ESCUELA DE INGENIERÍAS

Tema:

CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL

Proyecto de investigación previo a la obtención del título de Ingeniero deTecnologías de la Información y la Comunicación

Línea de Investigación:

Tecnologías de la información y la comunicación

Autor:

Carlos Alonso Santamaría Calucho

Director:

Teresa Milena Freire Aillón, Mg.

Ambato – Ecuador

Octubre 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL

Línea de Investigación:

Tecnologías de la información y la comunicación

Autor:

Carlos Alonso Santamaría Calucho

Teresa Milena Freire Aillon, Ing. f._____

CALIFICADOR

Ricardo Patricio Medina Chicaiza, Ing. f._____

CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. f._____

CALIFICADOR

Santiago Alejandro Acurio Maldonado, Ing. Mg. f._____

DIRECTOR ESCUELA DE SISTEMAS

Hugo Rogelio Altamirano Villaroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Octubre 2022

DECLARACIÓN Y AUTORIZACIÓN

Yo: **SANTAMARÍA CALUCHO CARLOS ALONSO**, con **CC. 180479497-0**, autor del trabajo de graduación intitulado: **"CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL"**, previa a la obtención del título profesional de **INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**, en la Escuela de **SISTEMAS.**

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, octubre 2022

CARLOS ALONSO SANTAMARIA CALUCHO.

CC.180479497-0

DEDICATORIA

Dedico este proyecto de Tesis a mi familia que tanto me apoyo, a cada persona que estuvo para mí. Así mismo desde un principio, al iniciar de mi carrera, para esa persona que me dijo que podría lograrlo todo y era capaz de mucho, de igual manera a mis padres quienes han realizado demasiados esfuerzos para darme la mejor educación, a mis maestros, quienes se empeñaron en lograr que sus materias y enseñanzas nos queden plasmados en la cabeza, a mis amigos y personas cercanas quienes siempre me alentaron a realizar de la mejor manera cada proyecto y meta personal que he tenido.

Con estas estas palabras, sé que no son bastas para expresar mi agradecimiento para cada persona que influyo en todos mis procesos de metas y logros, pero espero que sepan que mis sentimientos de aprecio y cariño se los entregó a cada uno de ellos.

AGRADECIMIENTO

Una vez culminado mi tan ansioso proyecto de titulación, solamente quiera dar una palabra: ¡Gracias!

Gracias a cada persona que supo guiarme en el camino, gracias a mis padres que, sin su apoyo incondicional y preocupación, todo seria diferente, gracias a ese angelito en el cielo que supo, no solo tranquilizarme a mí, si no a toda mi familia y nos ponía de buen humor, gracias a cada persona, amistad, compañía que estuvo para mi y me ayudo en lo que más pudo.

Gracias, también, a mis profesores que supieron guiarme, a mi tutora Teresa Freire, que, con su paciencia y bondad, me ayudo a lograr toda la realización del proyecto, de igual manera, a cada personal de la institución (IST) Pelileo, en especial a Pablo Morales, que lograron abrirme sus puertas y facilitarme todo para mi estudio y realización de tesis, así mismo a cada profesor que tuve dentro del salón de clases que con sus formas de enseñanza hacían que la carrera sea mucho mas agradable y me guste aprender.

Nada de esto hubiese sido posible sin todos ustedes y su gran apoyo. Este trabajo es el resultado de un sinfín de acontecimientos que supieron ayudarme y guiarme para mi proceso de titulación.

Gracias infinitas a cada uno de ustedes y, por supuesto, a Dios, que siempre supo ponerme las cosas tal como debían ser y a pesar de mucho, guio mi camino y me bendijo en cada momento.

RESUMEN

Las plataformas educativas han evolucionado y forman parte de la rutina escolar en centros educativos, permiten desarrollar clases virtuales y /o complementar clases presenciales. En el contexto actual, se requiere mayor seguridad para proteger la información de las organizaciones. Esta investigación tiene como objetivo implementar un procedimiento de control de seguridad para una plataforma educativa Institucional, con el cual se identifiquen las vulnerabilidades y riesgos de ciberseguridad, para brindar protección y confiabilidad a la plataforma educativa mediante el desarrollo de una guía de buenas prácticas. La investigación tiene un enfoque mixto, se aplicaron encuestas a docentes y estudiantes del Instituto Superior Tecnológico (ITS) Pelileo, se identificó que los usuarios desconocen de aspectos de seguridad y protección de datos, por otra parte, se entrevistó a los técnicos de la unidad de TI quienes determinaron la importancia de la implementación de medidas para protección de plataformas educativas. Para el desarrollo de la propuesta se utilizó el "Procedimiento de Gestión de riesgos de ciberseguridad dentro de los ITS de la Provincia de Tungurahua", que es una metodología que permite identificar las vulnerabilidades, dimensionar los riesgos, establecer normativas, controles y salvaguardas enfocados en la gestión de ciberseguridad. El resultado se evidencia a través de una guía de buenas prácticas para el aseguramiento y control de la plataforma educativa, además de la propuesta de implementación de una unidad de gestión de ciberseguridad. La validación se realizó con expertos que mediante un instrumento evaluaron la estructura, contenido, nivel técnico del análisis y propuestas realizadas.

Palabras Claves: Plataformas Educativas, Seguridad, Ciberseguridad, Riesgos, Vulnerabilidades.

ABSTRACT

Educational platforms have evolved and are part of the school routine in educational centers, allowing the development of virtual classes and/or complementing face-to-face classes. In the current context, greater security is required to protect the information of organizations. This research aims to implement a security control procedure for an institutional educational platform, with which vulnerabilities and cybersecurity risks are identified, to provide protection and reliability to the educational platform through the development of a good practices guide. The research has a mixed approach, surveys were applied to teachers and students of the Instituto Superior Tecnológico (ITS) Pelileo, and it was identified that users are unaware of aspects of security and data protection, on the other hand, technicians of the IT unit were interviewed who determined the importance of implementing measures for the protection of educational platforms. For the development of the proposal, the "Procedure for cybersecurity risk management within the ITS of the Province of Tungurahua" was used, which is a methodology that allows for identifying vulnerabilities, sizing risks, establishing regulations, controls, and safeguards focused on cybersecurity management. The result is evidenced through a guide of good practices for the assurance and control of the educational platform, in addition to the proposal for the implementation of a cybersecurity management unit. The validation was carried out with experts who evaluated the structure, content, technical level of the analysis, and proposals made using an instrument.

Keywords: Educational Platforms, Security, Cybersecurity, Risks, Vulnerabilities.

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN

La tecnología en la actualidad se ha visto envuelta en cambios revolucionarios por parte de cada entorno conocido, con trabajos o actividades simples las cuales han progresado para tener una mejor adaptación y flexibilidad con las personas y ayudar en gran parte a solucionar problemas. Es así, como en la educación se han implementado a lo largo de este tiempo, herramientas físicas y virtuales las cuales son conocidas hoy en día como plataformas educativas, estas brindan varias capacidades tanto a docentes como estudiantes de interactuar en un ambiente pedagógico al contribuir con procesos de enseñanza y aprendizaje.

Las plataformas educativas según Becerro (2009), han evolucionado a lo largo de la historia, las cuales con la implementación de materiales didácticos para páginas *web* han mejorado; desde los inicios de la década de 1990, el enfoque habitual de la documentación y programación *web* consistía en la creación de páginas mediante varios editores HTML, con la integración de varios recursos como *email*, foros y actividades, luego, con el avance de internet y con el nuevo avance de lenguajes de programación orientados a objetos (OOP) como Java o JavaScript, esto mejoró notablemente.

En este sentido, se considera actualmente, una alternativa interesante en relación con las cotidianas y tradicionales que se han llevado a lo largo del tiempo en la educación. Se menciona en base a esto, cómo mediante la pandemia por el COVID-19 que se dio en todo el mundo en el año 2020, se suspendieron las asistencias presenciales a clases. Esto causó a que, en el Ecuador según Padilla, Torres, & Padilla (2020), se opte por herramientas de teleeducación, las cuales cambiaron la modalidad de estudios; con lo que las instituciones educativas como escuelas, colegios, universidades e institutos implementaron necesariamente estas estructuras tecnológicas para la enseñanza y continuo aprendizaje de los estudiantes.

Así, un estudio realizado por León, Ramos, Mapp, & Reyes (2021), en Panamá, identificó las diferentes plataformas de aprendizaje virtual que detalla a siete como

las más usadas: Moodle con (23%), Educativa (16%), Google Classroom (15%), Microsoft Teams (14%), Canvas (14%), Chamilo (13%) y Schoology (5%). Estos datos que se muestra el estudio, como son los porcentajes de acuerdo con su usabilidad y cómo las universidades junto a los docentes han ido en aumento dentro de ellas.

En el contexto nacional, Bonifaz (2016), manifiesta que en Ecuador se encuestó a diversas universidades, las cuales son categoría A y B, basándose en varios criterios como eficiencia, investigación y organización, y dieron como resultado la utilización de las plataformas como Schoology, Sidweb y Moodle como las principales, estas dos últimas son las más usadas dentro del país.

Por otra parte, algunos de los hitos que propone la ciberseguridad en la actualidad, están relacionados a la pandemia del COVID-19, la cual se usó como gancho para estafas y localización de mayores ordenadores que sean vulnerables para ataques cibernéticos. Esta situación problemática ayudó a ver cómo las instituciones educativas que utilizaban en su gran mayoría pocos recursos de teleeducación, se vieron envueltas en implementar de manera inmediata nuevas plataformas, programas y herramientas las cuales ayudan a la enseñanza, esto de la misma manera fue considerado óptimo para la situación que se combate por otra parte resultó un problema muy poco conocido el cual fue la baja seguridad en todas estas aplicaciones impartidas por parte de las instituciones.

