantes para el S.O.	Borrar archivos accidentalmente.	2	3	6,8	Medio
A7	Infección de virus	Perdida de información	2	2	12	Alto
	Actualizaciones falsas	Enlaces maliciosos	2	3	18	Alto
	Suplantación	Navegación lenta	1	3	9	Alto
A8	Ataque de hackers.	Perdida de velocidad de navegación.	1	1	3	Bajo
	Eliminación del correo electrónico.	Contraseñas vulnerables.	1	2	6	Medio

Evaluación de riesgos					Ref. C	
No. activo	**Amenazas**	**Vulnerabilidades**	**Evaluación de riesgo**			
			Probabilidad		**Cálculo de evaluación**	**Nivel de riesgo**
			NA	**NV**		
	Robo de información confidencial.	Enlaces maliciosos.	1	1	3	Bajo
A9	Daño intencionado en el cable	Descargas eléctricas	3	3	18	Alto
	Mal estado del cable	Desastres naturales	2	3	12	Alto
A10	Anuncios automáticos	Puede ser hackeado	1	1	2,33	Bajo
	Paginas no seguras	Datos personales en la web	1	2	4,66	Medio
	Navegador no configurado	Se ejecutan archivos maliciosos automáticamente.	2	2	9,32	Alto
A11	Corte del servicio	Falla eléctrica	1	1	2,33	Bajo
	Divulgación de información	Desastres naturales	1	2	4,66	Medio
	Fallos en los enlaces de comunicación	Equipo de bajo rendimiento	2	1	4,66	Alto

Tabla 24 evaluación de riesgos

4.9 Manual de usuario

Guía

Para prevención de ataques informáticos a los docentes de la ULEAM Extensión El Carmen

Anderson Demera Zambrano

Contenido

Introducción

Esta guía surge a partir de las vulnerabilidades investigadas durante la ejecución de la auditoría, por lo que se sugiere implementar tips o consejos para mantener una mayor seguridad; tras el estudio realizado se pudo notar que dentro de la institución no todos los docentes están capacitados para desenvolverse ante alguna amenaza informática.

A continuación, se definirán las principales sugerencias que se deben tomar en cuenta para ser aplicadas en sus equipos informáticos y así poder brindar una mayor seguridad a su información, el objetivo es que esta guía pueda ser revisada por los docentes de la institución, aun mas por los que no pertenecen a la carrera de informática que son los que más vulnerabilidades presentan.

Objetivo de la guía

Fortalecer los conocimientos acerca de los ataques informáticos y métodos de prevención a los docentes de la ULEAM Extensión El Carmen.

Alcance

Esta guía de usuario está enfocada a los docentes universitarios, ya que la seguridad hoy en día es uno de los factores más importantes dentro de la informática, sin embargo, no todos los docentes de la institución están al tanto de todas técnicas que pueden aplicar a sus equipos informáticos para brindarle una mayor seguridad.

También se espera los estudiantes puedan hacer uso de esta guía, ya que es un documento generalizado y de igual ayuda tanto para profesionales como para estudiantes en formación, esperando ayude a la prevención de ataques informáticos y uso de buenas prácticas de seguridad informática.

1.1 Principales tips para evitar un ataque informático

- Mantener el sistema operativo y el navegador actualizados.

En el caso de la infección de dispositivos, los virus aprovechan los fallos del sistema operativo y del navegador. Los fabricantes responden actualizando los programas para solucionar los problemas. Activar las actualizaciones automáticas del sistema operativo, el navegador, los complementos del navegador y otros programas es la mejor forma de mantenerse a salvo.

- Proteger las contraseñas.

Debes estar seguro de que la página en la que las introduces es la correcta, porque las estafas de phishing suelen parecer sitios web reales. Evite utilizar la misma contraseña en muchos servicios, porque si alguien consigue acceder a uno, puede acceder rápidamente a todos ellos. Las credenciales no deben compartirse nunca con nadie, aunque digan pertenecer al equipo de asistencia técnica; las empresas de confianza nunca solicitarán tus contraseñas de forma proactiva.

- Precaución en la web.

Es importante mantener la mente abierta, porque no todo lo que se publica en Internet es necesariamente cierto. En caso de duda, confirme los datos con otras fuentes fiables. Evite hacer clic en enlaces sospechosos. Cuando navegue, lea el correo electrónico, reciba mensajes instantáneos o utilice las redes sociales, tenga cuidado antes de hacer clic en cualquier enlace. Los mensajes falsos que los acompañan pueden ser muy convincentes para llamar la atención del usuario y conducirle a páginas dañinas.

- Ser precavido en lo que descargas.

No se apresure a descargar nada porque constantemente aparecen nuevas amenazas que no pueden ser detenidas por los antivirus. Es esencial descargar programas y datos únicamente de sus páginas web oficiales.

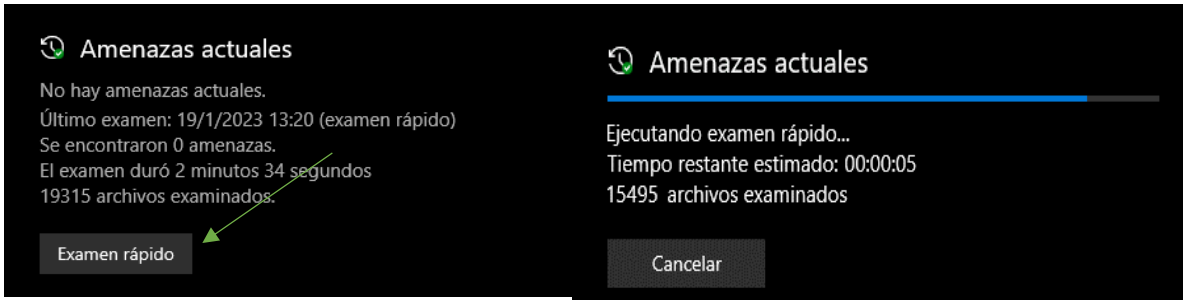
- Utilizar un antivirus que analice todas las descargas.

Asegúrese de que su sistema se analiza periódicamente en busca de malware y de que su software antivirus está actualizado e instalado.