En este contexto, Velásquez (2020), menciona que la mayoría de los estudiantes al estar en clases virtuales, estaban expuestos a los ataques cibernéticos, los cuales se propagaban en las aulas virtuales; al respecto, los institutos y organizaciones educativas en los últimos años han incrementado su infraestructura digital con una conectividad interesante, mediante aplicaciones o programas, lo cual integra a los estudiantes a un aprendizaje de forma remota, al ser indispensable en este contexto la protección de estos recursos educativos en línea, una vez ingresados datos e información personal en éstos, es muy fácil que sean sustraídos por agentes externos maliciosos.

El sistema educativo para Bogantes (2020), es un sector especialmente atractivo para los atacantes cibernéticos, cuenta con una gran cantidad de datos e información personal como institucional, como bases de datos de alumnos, detalles de proveedores o transacciones las cuales mediante estas plataformas se realizan e ingresan continuamente. Para Olaya Oliveros (2021), los ciberdelincuentes tienen muchas oportunidades de explotar la seguridad de estos campos, todas estas plataformas generalmente no están actualizadas ni cuentan con sistemas óptimos de seguridad, que causa que no estén preparados para mitigar los ataques actuales.

En este aspecto, según Peña & Segura (2014), menciona que los ataques a plataformas educativas se encuentran vigentes dentro del internet y sus aplicaciones, lo que exige promover la ciberseguridad dentro de las instituciones educativas, pues es indispensable ser más cuidadosos y optar por un conocimiento amplio en salvaguardar datos personales como primer indicio. Los centros educativos no deben esperar un ataque para ver las consecuencias que este tiene y cómo les afectaría, sino más bien junto a los departamentos y unidades de tecnologías de la información (TI), estudiantes y docentes creen un plan de seguridad para mantenerse a salvo en internet y su navegación.

Para Chulde Obando (2021), los administradores de TI ya mencionados son los más importantes para prevenir estos peligros, son los responsables de crear varios protocolos e implementar normas, que sirvan como base para conocer sus plataformas institucionales y disminuir vulnerabilidades que causen riesgos, así como solucionarlas. Una forma de lograrlo es destinar un grupo especializado en hacking, sea tanto interno como externo para tener una mayor seguridad al momento de ejecutar estos pasos, así mismo lograr revelar posibles agujeros o fallas de seguridad. De esta manera, el sistema escolar y sus plataformas de teleeducación se van a probar en condiciones reales. Con estas prácticas se identifica las debilidades en un sistema, las cuales no son fáciles de detectar en un estudio común y así mitigarlas de mejor manera.

En base a lo mencionado, la presente investigación se plantea las siguientes interrogantes, que serán respondidas a lo largo del trabajo desarrollado:

- ¿Es importante la identificación de elementos teóricos y metodológicos relacionados con la ciberseguridad y la gestión de seguridad en plataformas educativas?
- ¿Cómo mejorará la seguridad de las plataformas educativas con la aplicación de una metodología de gestión de riesgos de ciberseguridad?
- ¿Cómo se pueden mitigar los riesgos y vulnerabilidades en las plataformas educativas?

Se observa cómo es sumamente importante la identificación de elementos teóricos y metodológicos relacionados con la gestión de seguridad en plataformas educativas, una protección adecuada en contra de estos ciberataques es esencial para una buena seguridad en línea, la cual, con elementos teóricos aplicados por parte de los docentes y expertos en TI de cada departamento designado, se logra una mejor respuesta a estas vulnerabilidades.

Entonces, un estudiante o docente, tiene que estar muy bien informado de estos problemas que existen y saber que la institución a la cual pertenecen tiene que contar con una buena identificación de estos problemas y solución inmediata, para así ocupar estas plataformas educativas sin riesgos ni con la incertidumbre de saber si está correctamente protegida.

Para OEA (2020), la manera de mitigar los riesgos y vulnerabilidades en plataformas educativas se basa en la capacidad de implementar ciberseguridad en los recursos de aprendizaje en línea los cuales protejan no solo a la institución si no a sus estudiantes, al limitar el riesgo de datos en general que se roban o interferir, que con el tiempo generan pérdidas financieras. Por lo tanto, las instituciones educativas y organizaciones tienen que garantizar a toda costa la protección de sus aplicaciones y sistemas; de esta forma se crea un ambiente funcional y correctamente activo, el cual está protegido de cualquier ataque que surja.

Frente a este análisis, la investigación desarrolló las siguientes actividades que permiten dar respuesta a las preguntas científicas enunciadas:

1. Fundamentación teórica y metodológica sobre la ciberseguridad y la gestión de seguridad en plataformas educativas.
2. Aplicación de una metodología de gestión de riesgos de ciberseguridad en una plataforma educativa.
3. Propuesta de una guía de buenas prácticas para el aseguramiento y control de una plataforma educativa.
4. Evaluación de la utilidad y pertinencia de la guía propuesta mediante el método de validación de expertos.

Al respecto, Morales & Medina (2021), consideran que grado importancia de la ciberseguridad enfocado en lo educativo requiere de varias medidas de seguridad las cuales ayudan a garantizar el acceso y envió de información ya sea de estudiantes como son sus pruebas y actividades que suben a sus plataformas y el material expuesto con el cual el tutor se maneja para las clases.

En relación a ello, Viñas (2017) menciona que la ciberseguridad se ve como retos que tienen que enfrentan las instituciones educativas, presentan varios problemas como ataques cibernéticos los cuales roban información o la alteran y de la misma forma manipulan para fines propios de las organizaciones o del atacante, es así como las posibles deficiencias en la implementación de los mecanismos de seguridad dentro de estas plataformas los cuales permiten que las amenazas se lleven a cabo e inevitablemente pongan en peligro a una organización o usuario el cual ha sido vulnerado. Como menciona Zabalo Arteche (2019) es fuertemente significativo que se tomen protocolos o metodologías las cuales ayudan a mantener un nivel de ciberseguridad aprobado para el sector académico.

La mejora en seguridad de las plataformas educativas en base a implementaciones de metodologías de gestión y seguridad, hacen que las instituciones que se rigen

por estas normas tengan como propósito el determinar y reconocer cada riesgo y vulnerabilidad existentes como amenazas de los sistemas de aprendizaje online.

Para la investigación se toma como base la tesis: “Procedimiento Metodológico de Gestión de ciberseguridad para las plataformas *web* educativas en los IST de la provincia de Tungurahua”, propuesta por Morales & Medina (2021), que contribuye a un proceso de gestión de seguridad para plataformas educativas, con la finalidad de identificar debilidades ataques que pongan en riesgo la ciberseguridad con el fin de brindar protección y mitigar riesgos o fallos para la creación de un entorno seguro y óptimo dentro de las instituciones, este estudio tiene como ventajas que está sustentada en Magerit V3.0, la cual sirve para implementar un proceso de gestión de riesgos en el margen aprobado de tomar decisiones las cuales tienen en cuenta los riesgos agrupados al uso de la tecnología de la información; tal como dicta la norma ISO 27032, la cual se encarga de proporcionar un marco seguro con normas óptimas que ayudan al intercambio de información, el manejo de eventos y la coordinación para optimizar de mejor manera la seguridad del proceso dentro del sistema.

La metodología seleccionada comprende distintas fases, las cuales son Definir objetivos de Ciberseguridad, Identificar infraestructura tecnológica a proteger, Elegir sucesos de seguridad más frecuentes en aplicaciones *web*, Identificar las vulnerabilidades del IST, con la que se fragmentada en 4 etapas las cuales son de reconocimiento, exploración, enumeración e informe, Definir controles de Ciberseguridad y Generación de Salvaguardas**.**

De esta manera, el estudio y metodología mencionado ayuda a prepararse, detectar, monitorear y responder a los ataques de ciberseguridad en Plataformas educativas, para tener en cuenta que se incluye controles y fases, las cuales quieren centrarse más en la protección de información como punto primordial dentro del sistema y de igual manera dar una guía de monitoreo el cual ayudara a los usuarios finales a mantener un sistema seguro.

Como se observa, basándose en el análisis de ciberseguridad en plataformas educativas, se observa cómo en la actualidad éste es un tema muy importante para abordarlo y conocer a profundidad, la información y datos computacionales es considerado crucial para la continuidad dentro de empresas o establecimientos, que en este caso hace referencia a las instituciones educativas y su gestión de los procesos por medio de plataformas educativas. El asegurar los datos tanto de estudiantes como docentes, información institucional, evaluaciones o documentos, dentro de las plataformas, evita que la información sea modificada o saturada con ataques a servidores, que se tiene como resultado un colapso de las plataformas al perjudicar el acceso por parte de estudiantes y docentes.

Esta realidad que se vive en los medios digitales de la educación remota hace que se comprenda con mayor necesidad sobre las amenazas que plantean las redes (Internet) y como esta puerta es la base es la más utilizada para los procesos de ataques cibernéticos. En el Ecuador desde el año 2019, funcionarios del Ministerio de Telecomunicaciones y de la Sociedad de la Información llevan a cabo estrategias de la seguridad de la información digital, que se logre crear normas y procesos establecidos como planes de riesgos y respuesta rápida ante ataques a servicios informáticos, que se enfrentan en el ciberespacio por atacantes cibernéticos.

Mediante lo mencionado según Carrillo Morales, Zambrano Avellán, Zambrano Lectong, & Bravo Zambrano (2020) consideran, cómo en las organizaciones e institutos educativos, no se mantienen un buen plan que permita combatir estas vulnerabilidades. Por lo tanto, existen varios aspectos los cuales se toma en cuenta para proteger estos espacios educativos, como de la misma forma contar con metodologías y normas que son establecidas dentro de estas aplicaciones y plataformas de educación, de esta manera obtener un entorno más confiable y seguro para los usuarios y personas en general que hagan uso de estas herramientas de enseñanza.

CAPITULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Ciberseguridad en Plataformas Educativas Institucionales

Para empezar con la compresión del presente proyecto, es importante conceptualizar sobre la Seguridad de la Información, en base a aportes teóricos y criterios de varios autores, mostrados a continuación:

Cuadro 1. Definición de Seguridad de la Información

Autor	Definición
(ISOTools Excellence, 2015)	En base a la ISO 27001 hace referencia en cuanto a que la seguridad de la información cuenta con privacidad, integridad y disponibilidad, en relación con la información personal y datos verídicos del sistema que son considerados indispensables para cualquier organización o institución que este tenga, independientemente de su formato digital o físico.
(Cárdenas Solano, Martínez Ardila, & Becerra Ardila, 2016)	Resalta que la seguridad de datos e información digital y su paso a lo largo del tiempo desde la seguridad física diseñada para proteger las computadoras hasta un enfoque en las políticas, las operaciones y los controles basados en los usuarios y personas.
(Beteta Lazarte & Narva De la Cruz, 2019)	Explica que sobre la Seguridad de la Información se tiene que plantear técnicas para proteger, prevenir y controlar datos de una empresa u organización.
(Garay Quisbert & Sanchez Seña, 2021)	Menciona sobre la seguridad de la información y su definición sobre un recurso principal dentro de cualquier organización, el cual se basa en controles y políticas estructuradas para la protección de información.

Fuente: elaboración propia

A partir de los conceptos antes mencionados, se menciona que la Seguridad de la Información trata de varias normas y estándares políticos, que se definen para prevención de ataques que perjudican a la confidencialidad, integridad y disponibilidad, de la información, las cuales se gestionan específicamente orientadas al entorno de una organización o institución.

Para Alarcón, Barriga, Picón & Alarcón (2016), la seguridad es una parte primordial de las redes y telecomunicaciones, por lo que es imperativo contar con soluciones activas y, lo que es más importante, tiene que ser eficaz y óptimo para solucionar de manera segura las amenazas o fallos informáticos que perjudican la integridad de la información que no se altere y de igual manera la confidencialidad de los datos en el sistema.

En base a lo descrito por seguridad de la información, el autor Salazar (2019), menciona que existen tres principios que trabajan de la mano para garantizar solidez dentro de un sistema informático, a esto se le conoce como la Triada de la Seguridad de la Información CID, la cual se muestra a continuación por medio de un gráfico:

Figura 1. Triada CID

Fuente: elaboración propia

Para comprender de mejor manera la imagen se muestran los tres pilares fundamentales de la Tríada CIA:

- **Confidencialidad:** Este primer pilar, hace referencia ampliamente a los procesos que las organizaciones ejecutan para mantener toda su información privada. Esta, comprende a la no divulgación de información o datos a personas externas o no designadas como apropiadas. En el caso de realizar un procedimiento, deberán ser autorizados estos cambios y deberán contar con accesos permitidos por grupos los cuales limitan acciones a cada usuario.

  En base a esto, detalla Pérez (2017), que se tiene que asegurar el acceso a todo tipo de información dentro de una organización, muchas veces las seguridades se rompen fácilmente si datos personales de usuarios son divulgados o compartidos con personas no autorizadas, esto ocasiona que un atacante fácilmente entre al sistema y causar pérdida o manipulación de datos.

Se menciona diferentes pasos para seguir una buena implementación de medidas que se toman para proteger la confidencialidad incluyen permisos, los cuales manejan entidades designadas de seguridad, estas a su vez deberán implementar medidas de control de acceso y mecanismos de autenticación, para mejorar el ingreso al sistema y protección en base a los datos.

- **Integridad:** Al igual que la confidencialidad, la integridad compone el segundo pilar sobre la seguridad dentro de un sistema, el cual para Rivera & Ibarra (2019), trata de mantener toda información tal cual, sin ser modificada o alterada, ya sea accidentalmente por algún usuario o procesos no autorizados, por lo tanto, dentro de una organización, se tiene que enfocarse en esta fase para la obtención de datos confiables y precisos.

  Como toda institución u organización, deben confiar plenamente en sus datos, se refleja información de clientes o procesos los cuales realizan dentro de estos. Garantizar que la información sea verídica y en él envió y recibimiento de esta no sea manipulada, cuenta con la integridad para asegurar este punto.

  Las medidas óptimas para resguardar la integridad, se base en la protección de ésta, en donde se tiene que realizar encriptación de datos y mecanismos de verificación en cada proceso que se realice, al igual que controles de acceso los cuales permitan la manipulación segura de información.
- **Disponibilidad:** se refiere a la importancia de los datos y sistemas que una organización y como su valor significa mucho al momento de disponerlo e intentar acceder a ello, por ende, encontrar cualquier tipo de información designada a estos, la facilidad que cada miembro de una organización acceda a los datos siempre que lo requieran.
- Existen muchas variables las cuales ponen en riesgo la accesibilidad, como fallos ya se a nivel de *software* o hardware. Según Bautista (2019), menciona que el ataque más conocido hoy en día es el DDoS el cual ejecuta una denegación de servicios los cuales interfieren en los servidores y llegan a perjudicar la accesibilidad de la información solicitada en ese momento.

  Como medidas para asegurar la accesibilidad dentro de una organización, se crean redundancias y tolerancia en servidores, redes y aplicaciones, los

cuales ayuden a generar más vías de entrega de información y con ello, crear un sistema óptimo.

Una vez resaltados los tres pilares CID, es indispensable en cualquier organización según su dependencia priorizar uno más que otro, estos tres principios son prioritarios según la organización a la cual se enfocada su servicio. Pero no es necesariamente algo malo el no considerar todos de la misma manera, como una tríada, obliga a que los miembros de cada organización vean la seguridad la dependencia del trabajo y cómo incorporan a cada una de estas para su beneficio, lo que ayuda a priorizar la implementación de servicios de seguridad.

Una vez contextualizada la seguridad de la información y sus aspectos importantes dentro del contexto de la seguridad informática, es indispensable definir de igual manera lo que es Ciberseguridad, la cual, abarca al proceso de protección de datos computacionales de un ordenador y toda la información circulante a través de las redes; a continuación, se define en base a varios autores:

Cuadro 2. Definición de Ciberseguridad

Autor	Definición
(Becerra, y otros, 2019)	Define a la ciberseguridad como un conjunto de herramientas, tácticas y conceptos de salvaguardas de información, los cuales se utilizan para garantizar un ambiente seguro dentro de organizaciones y usuarios en el ciberespacio.
(CISCO, 2020)	La ciberseguridad tiene como objetivo el enfoque de protección de sistemas tecnológicos, ya sean programas o datos que los atacantes buscan interrumpir maliciosamente.
(Fernández Bermejo & Martínez Atienza, 2018)	Menciona que la ciberseguridad trata de la protección global de activos informáticos mediante métodos de seguridad.
(Mendivil Caldentey, Sanz Urquijo, & Gutierrez Almazor, 2022)	La ciberseguridad hace frente a las amenazas y vulnerabilidades que pongan en riesgo un sistema, al dar soluciones y medidas de prevención para combatir estos ataques.

Fuente: elaboración propia

En referencia a los criterios antes mencionados, se define a la ciberseguridad como, un conjunto de acciones que garantizan la protección de ordenadores y sistemas en general, que ayude en caso de un ataque cibernético no se sufran perdidas o daños de información.

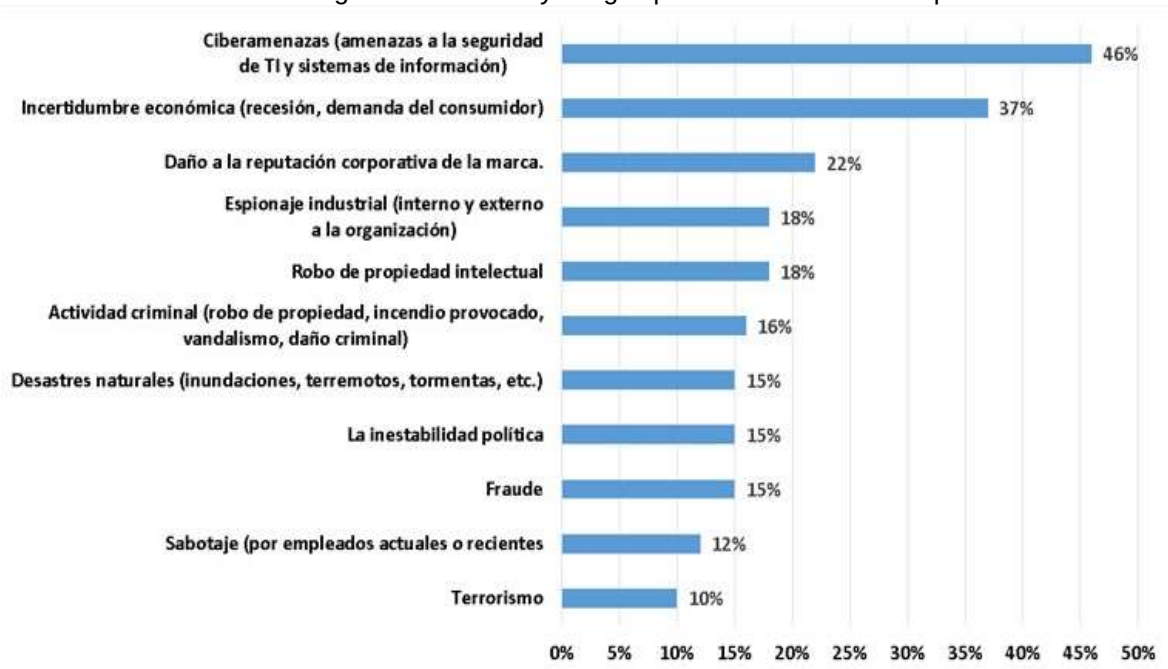
Se tiene como objetivos principales de la ciberseguridad la prevención de ataques maliciosos los cuales ayudan a organizaciones a estar lista para enfrentarlos, de igual manera la detección de estos ataques son prioridad dentro de la ciberseguridad, al saber a qué se enfrenta una organización, se opta por una solución y como último punto el de la recuperación, ya una vez mitigados los ataques, crear procesos de gestión de recuperación de información en el caso de haberlos perdido durante el mismo.