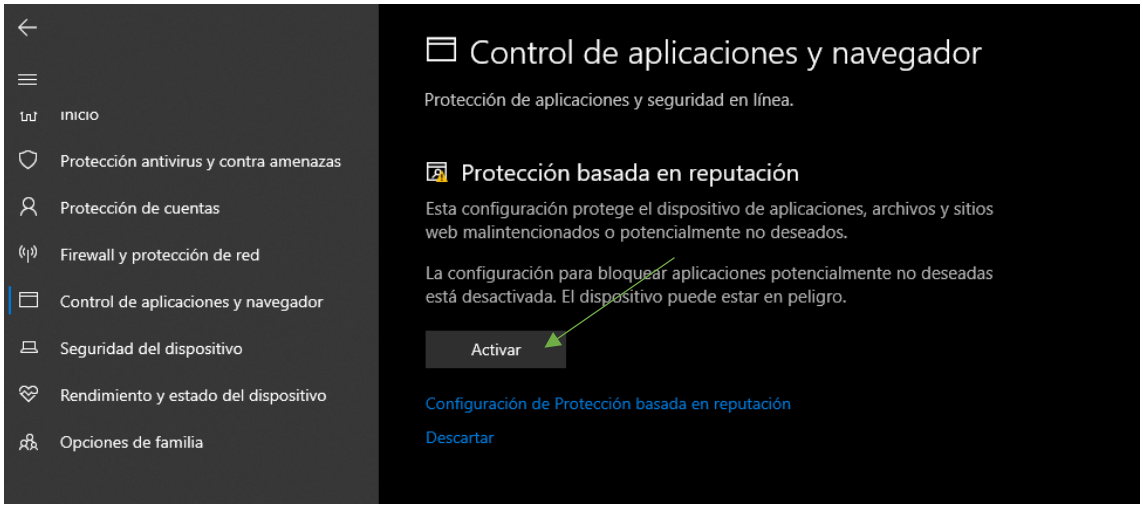
1.2 Protección

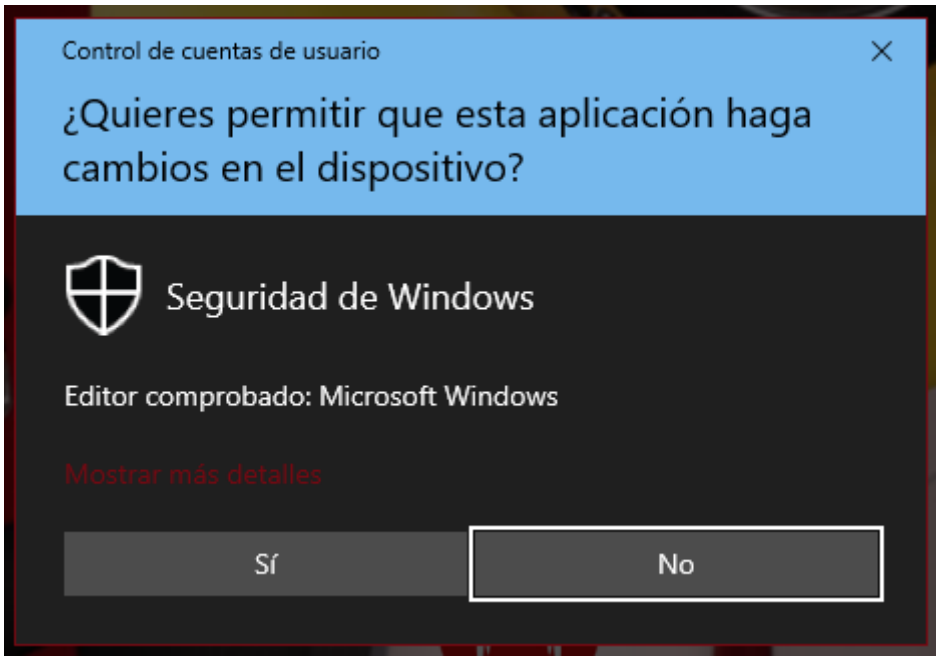
Es importante que a sus equipos se les brinde un mantenimiento periódicamente, por lo cual es fundamental tener instalado un antivirus en su ordenador, ya sea el que viene por defecto u otro de preferencia.

Una vez en el antivirus, se procede hacer un análisis rápido, esto con el fin de detectar algún tipo de archivo dañino.



Otra opción que puede ser muy útil en el antivirus que viene por defecto, es el control de aplicaciones y navegadores.

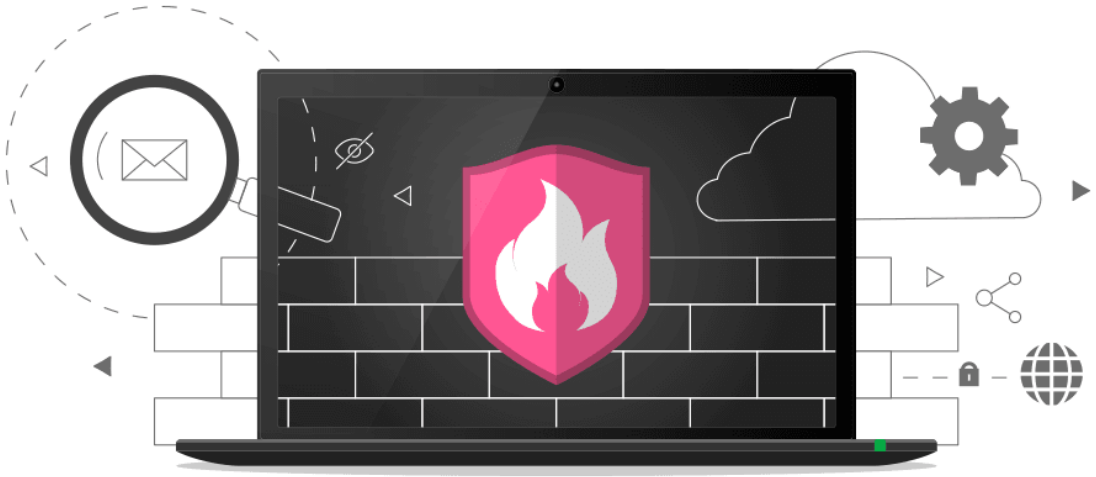




1.3 Firewall

Es importante tener activados los firewalls en tu equipo informático, ya que ayuda a brindar mayor seguridad dentro de la red, impidiendo que intrusos puedan penetrar la barrera de protección que brinda un firewall.

En caso de no tener, puedes acceder a internet, existen firewall que son gratuitos y puedes obtener funciones que son realmente de veneficio para proteger tu equipo.

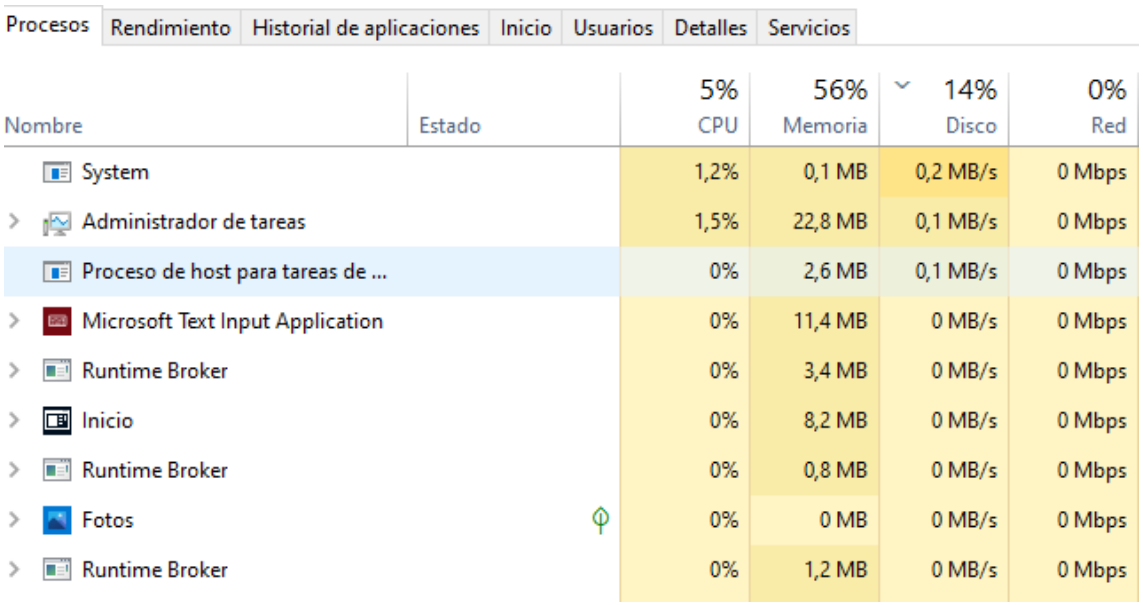


Un cortafuegos es un tipo de sistema de seguridad de red que hace un seguimiento de todo el tráfico que entra y sale de las redes y actúa como sistema de detección de intrusos para detener los ataques.

Esta tecnología puede desplegarse como software en un ordenador o como cortafuegos basados en hardware, que a menudo se ejecutan en dispositivos especializados y protegen redes

enteras contra los piratas informáticos. Aunque estos últimos suelen ser mejores para frustrar los intentos de infiltración, también son bastante más caros y considerablemente más complejos que los cortafuegos de software, que suelen ser gratuitos.

1.4 Sobrecalentamiento del dispositivo



Se debe a que se usan ejecutando demasiadas aplicaciones de manera simultánea y si su equipo informático no es de muy buenos recursos esto hace que se sobrecaliente y se quede la pantalla congelada, en un intento por hacerla reaccionar nuevamente puede llegar hacer cosas involuntariamente lo que puede provocar que se ejecuten archivos involuntariamente.

Como recomendación si su equipo no es de buenos recursos utilice solo las aplicaciones necesarias.