En este contexto, se presenta la ciberseguridad a nivel global en donde se aprecia como en la actualidad según Aon (2020), expresa los resultados de ciberataques, como por ejemplo a través de correos electrónicos, los cuales dentro de la informática son conocidos como phishing, los cuales son responsables de bajar un capital de más de 12 billones de dólares en menos de 5 años. Y en el caso de ataques cibernéticos como ransomware se ha estimado una cifra de 20 billones de dólares para el año pasado.

Del mismo modo manifiesta, Aguilar (2020), en los estudios de la Aon Corporation, que las administraciones gubernamentales alrededor del mundo tuvieron que invertir un aproximado de un trillón de dólares en gastos de ciberdefensa en 2019, en dónde se aprecia que los sectores más vulnerados son instituciones financieras y fábricas industriales, los cuales implementaron servicios digitales para la interacción de sus usuarios, sin percatarse que era una puerta para los ciber atacantes, estos riesgos se relacionaron al gobierno nacional, al no priorizar la ciberseguridad dentro de cada país.

Un estudio en el 2019 realizado por Karpspersky, en base a instituciones privativas y estatales, mencionan que se tiene un porcentaje de (46%) en ataques cibernéticos con el cual se muestra un daño mayoritario en cuanto a la seguridad dentro de cualquier organización o empresa.

Gráfico 1. Seguridad en TIC`s y riesgos percibidos en el ciberespacio



Fuente: Karspersky (2020)

Los datos mostrados en la imagen anterior detallan como la ciberseguridad es cada vez más importante dentro de cualquier organización, esto hace que se tenga más conciencia sobre cómo se tiene que proteger y tanto el gobierno como las entidades, creen nuevas estrategias para mantener un entorno seguro en internet. En ese sentido, se hace necesario mencionar como dentro del ciberespacio existe seguridad ya sea en base a cada dispositivo o aplicación que se use, para llevar así a la ciberseguridad como punto clave para prevenir estos casos.

Dentro del contexto educativo, las plataformas educativas institucionales según Barrera & Guapi (2018), se han convertido en un recurso indispensable hoy en día, la acogida que se ha ganado en espacios educativos cibernéticos es amplia. Tal como las instituciones educativas en la educación superior, son las que más usan estas herramientas con el fin de transmitir conocimiento en línea, las universidades a distancia han ocupado más estas herramientas y hoy en día por medio de la pandemia se ha optado por implementar en toda institución, esta plataforma educativa facilita la enseñanza en estudiantes y el impartir conocimiento por parte de los profesores.

De igual manera que todo sistema informático, para las plataformas educativas existen riesgos y amenazas a los que se han expuesto en los últimos años, como detalla Contreras & Oliveros (2018), en un cuadro el cual presenta las principales amenazas y la descripción que esta tiene.

Cuadro 3. Amenazas en Plataformas educativas

Principales Amenazas	Descripción
Violación de confidencialidad	Una parte no autorizada que obtiene acceso a los activos alojados en el sistema de e-learning.
Violación de integridad	Una parte no autorizada que accede y se apropia de un activo utilizado en el sistema de e-learning.
Denegación de servicio	Prevención de derechos de acceso legítimos al interrumpir el tráfico durante Transacciones entre los usuarios del sistema E-Learning.
Uso ilegítimo	Explotación de privilegios por parte de usuarios legítimos.
Programa malicioso	Líneas de código para dañar otros programas.
Repudio	Negación de la participación de uno de los participantes en la plataforma E-Learning en cualquier transacción de documentos.
Enmascaramiento	Una forma de comportamiento que esconde la identidad de los hackers.
Análisis de tráfico	Fuga de información al abusar del canal de comunicación.
Ataque de fuerza bruta	Un intento con todas las combinaciones posibles para descubrir lo correcto, en este caso las claves de acceso a la plataforma E-Learning.

Fuente: Contreras & Oliveros (2018)

En base a lo expuesto en el cuadro anterior, se notan los riesgos que tienen las plataformas educativas y como la mayoría de las amenazas que se presentan causan el abuso de información al violar protocolos de confidencialidad y de igual manera la denegación de servicios, al poner en riesgo la accesibilidad por parte de los usuarios al crear así un entorno ineficiente. Es así como las instituciones educativas deben enfocarse más en estos riesgos para prevenirlos y mitigarlos a tiempo.

La ciberseguridad en las plataformas educativas se gestiona prioritariamente, con ella se previene varios ataques los cuales ya han sido mencionados anteriormente, el ambiente virtual de estas plataformas de aprendizaje está conectado al internet, al ser así la puerta principal para que ciber atacantes quieran pasar. Es por esto por lo que menciona Valencia (2014), que la ciberseguridad ayuda a mejorar la calidad del usuario y la protección de su información. Por parte de los administrativos deberán optar por protecciones a ordenadores con programas que restrinjan el paso a usuarios no autorizados y de igual manera instruir al usuario al

cuidado y buen manejo de estas plataformas, para que no cometan errores que permitan el paso a ataques cibernéticos.

1.2. Normas y estándares de Seguridad en Plataformas Web

En este apartado se plantea un procedimiento de Gestión de riesgos de ciberseguridad en Plataformas Educativas, el cual se centra en primer lugar en el estudio de las normas, estándares y técnicas más utilizadas para dar soluciones a problemas cibernéticos en aplicaciones *web*.

Para esto, detalla Global Suite (2021), que la ciberseguridad hoy en día no es algo sencillo de implementar debido a su complejidad pues existen una gran cantidad de dispositivos los cuales deben ser protegidos y que cuentan con diferentes sistemas operativos que para ser asegurados requieren de diferentes técnicas las cuales ayuden a solventar estas amenazas.

A pesar de esto, existen varias formas de implementar medidas de protección a ordenadores y datos, se trata de normas y estándares ISO las cuales están relacionadas específicamente a la ciberseguridad y la seguridad de la información. Estas normas ISO están creadas por la Organización Internacional de Normalización (ISO). Tanto el estándar ISO como IEC (Comisión Electrotécnica Internacional) están especializados para la regulación a nivel global. A través de estas normas es posible observar cómo se cumplen lineamientos los cuales ayudaran a un mejor desenvolvimiento en el área de ciberseguridad.

En base a las normas ISO, se clasifican de diferente manera las cuales tienen numeraciones que dependen del propósito y las series que estas agrupan. Los estándares y normas plantean como objetivo primordial el identificar políticas y lineamientos los cuales ayuden a mejorar el área específica en donde se implemente esto.

La norma ISO 27000 que detalla ISOTools (2015), se clasifica en varias, con la que se tiene una familia de estándares los cuales se presentarán a continuación con una breve descripción.

Cuadro 4. Normas ISO 2700

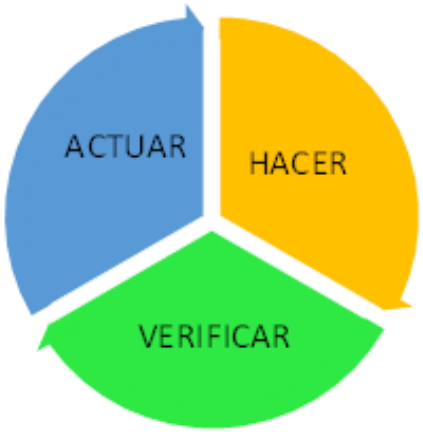
Normas	Descripción
ISO 27001	Trata de la norma primordial de toda la rama de estándares de gestión de seguridad de la información.
ISO 27002	Considerado como un control y procesos de implementación para la evaluación y registro dentro de la seguridad de la información.
ISO 27003	De igual manera que la anterior norma sirve como manual y ocupa el ciclo PHVA.
ISO 27004	Trata de la utilización de métricas para la gestión de un sistema de información (ciclo deming).
ISO 27005	En base a las directrices que otorga la ISO 27001 y 27002, la norma se aplica en diferentes empresas para temas de seguridad informática.
ISO 27006	El siguiente estándar ayuda a la certificación de diferentes entidades.
ISO 27007	Con este estándar se enfoca en guiar mediante procesos de operatividad y monitoreo la seguridad de la información.
ISO 27011	Este estándar fue constituido por la (ITU) y brinda una gestión de seguridad en telecomunicaciones.
ISO 27031	Explica conceptos iniciales de TIC y guía la continuidad de un negocio basado en tecnologías de la información.
ISO 27032	Este estándar garantiza las directrices de la seguridad, para reducir riesgos en Internet como prioridad, para proporcionar un marco seguro para el intercambio de datos.
ISO 27033	Es un estándar derivado del estándar de ciberseguridad ISO/IEC 18028. Este estándar describe la ciberseguridad y brinda orientación sobre la gestión de esta.
ISO 27034	Esta norma trata de una guía de ciberseguridad en aplicaciones.
ISO 27799	Apoya a los controles y directrices dentro de la salud informática.