1.5 Seguridad deficiente para el inicio de sesión

Es necesario utilizar contraseñas que cumplan con los parámetros suficientes para ser una contraseña segura, para esto debe cumplir los siguientes parámetros.

- Crear contraseñas de la menos 8 o más caracteres.
- Mezclar mayúsculas y minúsculas.
- Mezclar letras y números.
- No utilizar datos personales como (identificación, fechas importantes, iniciales u otro dato personal)

1.6 Recuerde utilizar una contraseña segura pero fácil de recordar.

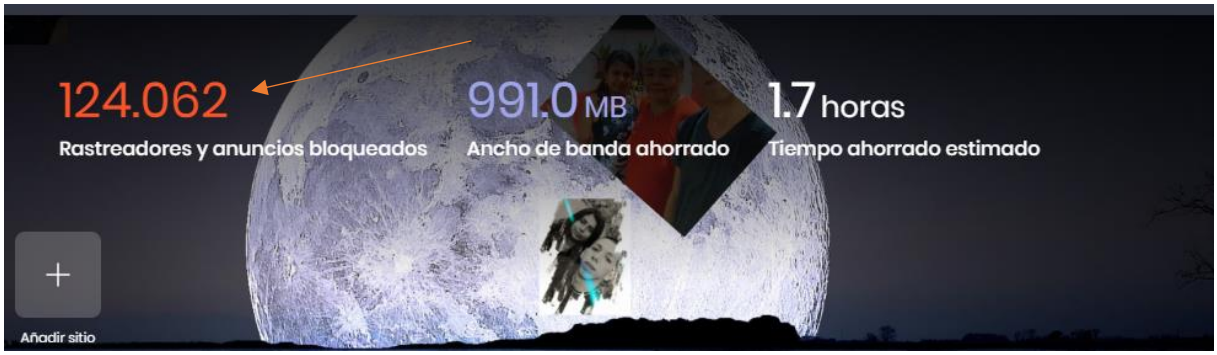
Falta de protocolos para la instalación de aplicaciones.

Verificar las páginas de donde se descargan cualquier tipo de software, ya sea para uso personal o académico, pueden abrirse enlaces donde se pueden descargar de manera automática cualquier tipo de virus, estos pueden robar tu información o infectar todo tu ordenador, dañando la información y haciéndola inaccesible.

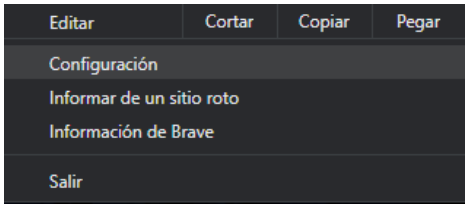
Se recomienda hacer uso de páginas oficiales, brindan mayor seguridad al usuario quien las va a utilizar.

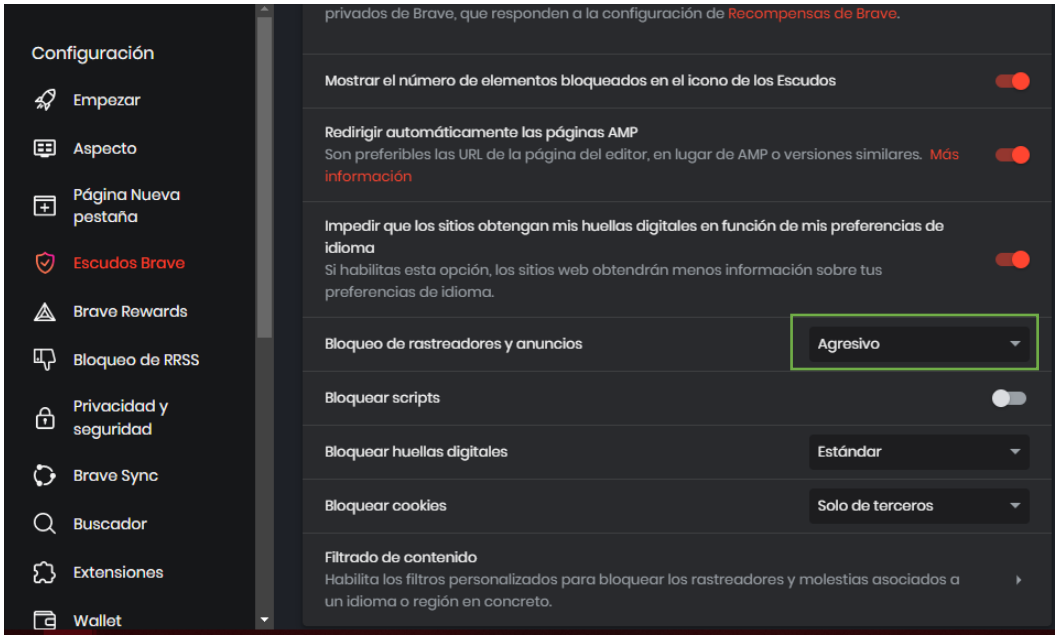
1.7 Navegador web

Los navegadores webs son muy importantes, pero no todos brindad la seguridad necesaria a un usuario al momento de navegar en el Internet, por lo que se debe ter cuidado, suelen ser una de las mayores causas por las cuales se infecta un dispositivo informático, actualmente uno de los navegadores que brinda mayor seguridad es Brave, que es un navegador que bloquea rastreadores y anuncios que pueden llegar a ser molestos por la publicidad que tienen y así mismo porque pueden ser anuncios falsos.

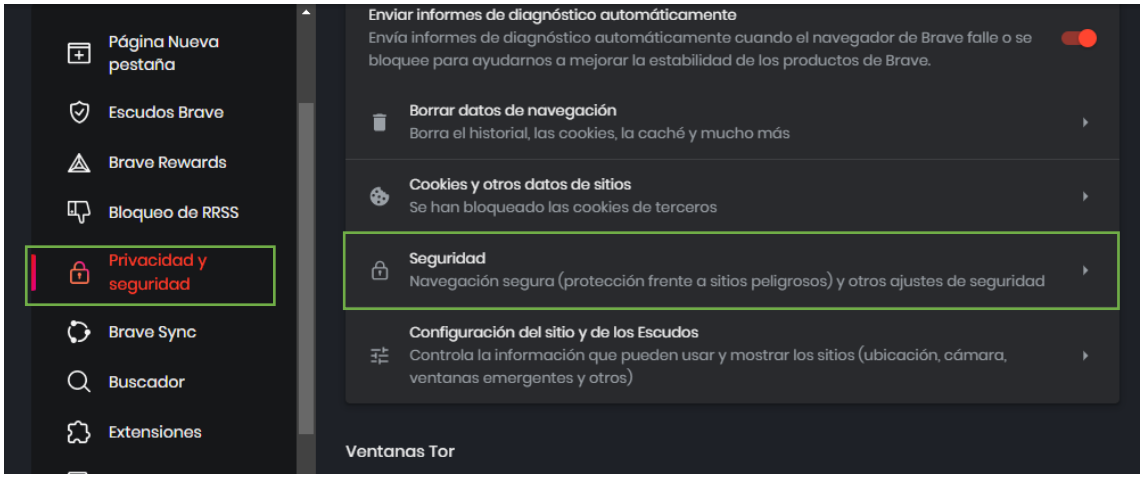


Permite una busqueda limpia, ademas que internamente se puede configurar de mejor manera.

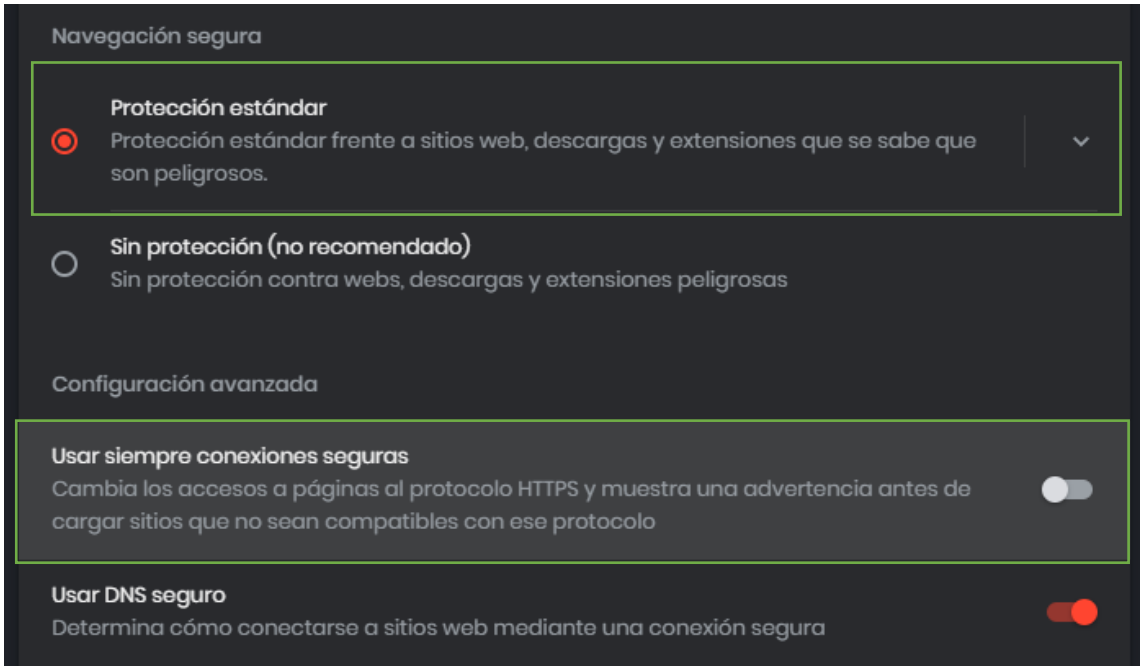




El bloque de anuncios esta por defecto en **estándar** y ponerlo en agresivo para una mejor experiencia y brindar mayor seguridad a su equipo informático.



En el apartado de seguridad y privacidad, se accede hasta la opción de seguridad, para una mayor protección contra sitios peligrosos.



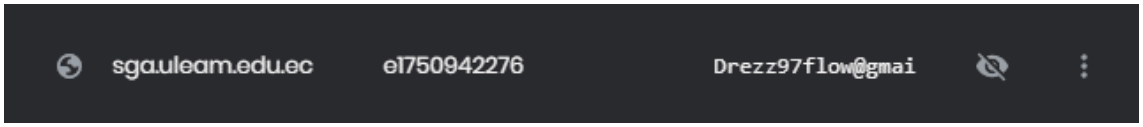
Se deben activar esas opciones, son muy importante, permite brindar al usuario una mayor seguridad al hacer uso del navegador y utilizar páginas webs.

1.8 Contraseñas guardadas en las páginas webs

Es muy frecuente que pase este tipo de percances, ya sea por el temor de olvidar la contraseña o realizar los procesos mucho más rápido, pero guardar las contraseñas en los navegadores es una mala decisión.

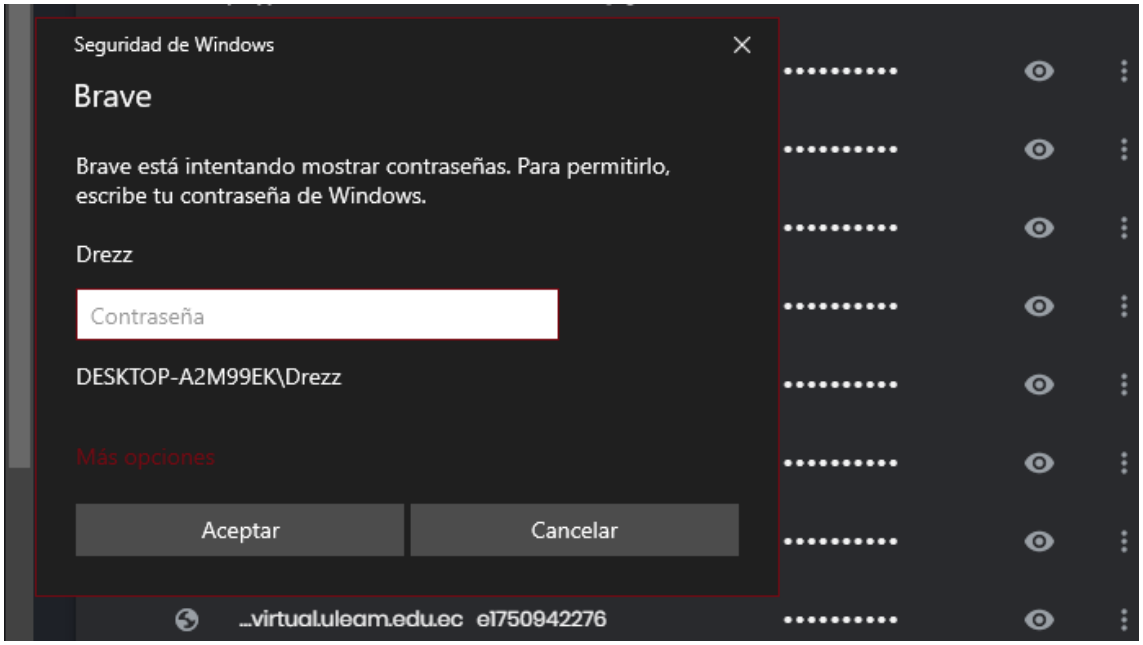
Si un usuario utiliza contraseñas distintas y seguras para cada servicio, la capacidad del navegador para recordar contraseñas puede resultarle muy útil. Sin embargo, en la práctica, los navegadores guardan estas contraseñas en una lista de texto y algunas de ellas ni siquiera están cifradas, lo que las hace vulnerables a los piratas informáticos.

Esto implica que cualquier persona con acceso al ordenador, ya sea un compañero de trabajo, un familiar, un ciberdelincuente que haya robado las credenciales del navegador o incluso un niño, podría buscar estas contraseñas en la configuración del navegador.

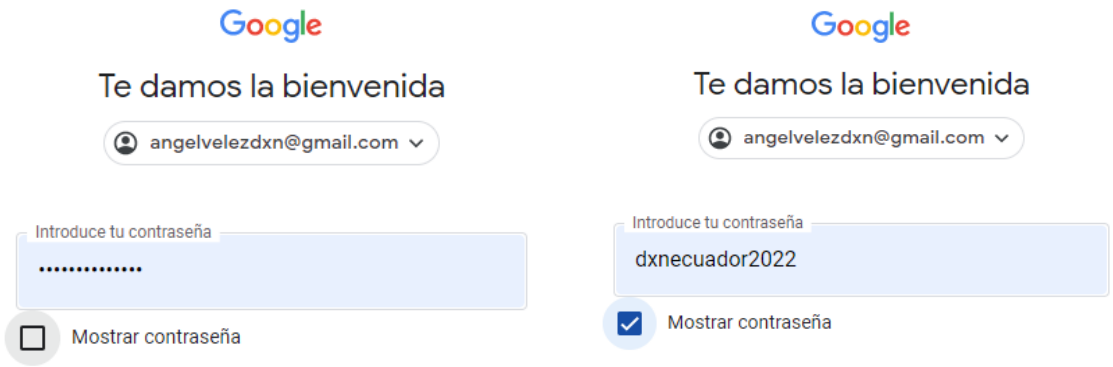


Es muy fácil vulnerar tus contraseñas, así que se recomienda no dejarlas guardadas en los navegadores.

Una de las ventas de Brave es que, en el apartado de contraseñas, para poder visualizarlas debes poner tu clave de inicio de sesión al encender tú equipo, en caso de estar en el celular te pedirá que pongas tu huella dactilar o patrón de desbloqueo.



Sin embargo, aunque esta sea una buena opción no se recomienda guardar contraseñas, ya que, aunque el navegador las oculte, en muchos sitios web se puede visibilizar la contraseña guardada.



1.9 Correo electrónico

- Tipos de correos que debes evitar.