Fuente: elaboración propia

Como se observa las distintas normas ISO que se muestran en el cuadro anterior, son conjuntamente enfocadas a la seguridad de la información, estas cuentan con normas y lineamientos los cuales una vez implementados, harán que una organización o institución sea acreditada como aceptable dentro de su nombramiento. Esta serie de normas compuestas detallan los modelos y requisitos que se tiene que implementar en un Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de gestionar la seguridad de la información de las organizaciones.

Las organizaciones deben implementar planes de gestión y mejora continua con las que se optimizan los procesos y perfeccionar la productividad en base al producto o servicio que se otorgue, es por eso por lo que existe un sistema llamado Ciclo Deming o PDCA que consta de las 4 fases las cuales se muestra a continuación:

Figura 2. Ciclo Deming o PDCA



Fuente: elaboración propia

Como menciona Rueda (2018), el Ciclo Deming trata de un sistema de mejora continua que sirve para empresas y organizaciones las cuales desean impulsar o mejorar la productividad, para seguir con un ciclo el cual permita planear, hacer, verificar y actuar. Este procedimiento se aplica en la norma ISO 27002 la cual se mencionó anteriormente y es posible la mejora en procesos de TIC para garantizar servicios seguros en la información.

Además de las normas ISO ya presentadas, existen muchos otros estándares fuera de esta familia, cada uno de ellos sigue enfocado al contexto de la seguridad y cómo estos protegen al sistema de ataques.

Cuadro 5. Normas y Estándares en Sistemas de Información

Norma o Estándar	Enfoque	Autor
Estándar del NIST	Otorga un listado de controles y guías, los cuales apoyan al desarrollo seguro de sistemas de la información	(Luna & Rosa, 2009)
Normas (SOC 2)	Son llamados Controles de Servicio y Organización 2, esta norma trata de gestionar los riesgos de ciberseguridad dentro de las organizaciones.	(Rodríguez, 2020)
Norma ENS y CNN-CERT	La guía (CCN) trata de proteger organizaciones públicas con el fin de aumentar el grado de seguridad en los ciberespacios. La (ENS) proporciona medidas y requisitos para seguridad informática.	(Naveiro Cabanas, 2021) (Sanz, 2021)
Estándar COSO y COBIT	Estos modelos son enfocados en la administración ejecutiva y de gobierno, para otorgar guías de control empresarial y buenas prácticas para la gestión de sistemas de la información.	(Torres Arízaga, 2018)
MAGERIT V3.0	Esta metodología analiza y gestiona ataques que se sufren en sistemas informáticos, ayuda a identificar problemas y los mitiga mediante implementación de tecnologías.	(Jácome Chávez, 2019)

Fuente: elaboración propia

Una vez conocida todo tipo de norma existente y que rige dentro del ámbito de seguridad de la información y ciberseguridad, se presentaron en el cuadro anterior opciones de estándares y lineamientos las cuales ayudan a organizaciones a mejorar sus servicios y proteger toda información.

En base a la investigación realizada, se define normas específicas las cuales para Morales & Medina (2021), son las principales en ejecutar para el procedimiento de gestión, estas son Magerit V3.0 la cual trata de una metodología de análisis y gestión de riesgos, esta se utiliza libremente y proporciona métodos preventivos que ayuden al análisis y estudio sistemático de vulnerabilidades y riesgos que se presenten en las TICS, de igual manera se centra en la norma (ISO/IEC 27032) la cual se detalló anteriormente y está enfocada en proporcionar lineamientos de seguridad y confiabilidad para proteger la privacidad de las personas y organizaciones que manejan datos e información muy delicada. En base a esto, se tiene en cuenta que esta norma busca en particular la gestión de todo el ciberespacio y su seguridad por medio de buenas prácticas.

Es importante resaltar que, dentro del ámbito educativo, las normativas y procesos para implementación de la ciberseguridad en sus plataformas, son escasas, y

dentro de la investigación se ha determinado que el trabajo de Morales & Medina (2021), propone una metodología enfocada en la gestión de ciberseguridad para plataformas *web* educativas en Institutos Técnicos Superiores (IST). Esta tiene como objetivo un procedimiento de ciberseguridad que comprende las siguientes fases:

- **Fase 1.-** Definir objetivos en ciberseguridad. -En esta fase, se establecen los procesos internos de seguridad indispensables los cuales tienen como objetivo determinar la ciberseguridad de los IST y brindar con esto la protección correcta y los niveles en los cuales se alinearán los procesos.
- **Fase 2.-** Identificar infraestructura tecnológica a proteger. -En esta fase, se centra específicamente en las infraestructuras de hardware y *software* que se pretenden resguardar, las cuales se referencian como las más vulnerables para los ciberataques y deberán ser mitigadas.
- **Fase 3.-** Seleccionar incidentes de seguridad más comunes en las aplicaciones *web*. -En esta fase, se hace más énfasis en el "Catálogo de Amenazas" definido en la metodología MAGERIT V3.0 la cual ayuda a seleccionar las amenazas o riesgos más activos que se tengan en la infraestructura educativa y a partir de estos se dividen en tres áreas las cuales son: Administración del Sistema, Plataforma Web y Usuarios. Estos tendrán referencias e incidentes detectables por cada área afectada y sus aplicaciones.
- **Fase 4.-** Identificar las vulnerabilidades del IST. -En esta fase, se realiza 4 etapas basadas en el estudio de Páez (2014) el cual detalla:
  a) Reconocimiento: Establecer el objetivo a estudiar, para la búsqueda de posibles vulnerabilidades que estas tienen.
  b) Exploración: Una vez recolectada la información en la etapa anterior, se detectan las vulnerabilidades definidas en la Fase 3.
  c) Enumeración: Dentro de este apartado se recopilan información clave que afectan gravemente el sistema.
  d) Informes: como última etapa, trata en registrar las vulnerabilidades localizadas en el sistema de educación y sobre estas generar

recomendaciones y salvaguardas para evitar posibles ataques cibernéticos que afecten a la institución en si o su información vital.

- **Fase 5.-** Definir controles de ciberseguridad. -En esta fase, se incorporan los riesgos definidos anteriormente para realizar controles necesarios de la norma ISO 27032, con el objetivo de obtener mejores soluciones de seguridad y determinar de mejor manera incidentes y sus soluciones propiamente de estos.
- **Fase 6.-** Generación de Salvaguardas. - En esta fase, se implementan las salvaguardas necesarias las cuales darán como resultado una solución a las áreas de afectación encontradas y así mejorar el sistema de la plataforma educativa.

Como metodología de investigación para esta investigación se utiliza la ya antes mencionada, la cual tiene como objetivo el estudio de todos los componentes y funciones del sistema, para garantizar la confiabilidad, la seguridad y el desempeño de los requisitos que los usuarios o el cliente requiera.

Los procedimientos y estrategias que serán utilizadas ayudarán a proteger y mejorar el ambiente de ciberseguridad dentro de las plataformas educativas, las cuales están enfocadas para la utilización de los IST en específico. De esta manera, la metodología detallada por Morales & Medina (2021), se enfoca en detectar, monitorear y responder a los ataques de ciberseguridad, se tiene en cuenta que incluye controles como son el de Aplicación, el cual quiere centrarse más en la autenticación de información la cual es primordial dentro del sistema para evitar cualquier daño o modificación.

1.3. Gestión de Seguridad en Plataformas Educativas

La educación virtual está en constante evolución desde lo ocurrido con la pandemia del COVID-19, en donde varias organizaciones y entidades vieron la necesidad de contar con un sistema de enseñanza remota el cual permita seguir con aportes de educación para los estudiantes. Este panorama mundial evidenció cómo desde la educación primaria hasta la educación superior cuentan con estas plataformas, las

cuales son programas virtuales que buscan crear ambientes de aprendizaje instantáneos, en donde los estudiantes y docentes interactúan y organizan varios contenidos digitales que ofrezcan enseñanza y por parte del docente evaluación de procesos.

Como detalla García, Cen, & Us (2016), la mayoría de las instituciones que aplican estas plataformas educativas son instituciones públicas y privadas: colegios, bachilleratos, universidades e IST, las cuales ofertan sus servicios educativos a través de ambientes virtuales; lo que anteriormente era común únicamente en instituciones a distancia las cuales desde hace mucho tiempo fueron las primeras en tener sus plataformas funcionales dentro de su organización. La necesidad de esta implementación fue el hecho de no contar con espacios requeridos para los estudiantes, se enfocan en la comodidad horaria de las personas.

Las plataformas educativas en Educación Superior han tenido gran repercusión en cuanto a la educación, como se muestra en la investigación realizada por Escobar (2019), quien señala las capacidades administrativas las cuales gestionan estas instituciones en base a sus contenidos y como hoy en día estos materiales didácticos son necesarios para la interactividad.

Por lo anterior, las plataformas educativas en estas instituciones más centradas en los IST están expuestas a amenazas y riesgos por parte de ciber atacantes, quienes alteran información y contenidos al violar derechos y protocolos de estas.