Los correos electrónicos infectados siguen siendo una de las formas más eficientes de distribuir virus informáticos, ya que pueden infectar cualquier máquina moderna cuando se accede a ellos por descuido.

- Un virus disfrazado en correos electrónicos de comercio electrónico.

En este caso se trata del mismo correo electrónico y se comporta de la misma manera que un virus típico: se propaga, atasca servidores y buzones de correo, y con frecuencia contiene virus dañinos que pueden robar nuestra información personal a través de los enlaces incluidos en estos correos electrónicos.

- Un virus disfrazado en correos electrónicos bancarios.

Los falsos correos electrónicos que a diario atascan nuestras bandejas de entrada y las de bancos, entidades de crédito, tarjetas de crédito, etc. Estas alertas, aparentemente inofensivas, avisan al usuario de un bloqueo repentino de su cuenta, del ingreso de cientos de miles de euros (¡pero posiblemente!), de una transacción que puede ser aprobada y de un acceso ilícito desde un PC desconocido.

- Un virus oculto en el archivo adjunto del correo electrónico

Al abrir cualquier tipo de archivo adjunto, archivo ejecutable (.Com,.Exe,.Vbs,.Zip,.Scr,.Dll,.Pif,.Js) o documento de Office corrupto (.Doc,.docx,.pst,.Dot,.xls,.xlt) se iniciará la infección, dejándole sin poder hacer nada más que

ver cómo sus archivos personales se bloquean o corrompen El mejor método para prevenirlos es ser precavido al abrir archivos adjuntos de correo electrónico, especialmente si no sabemos quién los envía. Simplemente elimine el correo electrónico o márquelo como spam para estar seguro si no reconoce al remitente y el texto del correo es dudoso o está escrito en inglés.

- Un virus escondido en el cuerpo del mensaje.

Incorporando virus en el cuerpo de los mensajes de correo electrónico es como se propagan a través del correo electrónico. Ni siquiera es necesario hacer clic en enlaces o archivos adjuntos, basta con abrir el correo electrónico y dejar que el simple código HTML, el lenguaje de programación de sitios web, cargue material multimedia como imágenes- para iniciar una infección en el ordenador.

CAPITULO V

5 Evaluación y resultados

5.1 Introducción

Una evaluación de resultados es la herramienta que permite identificar los problemas actuales o anticipar otros nuevos. Para poder crear planes que beneficien y mejoren, una evaluación adecuada debe incluir información detallada sobre los procesos que se ejecutan de manera incorrecta.

Se hace una presentación de los datos obtenidos durante la ejecución de la auditoria, aplicada a los equipos informáticos de los docentes de la ULEAM, Extensión en El Carmen. En base a los resultados obtenidos y los hallazgos donde se determina los parámetros que se incumplen y no permiten brindar la seguridad necesaria.

Se describe también en este capítulo el manual de usuario que se deberá seguir para brindar a los docentes un mejor uso de las buenas prácticas para seguridad informática, también se hace una interpretación objetiva de los resultados que se obtuvieron en la auditoría, y posteriormente se pasa a las conclusiones y recomendaciones.

5.2 Presentación y monitoreo de resultados

5.2.1 Hallazgos

Auditoría Informática con Norma ISO/IEC 27002	**Ref. Pt1**
Hallazgo No. 01	Contraseñas de acceso incumplen parámetro para ser contraseñas seguras.
Descripción	Los equipos informáticos, dispositivos móviles y correos electrónicos considerados como activos importantes, no cumplen con los parámetros determinados para una contraseña segura.
Consecuencia	Personas no autorizadas podrían abusar de estas herramientas, lo que podría repercutir en los programas u otras actividades de los docentes.
Recomendación	Poner contraseñas más seguras en los inicios de sesión, que sean consideras complejas.

Tabla 25 hallazgo 1

Auditoría Informática con Norma ISO/IEC 27002	Ref. Pt2
Hallazgo No. 02	El mantenimiento de los equipos no es el requerido.
Descripción	No realizar una limpieza frecuente mediante un antivirus puede generar que algún documento se infecte de virus y dañe los demás archivos obstaculizando las funciones normales de los docentes.
Consecuencia	Personas no autorizadas podrían abusar de estas vulnerabilidades, lo que podría repercutir en los programas o tareas de los alumnos además de otras actividades de los docentes.
Recomendación	Eliminar archivos que no se necesiten, subir en una nube, realizar escáner con el antivirus.

Tabla 26 hallazgo 2

Auditoría Informática con Norma ISO/IEC 27002	Ref. Pt3
Hallazgo No. 03	Protocolos para instalación de aplicaciones no son seguros.
Descripción	Las personas no tienes conocimientos de todos los riegos que se corren al instalar aplicaciones sin medidas de seguridad.
Consecuencia	El dispositivo puede estar vulnerable a ataques de virus, perdida de información o hackeos.
Recomendación	Se recomienda descargar las aplicaciones o programas siempre de sitios que sean oficiales y seguros.

Tabla 27 hallazgo 3

Auditoría Informática con Norma ISO/IEC 27002	Ref. Pt2
Hallazgo No. 04	Protocolos para uso de la web no son los apropiados.
Descripción	Se puede navegar sin precauciones adecuadas, corriendo los riegos de infectarse de virus, o hacer que se vuelva lenta la respuesta del computador.

Consecuencia	Pérdida de información al realizarse este tipo de actos, puede ser suplantado y realizar acciones que perjudican al usuario, si el equipo es de bajo rendimiento puede ser aún peor las consecuencias
Recomendación	Existen diversos tipos de almacenamiento en la nube para alojar la información que menos se necesite, así poder hacer un mejor uso de los equipos informáticos.

Tabla 28 hallazgo 4

Auditoría Informática con Norma ISO/IEC 27002	**Ref. Pt3**
Hallazgo No. 05	Protocolos de cuidado de la red física puede que no sean eficientes.
Descripción	los cables de conexión pueden ser averiados a causa de la inmadures de las personas que lo hacen con malas intenciones.
Consecuencia	Se puede infectar la red de internet dentro de la institución ya que cualquiera puede conectarse desde las redes físicas.
Recomendación	Se recomienda tener mayor protección en las conexiones, y cuidados en las extensiones de cables distribuidas dentro de la institución.

Tabla 29 hallazgo 5

5.3 Interpretación objetiva

Existen muchas falencias en la seguridad de la información, el principal motivo es el avance de la tecnología y las personas que hacen usos de herramienta para acciones mal intencionadas, por lo que se debe tener medidas de seguridad más eficientes. Después de haber realizado el análisis de los activos se puede deducir que no se hace uso de prácticas para la seguridad de la información.

De acuerdo con la investigación realizada, muchos docentes desconocen acerca de los tantos virus informáticos que existen y que se pueden encontrar en todos lados mientas se hace uso de un ordenador u otro dispositivo conectado a la red de internet, tampoco se tienen las medidas necesarias para cuando se hace la instalación de un software, ya que se desconoces de los riesgos que corren a utilizar programas piratas.

Por otra parte, se ignora en gran parte las vulnerabilidades que se pueden presentar al dejar sus datos guardados en los navegadores, esto puede ser un problema grave por todos riesgos informáticos que implica, así mismo, no se hace el correcto mantenimiento de los equipos informáticos, ya que basado en los instrumentos aplicados se da a notar que no se hacen análisis concurrentemente.

Existen docentes de la universidad Laica Eloy Alfaro de Manabí Extensión El Carmen que han padecido bajo una amenaza informática entre las más comunes los malwares, por lo que es necesario estar alertas antes cualquier vulnerabilidad que exista o se detecte, para así poder resolver el problema de la mejor manera posible, siempre priorizando la integridad, disponibilidad y confidencialidad de la información.

CAPITULO VI

Conclusiones

La seguridad de los equipos informáticos es muy importante, ya que son una de las principales herramientas de los docentes para sus labores diarias, hoy en día la ciberseguridad debe ser un factor primordial dentro de la institución, sin embargo, no se les da el mantenimiento necesario, ni se tienen las precauciones apropiadas para prevenir cualquier tipo de ataque informático.

Mediante la información obtenida a través de los instrumentos de recolección de datos se puede denotar que la gran mayoría de docentes no sabrían identificar un ataque malicioso en sus equipos, tampoco se tiene precaución con la seguridad de la información que tienden en sus ordenadores, ya que se encuentran muchas falencias, una minoría tiene mayor precaución en este ámbito, lo que se puede deducir que son docente de la carrera en informática.

Es importante siempre mantener los equipos informáticos protegidos ante cualquier circunstancia, es importante la evaluación de resultados porque los hallazgos encontrados ayudan a hacer un mejor uso de las buenas prácticas de seguridad informática permitiendo mejorar los estándares de seguridad y mitigar las vulnerabilidades existentes.

Recomendaciones

Los docentes de la ULEAM deben tener mayor precaución con sus equipos informáticos, ya que hoy en día la seguridad es muy vulnerable, esta investigación no erradica los riesgos que existen, pero ayuda a disminuirlos y depende de los docentes lograr la mayor eficacia posible.

Hacer uso del manual de usuario que se desarrolló en esta investigación para brindar una mayor seguridad a sus equipos informáticos y así, poder brindar mayor integridad, confidencialidad e integridad a su información.

Al decano que en las capacitaciones que se les da a los docentes hacer mayor énfasis en el área de seguridad informática, porque pueden presentarse problemas a partir del desconocimiento en el tema, también porque existen muchos docentes que presentan inconvenientes informáticos.

Anexos

Ilustración 9 Aplicación de entrevista

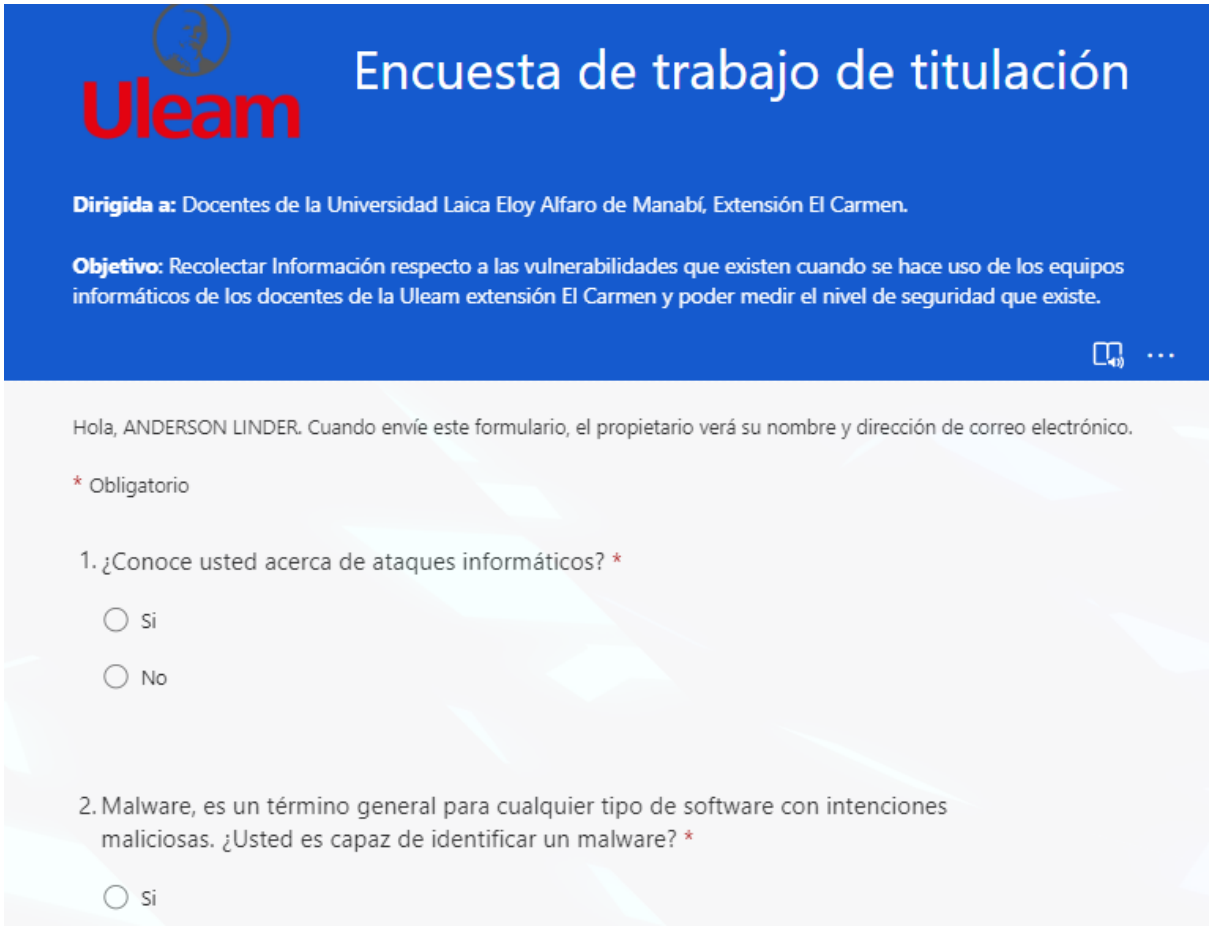


Ilustración 10 Aplicación de encuesta

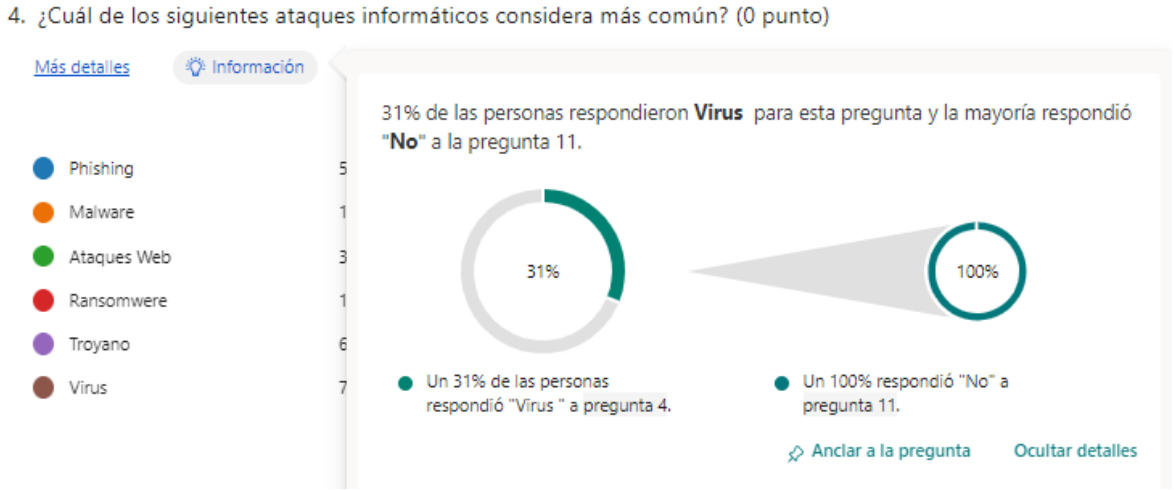
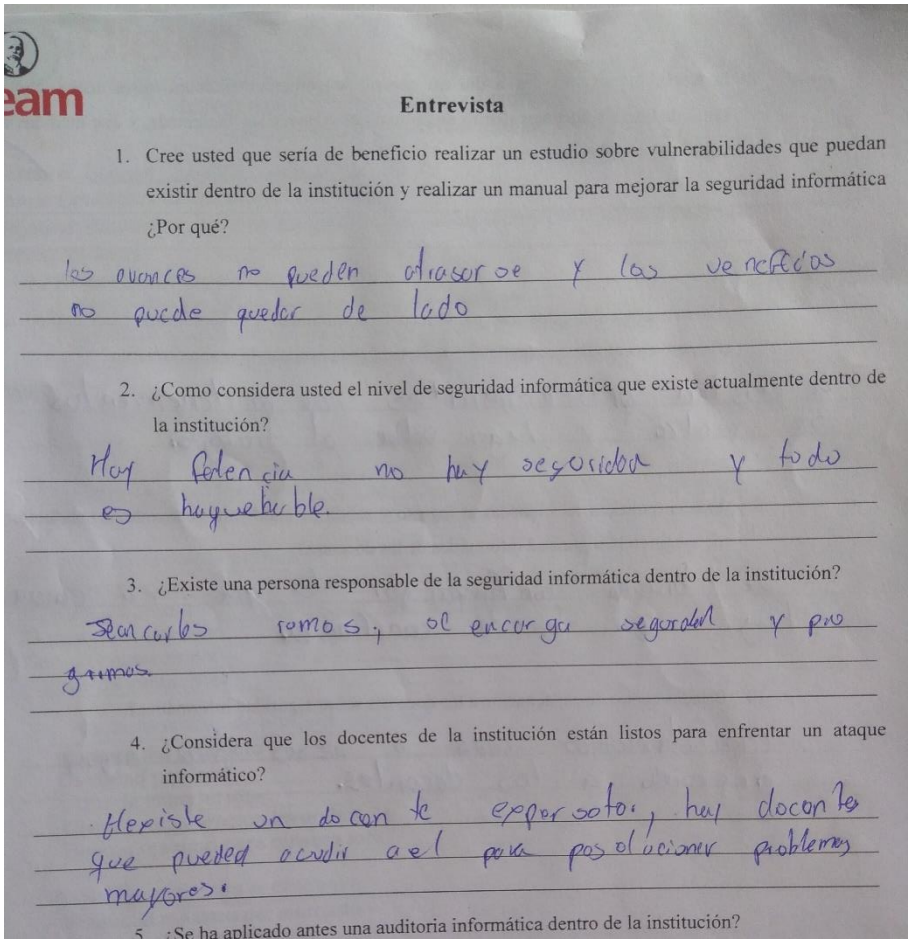