Los entornos virtuales poseen cada vez más capacidades de recolección y almacenamiento de datos los cuales para Serrano (2006), hacen que se consideren más difícil proteger, enfocándose precisamente a que se tomen medidas preventivas de seguridad para su resguardo. En el 2020 según Group IT Digital Media (2021), expuso sobre el incremento de ataques realizados a usuarios de plataformas educativas, como mención a las más utilizadas; Zoom, Moodle y Google Meet; se resaltó que el 98% de las amenazas encontradas no fueron virus, sino específicamente ataques de *riskware* y *adware*.

Para entender de mejor manera lo que significan estos ataques, se define a *riskware* según Kaspersky (2021), como programas maliciosos que causan alteraciones a usuarios, estas son de eliminar, bloquear, alterar o sustraer datos informativos, para perjudicar así la accesibilidad del usuario en su plataforma, de igual manera el hecho de atacar este sistema causa el rendimiento bajo en ordenadores y redes.

Este método de hurto de información y manipulación se comprende de diferentes maneras e ingresar a un sistema fácilmente al dar permisos no autorizados, la mayoría de las veces por desconocimiento, se instala programas no seguros los cuales crean estos ataques, para reconocer cómo estos programas se presentan, se crea un cuadro el cual muestra alguno de estos comportamientos:

Cuadro 6. Comportamientos de riskware

Comportamiento	Definición
IRC de cliente	Trata de una aplicación la cual ataca a puertos para el acceso a redes de comunicación, se utiliza el protocolo IRC.
SMTP de cliente	Al ser un remitente de correos electrónicos, se interrumpe o modificar la información.
Descargador	Se camufla en algún archivo ejecutable el cual este lleno de virus o programas los cuales causan ataques a el ordenador.
Herramienta de fraude	La relación que esta tiene con documentos modificados, los cuales generen información errónea sobre alguna organización o servicio.
NetTool	Este comportamiento al prestar servicios de control de host, escaneado en red, entre otros se generan ataques con una interfaz muy intuitiva, la cual se modifica para la recolección y robo de datos.
PSWTool	Al ser un programa para ver o restaurar contraseñas olvidadas, se ocupa como programa malicioso para robar estas claves y acceder a ordenadores de manera indebida.
RemoteAdmin	Trata de un programa keylogger el cual se encarga de capturar las pulsaciones del teclado del usuario para obtener los datos o información que este ingresa o procese en su ordenador.
RiskTool	Este programa oculta archivos del sistema, ya sean documentos, aplicaciones o procesos. Al poseer estas propiedades logran causar daños en el sistema.
WebToolbar	Junto con otros componentes del sistema, se recibe automáticamente permisos de instalaciones, al dar acceso a que cualquier programa malicioso logre entrar.

Fuente: modificado a partir de Kasperky

Al ver estos comportamientos los cuales un *riskware* logre tener, ayuda mucho identificar como usuario, al utilizar las plataformas educativas, como estas logren ser atacadas fácilmente al no tener una protección adecuada en el sistema. La detección y eliminación que se opte para este caso como paso principal la

instalación correcta de un buen antivirus, posteriormente cuidar los ordenadores de terceros los cuales ya sean con intención maliciosa o accidental instalen programas o archivos los cuales contengan esta amenaza, para prevenir esto es bueno contar con personas de servicios técnicos de confianza y que sepan lo que hacen con el ordenador sin ponerlo en peligro.

De igual manera la otra amenaza mencionada adware, según Avast (2021), trata de un *software* que ataca al navegador y crea anuncios los cuales son como spam, que hace que el usuario se sienta atrapado o tenga la necesidad de atender a uno de ellos y dé *clic*, con el que repercute a una serie de pasos graves lo que lleva a que el ordenador se llene de anuncios no deseados.

La mayoría de estos anuncios que resultan ser adware se encuentran en páginas no seguras las cuales dan paso a descargas que perjudiquen al sistema, la manera de protegerse de esto es tener un bloqueador de publicidad fiable y no dar clic en lugares o pestañas emergentes que no conozca su procedencia o sea un sitio de confianza.

Normalmente estas amenazas dentro de las plataformas educativas se ven disfrazadas como links de descargas ya sea de documentos necesarios en clases o aplicaciones, links de conferencias o plataformas que guían a procesos específicos, estas no son oficiales y causa al usuario una confusión o de igual manera correos que lleguen de fuentes extrañas con peticiones y datos falsos para que el atacante se infiltre y afecte la máquina.

En contexto al proceso de gestión de seguridad, se identifica en un estudio realizado por Kaspersky en el año de 2020, el número de usuarios que se encontraron con diversas amenazas dentro de una plataforma en línea y aplicaciones de videoconferencia fue un estimado de 168,550 casos de vulnerabilidades dentro de estas plataformas educativas, las cuáles se muestran a continuación.

Gráfico 2. Número de usuarios que encontraron amenazas en Plataformas educativas

Fuente: Karspersky (2020)

Como se observa en el gráfico la herramienta que más ataques ha sufrido es la de Zoom, la más usada a nivel mundial para realizar conferencias, seminarios o dictar clases en sí. En segunda posición está Moodle y consecuente Google Meet. En comparación a estas dos últimas plataformas educativas en línea, se ve que en Ecuador Moodle es una de las más implementadas de igual manera, lo cual hace que sea preocupante el riesgo que estas tienen al no estar bien protegidas.

Como se muestra en este estudio el 98% de estas amenazas fueron por motivos ya mencionados de *riskware* y *adware*. Para ayudar a protegerse de estos ataques tanto profesores como alumnos deberán ser capacitados para el uso correcto de estas plataformas en línea y conjuntamente a protocolos y metodologías resguardar los ordenadores y procesos de red que se efectúen dentro de cualquier organización o institución educativa.

Desde el punto de vista numérico a nivel global el Equipo Mundial de Investigación y Análisis de Kaspersky elaboró un pronóstico para el 2021 de los desafíos y posibles amenazas que las plataformas educativas enfrentaran.

A medida que aumentan las plataformas educativas y su popularidad dentro del ámbito académico, también crece el número de ataques que estas reciben como sitios de phishing asociados a servicios educativos y de videoconferencia los cuales utilizan mayormente docentes y estudiantes. Los principales objetivos que estos ataques cibernéticos tienen son el robo de información personal o la cantidad de

anuncios considerados spam, que sirven para confundir al usuario. Además, las plataformas educativas se enfrentarán cada vez a nuevas formas de amenazas las cuales para los ciber atacantes es una manera de aprovechar estas vulnerabilidades.

Actualmente, los profesores o encargados administrativos tienen que manejar el contenido de estas plataformas, para subir tareas o actividades para los estudiantes y de igual manera configurar las aplicaciones de videoconferencia, lo cual es una tarea compleja. La manera en la que manejan estas propiedades en las plataformas hace que se tome mucho en cuenta sobre la importancia de no dejar puertas que sirvan para ataques cibernéticos. La privacidad es otra propiedad la cual se tiene que cuidar mucho en este sentido, una actividad o servicio mal configurado es una puerta fácil de atacar y conseguir datos personales, en este caso, de docentes y estudiantes los cuales resultan como víctimas de ciber ataques.

Como punto principal ya mencionado, la confidencialidad de datos es el objetivo que tiene mayor énfasis en proteger. La gestión de esta en cualquier servicio requiere del usuario como primer punto para el cuidado de datos, pero como se sabe hoy en día, el manejo de las plataformas educativas ya está desde niños pequeños hasta universitarios, los cuales no tienen el conocimiento necesario para reconocer amenazas cibernéticas o controlar adecuadamente su configuración de privacidad en línea.

Además, como menciona Carrillo (2021), las actualizaciones y nuevos funcionamientos que tienen las plataformas educativas en la actualidad ofrecen numerosos y nuevos servicios como herramientas que permiten mejorar el proceso educativo en línea, y es muy probable que los docentes no sólo ocupan uno, sino varios componentes los cuales les sirva para mejorar sus contenidos y forma de enseñanza. Por tanto, por cada herramienta o servicio utilizado dentro de estas plataformas se enfoca en tener especial énfasis en la protección de todos los datos que se ingresen para ese recurso y de igual manera cuidar la información subida, que sea confiable y segura.

Para Castillo & Álvarez (2021), mencionan que es fundamental que los estudiantes se encuentren en un ambiente seguro de educación, el cual ayuda a las familias a sentirse tranquilas para saber que no se encuentran con algún riesgo dentro de estas plataformas, los equipos educativos en los que se manejan deberán permanecer resguardados con antivirus o servicios de protección informática y mantener buenas prácticas de seguridad informática.

La manera de ayudar tanto a estudiantes y docentes es otorgar el conocimiento necesario para mostrar la forma adecuada de utilizar estas herramientas con su grado de seguridad. A continuación, se presenta algunos pasos sencillos que ayudarán a docentes y estudiantes a navegar en un ambiente de internet seguro y controlar sus dispositivos y servicios de la mejor manera:

Pasos técnicos para mejorar la ciberseguridad

- Configuración inicial: los dispositivos que se utilizarán para la conexión a estas plataformas educativas ya sean móviles, *tablets* o un ordenador deberán contar con actualizaciones correctas y configuración de privacidad, estas desde programas como antivirus a permisos básicos que se utilice para acceder a cualquier sitio de internet, esto ayuda a la seguridad y privacidad del usuario. Aunque parezca complicado, estas técnicas son fáciles de implementar y sirven como primer punto para proteger la información personal, para evitar filtraciones involuntarias o robo de estas.
- Configuración de privacidad: Como cualquier servicio depende del usuario que esté al control el ordenador, cada plataforma ofrece opciones de perfil los cuales se logra configurar ya sea desde niños hasta jóvenes universitarios, que se les bloquee páginas indebidas y limitar los servicios.
- Contraseña de acceso segura: Muchas veces se ve que al crear las cuentas se indica que deben tener mayúsculas y números, esto no es por simple coincidencia que pidan en la mayoría de las páginas seguras estos pasos. Esto sirve para que, si un atacante quiere hackear las cuentas, no se le haga fácil descubrir la contraseña, se crea una contraseña segura con caracteres

especiales y alfanuméricos, estos no deberán tener relaciones con las fechas de nacimiento o datos personales, harán que sea más fácil descifrar.