Ilustración 11 Tabulación de encuestas



Entrevista

1. Cree usted que sería de beneficio realizar un estudio sobre vulnerabilidades que puedan existir dentro de la institución y realizar un manual para mejorar la seguridad informática ¿Por qué?

los avances no pueden atrasarse y los vencidos no puede quedar de lado

2. ¿Como considera usted el nivel de seguridad informática que existe actualmente dentro de la institución?

Hay ferencia no hay seguridad y todo es hackeable.

3. ¿Existe una persona responsable de la seguridad informática dentro de la institución?

Encargados somos, el encargado seguridad y programas.

4. ¿Considera que los docentes de la institución están listos para enfrentar un ataque informático?

Hexiste un docente especifico, hay docentes que pueden acudir a el para posibles problemas mayores.

5. ¿Se ha aplicado antes una auditoria informática dentro de la institución?

Ilustración 12 Encuesta al decano de la Uleam

Glosario

Activo

Es cualquier información, hardware, software u otro elemento del entorno que soporta actividades relacionadas con la información.

Auditoría

Encontrar pruebas pertinentes es un proceso metódico, independiente y documentado. Básicamente, auditar es analizar algo objetivamente para ver si se han cumplido los requisitos administrativos o si sus estados financieros son legítimos.

Cortafuegos

Es un sistema cuya finalidad es proteger nuestra red privada de los asaltos de otras redes denegando el acceso e impidiendo las invasiones

Ecuánime

es un adjetivo que permite nombrar a aquel que tiene ecuanimidad. Este término, por su parte, hace referencia a la imparcialidad.

Escala de Likert

Es un método de medición que, a diferencia de las preguntas binarias, permite medir características cualitativas de la encuesta.

Extorsión

Acto ilícito en el que el autor coacciona a la víctima para que haga algo en contra de su voluntad.

Gadgets

Dispositivo con un propósito y una función claros que es práctico y único al mismo tiempo, normalmente de pequeñas dimensiones.

Génesis

Principio u origen de algo; génesis también puede referirse a una serie de circunstancias que dan lugar a un resultado determinado.

ISO

Organización Internacional para la Estandarización

ISO tools

Instrumento técnico eficaz que dota a las organizaciones de una gestión automatizada, les permite cumplir sus compromisos de mejora y aporta soluciones a sus demandas reales.

Magerit

Es una metodología a disposición del público, de uso abierto y que no necesita autorización previa.

Malware

Un programa malicioso es cualquier tipo de software que, a sabiendas, causa daños en un sistema informático. A menudo se denomina malware, programa o código malicioso.

PHVA

Planear, hacer, verificar y actuar.

SGSI

sistema de gestión de la seguridad de la información.

Sofisticado

En informática, algo así como "han identificado un virus muy inteligente en su diseño" o "es algo particularmente exquisito o refinado" oculto en los ordenadores, incluida su ejecución".

TIC

tecnologías de la información y la comunicación

Uleam

Universidad Laica Eloy Alfaro de Manabí

WPA2

Una tecnología de seguridad Wi-Fi llamada WPA2 protege las comunicaciones inalámbricas. Salvaguardan tus conversaciones, mantienen tus datos en secreto y disuaden a los piratas informáticos de acceder a tu red.

Bibliografía

Ahamah Levy, T. (2019). *LA ENTREVISTA Y LA ENCUESTA.* Mexico. Obtenido de https://www.scielosp.org/pdf/spm/2019.v61n5/678-684/es

Arguezo Ramirez, E. (2019). *PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD.* Perú. Obtenido de http://repositorio.udh.edu.pe/handle/123456789/2084

Bravo Indacochea, G., & Barrera Landires, F. (2020). *Auditoría de seguridad informática en la red de datos de una empresa utilizando como mecanismo de hacking ético el sistema operativo kali linux previo a la propuesta de implementación del firewall PFSENSE y correlacionador de eventos SIEM.* Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones. Obtenido de http://repositorio.ug.edu.ec/handle/redug/48851

Cabrejos Torres, R. (2020). *Influencia de la metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC.* Chiclayo - Perú. Obtenido de https://hdl.handle.net/20.500.12802/7573

Calderón Carrasco, C., & Ocaña Aldaz, D. (2014). Artículo Científico - Auditoría informática basada en el análisis de riesgos a la empresa Tecniseguros S.A. *Repositorio Dspace*, 9. Obtenido de http://repositorio.espe.edu.ec/handle/21000/9693

De Santiago Bartolomé, I. (13 de Agosto de 2019). *ANÁLISIS DE MAGERIT Y PILAR.* Valladolid. Obtenido de https://uvadoc.uva.es/bitstream/handle/10324/37736/TFG-I-1213.pdf?sequence=1&isAllowed=y

Ferrino, A., Regueira, U., & Zapico, M. (2019). 1Actitudes de alumnado preadolescente ante la seguridad digital: un análisis desde la perspectiva de género. *Revista de Educación a Distancia (RED)*. Obtenido de https://revistas.um.es/red/article/view/400811

Figueroa Suárez, J. (14 de Junio de 2022). La seguridad informática y la seguridad de la información. *Polo del conocimiento*, 146-155. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

Gallegos Arrufat, M., Torres Hernandez, N., & Pessoa , T. (01 de Octubre de 2019). Competencia de futuros docentes en el. *Revista Científica de Educomunicación* |. Obtenido de https://digibug.ugr.es/bitstream/handle/10481/58641/Gallego-Competence.pdf?sequence=1&isAllowed=y

Gómez Vieites , Á. (2018). *Auditoría de seguridad informática.* Bogotá: Ediciones de la U. Obtenido de https://books.google.es/books?id=No5dEAAAQBAJ&lpg=PA41&ots=RfAK0BQxm5&dq=seguridad%20informatica&lr&hl=es&pg=PP1#v=onepage&q&f=true

Gómez, E., Duchimaza, J., Ramos, J., & Alejandro, M. (2019). *Plan de contingencia para los equipos informáticos y sistemas informáticos utilizando la metodología magerit.* Santa elena. Obtenido de https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/429/362

Gordón Revelo, D., & Pacheco Villamar, R. (2018). *Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranetde una Institución de Educación Superior.* Guayaquil. Obtenido de http://recibe.cucei.udg.mx/index.php/ReCIBE/article/view/90/84

Guevara Maldonado, C. B. (2017). *DESARROLLO DE ALGORITMOS EFICIENTES PARA.* Madrid.