- Permisos de administrador: Cada docente es el responsable de su grupo de estudiantes, el cual deben bloquear acceso a cada servicio que no sea permitido por el estudiante, la supervisión de cada actividad tiene que ser monitoreada y limitada par ciertos usuarios. Cada plataforma otorga diferentes funciones o servicios que sirven para interactuar, siempre se opta por designar medidas que controlen a los estudiantes del ingreso o acceso a información, para evitar de esta manera conflictos de seguridad.

Una vez mostrado algunos pasos para ayudar a resguardar la privacidad y crear un entorno seguro dentro de las plataformas educativas, se tiene que tomar en cuenta el esfuerzo que docentes y administradores hacen para implementar políticas y normas de seguridad.

Al utilizar una plataforma se comprende la gravedad de los ataques que se sufren y como se opta por intentar evitarlos, la mayoría suplanta identidades para el acceso a información, al perjudicar así al usuario suplantado como la organización o instituto educativo. Al igual que ocurre con otros servicios dentro del ciberespacio, las situaciones que a menudo los estudiantes manejan no les dan importancia al pensar en que son simples inocentadas, cuando así se abre brechas de vulnerabilidades que llevan a delitos informáticos con consecuencias importantes que se deben considerar dentro de una plataforma educativa.

A continuación, se presenta una imagen en donde se muestra varios pasos de seguridad en los dispositivos, accesos a las plataformas y opciones de privacidad las cuales se toman mucho en cuenta para el ingreso online a estas plataformas educativas.

Figura 3. Plataformas Educativas online con seguridad

Fuente: Díaz (2020)

Al nombrar a las plataformas educativas, se observa a las herramientas virtuales como una gran oportunidad de enseñanza que ayuda, no solo para la educación a distancia como ya se conoce, sino como complemento de las clases habituales que se han tenido que implementar en los últimos años. Todas estas nuevas formas de aprendizaje deben tener una buena seguridad para crear un ambiente positivo y seguro dentro de la tecnología.

La forma que se deben mejorar estas gestiones de seguridad depende del paso del tiempo y como las organizaciones evolucionan en protegerse y mitigar cada riesgo que se efectúen, siempre se considera pilares fundamentales dentro de estas plataformas para resguardar datos y permitir que sea siempre accesible toda información.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la institución

El Instituto Superior Tecnológico Pelileo, ubicado en la provincia de Tungurahua, fue fundado en 1994, este instituto otorga títulos de tercer nivel con horarios flexibles en cuanto a las carreras, el tiempo de duración es de 3 años, esta institución de Educación Superior es reconocida por ofrecer educación de calidad y una formación académica de excelencia, cuenta con tres carreras: Tecnología Superior en Contabilidad, Tecnología Superior en Desarrollo de *Software* y Tecnología Superior en Diseño de modas.

Dentro de lo que trata la misión del Instituto Superior Tecnológico es el de contribuir al desarrollo y estudio de la investigación, a través de la generación de conocimientos científicos y tecnológicos, de la misma manera la difusión y aplicación de ellos a la par con la aportación a la formación como investigadores de calidad. De igual manera la visión en sí reconoce al Instituto Superior Tecnológico Pelileo como una de las principales instituciones a nivel nacional, por su producción intelectual, generación de conocimiento en estudiantes y la contribución a la ciencia y sociedad, desde la perspectiva del desarrollo humano.

Dentro de este Instituto Superior Tecnológico se realiza un procedimiento de gestión de seguridad para las plataformas educativas, el cual cuenta con la plataforma Moodle la cual es una de las más utilizadas como ya se mencionó anteriormente. Esta plataforma ayuda tanto a docentes como estudiantes para la integración de materiales didácticos y recursos virtuales de educación.

El instituto cuenta con 382 estudiantes, estos se dividen en las tres carreras que tiene el instituto y estudiantes externos que cursan inglés, de igual manera para los docentes, los cuales son 36 en total los que utilizan la plataforma educativa institucional.

2.2. Metodología de investigación

En este apartado se da una explicación sobre la metodología de investigación que se usa y cómo este concepto para Cortés & Iglesias (2005), define a la metodología de la investigación como una ciencia que ayuda a los investigadores con una serie de métodos que abarca la recolección de información, ya sean; definiciones, principios y normativas las cuales permiten mostrar un método eficiente el cual demostrara la veracidad de un estudio o procesos de la investigación científica.

Método Analítico Sintético

Para Rodríguez & Pérez (2017), el método analítico sintético trata de un elemento filosófico dualista en el cual se divide en dos procesos que operan inversamente: el análisis y la síntesis. El método de análisis trata de un proceso específico que descompone información, la examina y se estudia cada parte determinada, ya sean cualidades o múltiples propiedades que esta compone. Mientras que el método sintético se refiere a una operación inversa sobre el estudio que establece una composición de un todo mediante partes previamente analizadas, por lo tanto, funciona como un proceso simple para definir características a partir de un análisis. Esta tiene específicamente lo necesario y justo para entender el tema que se desea mostrar.

Tipo de investigación

Investigación Bibliográfica

En este apartado se presenta una investigación y revisión bibliográfica de los elementos teóricos los cuales se realizó mediante recolección de información consultada en Google académico, Scopus y Microsoft Academic Search, en donde se recopiló datos tanto de revistas, libros y documentos de internet sobre temas de Ciberseguridad en plataformas educativas.

Por otro lado, se utilizó la herramienta tecnológica Zotero que ayudó a recopilar y organizar toda la información de los documentos investigados sobre el tema a tratar. Adicional se aplicaron métodos de análisis-síntesis para obtener conclusiones del objeto de estudio de manera inductiva y deductiva que permitieron analizar de lo general a lo específico y viceversa.

Investigación de Campo

Para Leyva Haza & Guerra Véliz (2020), esta investigación de campo trata de la recopilación de datos directamente de una población real y proporciona conocimiento directo de datos en base a un problema o situación en específico.

Este tipo de investigación ayuda en varios aspectos los cuales son la muestra de datos y resultados que se recopilaron mediante encuestas las cuales se realizaron a estudiantes y docentes y de igual manera se optó por efectuar una encuesta a los miembros de la unidad de TIC, para así recolectar información de todos los usuarios que manejan las plataformas educativas en el Instituto Superior Tecnológico Pelileo.

Técnicas e Instrumentos de recopilación

Para la recopilación de datos dentro del Instituto Superior Tecnológico Pelileo se usaron las siguientes técnicas e instrumentos que se detallaran a continuación:

- **Entrevista:** Esta técnica según Folgueiras (2016), sirve para una investigación cualitativa la cual recolecta datos que se deseen conocer, esta se define como una conversación que se propone con el fin de conocer la opinión sobre un tema en específico, el cual en este caso es sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional. Se plantea dentro de la entrevista, siete preguntas las cuales se enfocan en la utilización de la plataforma educativa y su seguridad, esta entrevista está dirigida directamente a los integrantes de la unidad de TIC, el instrumento de recopilación de datos se encuentra

en el Anexo 1, y las respuestas de cada entrevista son accesibles en el Anexo 11.

- **Encuestas:** Para esta encuesta se optó por realizar la escala de Likert la cual según Luna S (2007), trata de un estudio en grados de calificación que se utiliza en proyectos de investigación, más relacionados a cuestionarios los cuales sirven para conocer reacciones, actitudes o comportamientos de una persona. En base a lo planteado en este proyecto se realizaron dos encuestas, una para docentes y otra para estudiantes las cuales tendrán nueve preguntas basadas en la triada de seguridad que se dividen en tres según cada apartado que es: confidencialidad, integridad y disponibilidad. En base a esta escala que se optó como medida de recolección de datos, se muestra si los usuarios están totalmente de acuerdo o totalmente en desacuerdo en cuanto a la seguridad de las plataformas educativas. El instrumento recolección de datos se encuentra en el Anexo 10.

Población y muestra

La población que se determina abarca a los estudiantes, docentes y la unidad de TIC del Instituto Superior Tecnológico Pelileo.

Tabla 1. Datos generales de la población

Descripción	Total
Estudiantes	382
Docentes	36
Unidad de TIC	8

Fuente: elaboración propia

Para el cálculo de la muestra, se considera un universo finito, se toma como población a 382 estudiantes, de ellos se obtiene un valor al aplicar la fórmula respectiva, a este grupo se le orienta la primera encuesta; 36 docentes para la segunda encuesta y 7 personas de la unidad de TIC para la entrevista, de estos dos últimos grupos fueron evaluados todos.