Gusmán, V. (2019). *Evaluación de seguridad de la información aplicado al sistema de evaluación de docentes de la Universidad Técnica del Norte basado en la ISO 27002:2017 con la metodología magerit V3.* Ibarra- Ecuador. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/9535

Herrero Álvarez, R. (2018). *Seguridad en redes y aplicaciones distribuidas. Programas maliciosos, antivirus,¿ y uso de emuladores de CPU en técnixas de análisis de malware.* Tesis. Obtenido de http://openaccess.uoc.edu/webapps/o2/handle/10609/91026

Imbaquingo, D., Días, J., Saltos, T., Arciniega, S., De La Torre, J., & Jácome, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informacíon*, 427- 440. Obtenido de https://www.proquest.com/scholarly-journals/análisis-de-las-principales-dificultades-en-la/docview/2452331691/se-2

Jácome León , J. G., Pusdá Chulde, M. R., & Imbaquingo Esparza, D. E. (2016). *Fundamentos de Auditoría Informática basada en riesgos.* UNIVERSIDAD TECNICA DEL NORTE. Ibarra-Ecuador: UTN Ibarra-Ecuaor. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/6794

La seguridad informática en sistemas de gestión académica y educativa de las unidades educativas fiscales del cantón Santo Domingo. (2021). (P. Cañizares Galarza, & G. Calazacón Aguavil, Trads.) Santo Domingo. Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/14303

López Suarez, L. (2020). *INVESTIGAR Y DOCUMENTAR ATAQUES INFORMATICOS MAS COMUNES PRESENTADOS A HERRAMIENTAS DE TRABAJO COLABORATIVO EN EL CONTEXTO ORGANIZACIONAL COLOMBIANO.* Bogotá. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/40363/79646670.pdf?sequence=1&isAllowed=y

Matos, A. A. (23 de Octubre de 2020). *Investigación Bibliográfica: Definición, Tipos, Técnicas.* Obtenido de Investigación Bibliográfica: Definición, Tipos, Técnicas: https://www.lifeder.com/investigacion-bibliografica/.

Molina Miranda, M. (Diciembre de 2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. *Espirales revista multidisciplinaria de investigación*, 10. Obtenido de https://scholar.archive.org/work/ovnggnnarnh6vdmlijlryz7xga/access/wayback/http://www.revistaespirales.com/index.php/es/article/download/125/68

Moreno , D. (2018). *TIPOS DE MECANI SMOS PARA LA PROTECCIÓN DE LOS SERVICIOS INFORMÁTICOS Y SUS MODELOS DE SEGURIDAD.* Colombia. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/4928

Palacios-Bayas, R., Bosquez-Barcenes, V., Palacios-Vayas, J., & Camacho-Castillo, L. (2019). *AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN, APLICANDO COBIT 5.* Quito: ISSN Impreso: 1390-8197. doi:https://doi.org/10.33789/talentos.6.2.103

Pallerola Comamala, J., & Monfort Aguilar, E. (2022). *Auditoría Enfoque Teórico - practico.* Bogotá: SB STARBOOK. Obtenido de https://books.google.es/books?hl=es&lr=&id=MI5dEAAAQBAJ&oi=fnd&pg=PA35&dq=auditoria&ots=PDlGMFA1XC&sig=LQovhKYhXHBGK5Npq_0qdSUL-Xw#v=onepage&q=auditoria&f=true

Pazmiño Rosero, D. A. (2020). *Propuesta metodológica para aplicación de auditoría informática en el ciclo de ingresos de empresas de servicios de Guayaquil.* Guayaquil:

Universidad Católica de Santiago de Guayaquil. Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/15192

Postigo Palacios, A. (2020). *Seguridad informática.* España: Ediciones Parininfo. Obtenido de https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=estrategia+de+seguridad+inform%C3%A1tica&ots=-HZZkkaSg3&sig=CPv9eF5h869c8a20HNtv9iiuMrc#v=onepage&q=estrategia%20de%20seguridad%20inform%C3%A1tica&f=true

Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., . . . Castillo Merino, M. (2018). *Introducción a la seguridad Informática y el análisis de vulnerabilidades.* Obtenido de https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=tipos+de+virus+inform%C3%A1ticos&ots=ymvTvTe4Vs&sig=9RPIcGAGj96fUbi5DOrZ10ZhG5w#v=onepage&q=tipos%20de%20virus%20inform%C3%A1ticos&f=true

Saenz Flores, O. (2019). *Auditoría de Sistemas Informáticos.* Moquegua-Perú. Obtenido de http://repositorio.ujcm.edu.pe/handle/20.500.12819/729

Salcedo Díaz , J. (2022). *ESPECIFICACIÓN DE UN MÉTODO QUE AYUDE AL BANCO POPULAR A IDENTIFICAR Y DISMINUIR LA BRECHA DE SEGURIDAD DE SU SOFTWARE ANTIVIRUS.* Bogatá. Obtenido de http://hdl.handle.net/11634/44073

Seid, G. (2016). *Procedimientos para el análisis cualitativo de entrevistas. Una propuesta didáctica.* ISSN 2408-3976. Obtenido de https://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.8585/ev.8585.pdf

Seid, G. (2016). *Procedimientos para el análisis cualitativo de entrevistas. Una propuesta didáctica.* ISSN 2408-3976. Obtenido de https://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.8585/ev.8585.pdf

Sosa, A. (21 de Diciembre de 2018). *Prezi*. Obtenido de https://prezi.com/c3cu3jwuax79/el-metodo-analitico-sintetico/

Torres López , N. (2022). *ESTUDIO COMPARATIVO DE TECNOLOGÍAS DE LA SEGURIDAD INFORMÁTICA PHISHING Y SPOOFING PARA LA DETECCIÓN DE UN ATAQUE INFORMATICO.* Tesis, Babahoyo. Obtenido de http://dspace.utb.edu.ec/handle/49000/11680

ULEAM. (2020). *ULEAM sistema de gestion académica*. Obtenido de https://sga.uleam.edu.ec/auth/module.php/core/loginuserpass.php?AuthState=_ec79628d5ac700f5e296fe0d04632fe557beee61c8%3Ahttps%3A%2F%2Fsga.uleam.edu.ec%2Fauth%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252Fsga.uleam.edu.ec%26cookieTime%3

ULEAM. (2020). *ULEAM sistema de gestion académica*. Obtenido de https://sga.uleam.edu.ec/auth/module.php/core/loginuserpass.php?AuthState=_ec79628d5ac700f5e296fe0d04632fe557beee61c8%3Ahttps%3A%2F%2Fsga.uleam.edu.ec%2Fauth%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252Fsga.uleam.edu.ec%26cookieTime%3

Westrecher, G. (14 de Agosto de 2020). *Definición de técnica* . Obtenido de Conomipedia: https://economipedia.com/definiciones/metodo-deductivo.html

Yana Viveros, W. (2018). *Propuesta de un sistema de gestión de seguridad de la información, aplicando la metodología Magerit para el Gobierno Regional Puno Caso: Proyecto especial Camélidos Sudamericanos – Pecsa, 2017.* Universidad Privada Telesup. Obtenido de https://repositorio.utelesup.edu.pe/handle/UTELESUP/371

Zambrano Zambrano, S., & Vera Mesías, D. (Enero-Abril de 2020). CONTROL DE MANTENIMIENTO PREVENTIVO EN COMPUTADORES A NIVEL DE SOFTWARE. *UNESUM Ciencias*. doi: https://doi.org/10.47230/unesum-ciencias.v4.n1.2020.213