Para calcular la muestra de los estudiantes se tienen las siguientes variables: un nivel de confianza del 1.96%, un 5% que corresponde al porcentaje de población

que no tiene el atributo, un 95% correspondiente al porcentaje de población que si tiene el atributo y un margen de error del 3.5%, para el cálculo de la muestra correspondiente se aplicó la siguiente formula:

Figura 4. Fórmula para el cálculo del tamaño de la muestra

$$n = \frac{Z^2 * N * p * q}{e^2 * (N-1) + (Z^2 * p * q)}$$

Fuente: Asedesto (2022)

Donde:

- Z = Nivel de confianza correspondiente a la tabla de valores Z

Figura 5. Tabla de valores de confianza

Valores de confianza tabla Z	
95%	1,96
90%	1,65
91%	1,7
92%	1,76
93%	1,81
94%	1,89

Fuente: Asedesto (2022)

- p = Porcentaje de la población que tiene el atributo deseado
- q = Porcentaje de población que no tiene atributo
- N = Tamaño del universo
- e = Error de estimación
- n = Tamaño de la muestra

Ingreso de datos

Tabla 2. Ingreso de datos

Z=	1,96
P=	95%
Q=	5%
N=	382
e=	4%

Fuente: Asedesto (2022)

Una vez ingresados los datos como se muestra en el cuadro anterior, se da como resultado una muestra para los estudiantes de n = 107.37, que es el número de encuestas que deberán aplicarse dentro del Instituto Superior Tecnológico Pelileo.

Análisis de la información recopilada

A continuación, se muestran los resultados de las técnicas e instrumentos aplicados con la población definida previamente:

Entrevista realizada a los integrantes de la unidad de TIC del Instituto Superior Tecnológico Pelileo

La entrevista se realizó a los integrantes de la unidad de TIC del instituto, que lo conforman 7 personas, las cuales fueron contactadas de manera personal para emitir sus criterios sobre cada pregunta, lo cual se logra evidenciar el modelo de la entrevista en el Anexo 3 y los resultados de la aplicación en el Anexo 4, y cuyo análisis es mostrado a continuación:

Pregunta 1. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?

- **Resumen**
  Los entrevistados mencionan como beneficios: el mitigar la información y resguardarse de una manera segura en la cual se prioriza dicha información para que se cree un beneficio de seguridad en las plataformas educativas.
- **Interpretación**
  En base a las respuestas, se menciona que los integrantes de la unidad de TIC se enfocan en el beneficio de seguridad de la información y cómo ésta es sumamente importante cuidarla para tener una mejor confianza dentro de las plataformas educativas.

Pregunta 2. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?

- **Resumen**

  Los entrevistados manifiestan aspectos como los datos personales de los estudiantes y su información académica en sí las cuales priorizan como importantes para ser resguardadas.
- **Interpretación**

  Estos aspectos mencionados en general son contundentes en cuanto a resguardar información dentro de las plataformas educativas, se centran en los estudiantes y su información la cual permanece privada y segura dentro de estos sistemas.

Pregunta 3. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?

- **Resumen**

  En la mayoría de los resultados consideran a la protección de datos sumamente importante, si el uso de esta es indebido perjudica a la institución y los propietarios de esta información.
- **Interpretación**

  En base a las respuestas se observa cómo la protección de datos de estudiantes y docentes es primordial para que no se logre cambiar ningún dato o este sea alterado, que ocasiona fallos de información.

Pregunta 5. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?

- **Resumen**

  Los resultados indican que la integridad de la información personal de la institución y todo lo que abarca datos en general de estudiantes y docentes que deban ser objetivos directos para un resguardo de información general.

- **Interpretación**

  Se menciona que la información en general de toda la institución tiene que ser más resguardada, al llevar así a que los datos estén completamente protegidos.

Pregunta 6. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?

- **Resumen**

  Creen que los beneficios son positivos, la información y datos de la institución permanecerán resguardados y se logra un mejor control de seguridad en cuanto a datos.
- **Interpretación**

  En base a las respuestas se menciona que la integridad de los datos tiene que resguardarse de una mejor manera al contar con un control de gestión el cual ayude a identificar vulnerabilidades y mitigarlas a tiempo.

Pregunta 7. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

- **Resumen**

  La mayoría de las respuestas se enfocan en el bienestar estudiantil y en cuanto el docente guarde información sin que esta sea alterada, para emitir así un control apropiado de seguridad, al crear un ambiente seguro en cuanto a la información personal de cada usuario de la institución.
- **Interpretación**

  Los conceptos y resultados son importantes, se centran en tener un ambiente óptimo que se encuentre resguardado por controles de seguridad de la información, al crear así un entorno resguardado en caso de ataques cibernéticos.

- **Resumen general de las entrevistas**

  Se observa cómo los docentes se preocupan de la información dentro de la plataforma, ya sean estas su información personal o más puntualmente en las notas y datos que estos logren ser cambiados o alterados por personas externas o internas. Un control de seguridad dentro de estas plataformas lleva a que los usuarios se sientan más seguros y logren navegar en un ambiente educativo positivo. De igual manera los estudiantes al no conocer mucho sobre estos daños cibernéticos se mantienen al margen y les preocupa más la información personal que la general en si de la institución.

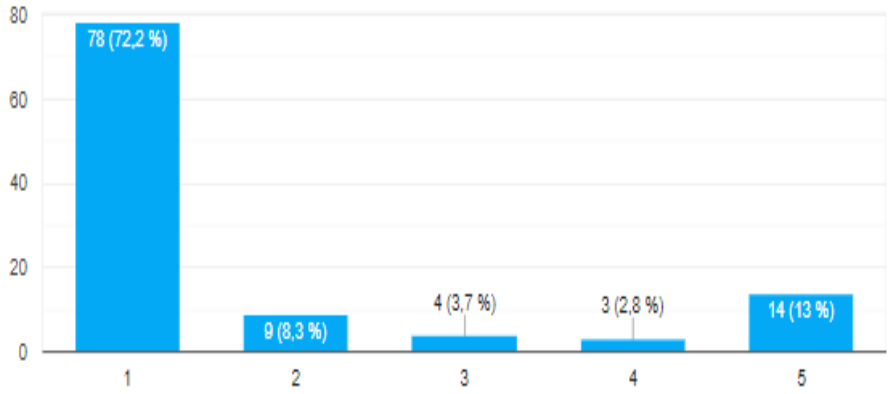
Encuesta realizada a los estudiantes del Instituto Superior Tecnológico Pelileo

Dentro de la recopilación de datos centrado en los estudiantes del Instituto Superior Tecnológico Pelileo se muestra las respuestas de cada pregunta planteada a continuación:

Pregunta 1. ¿Cree que su información dentro de su Plataforma Educativa debe permanecer privada?

1. Totalmente de acuerdo
2. De acuerdo
3. Indeciso
4. En desacuerdo
5. Totalmente desacuerdo

Gráfico 3. ¿Cree que su información dentro de su Plataforma Educativa debe permanecer privada?



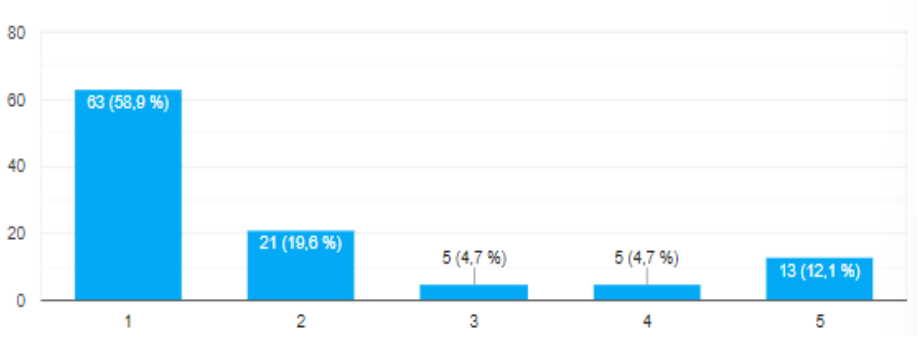
Fuente: elaboración propia

- **Interpretación**

  Se observa que el 72.2% de los estudiantes encuestados están totalmente de acuerdo en que la información dentro de la plataforma educativa debe permanecer privada, mientras que el 8.3% está de acuerdo, el 3.7% indeciso, el 2.8% desacuerdo y el 13% de estudiantes está totalmente desacuerdo con este tema. En base a esto se observa que un gran porcentaje está en una posición correcta la cual debería tener una institución, para que se mantenga segura y los estudiantes conozcan la importancia de sus datos e información.

Pregunta 2. ¿Cree que es riesgoso transmitir datos personales de usuario en entornos no seguros?

Gráfico 4. ¿Cree que es riesgoso transmitir datos personales de usuario en entornos no seguros?



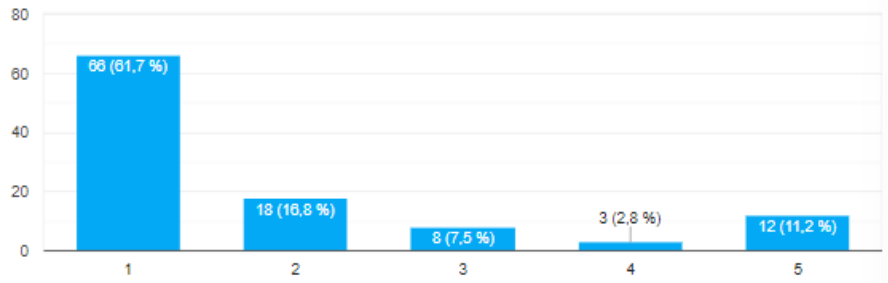
Fuente: elaboración propia

- **Interpretación**

  Se observa que el 58.9% de los estudiantes encuestados están totalmente de acuerdo en que es riesgoso transmitir datos personales del usuario en entornos no seguros, mientras que el 19.6% está de acuerdo, el 4.7% indeciso, el 4.7% desacuerdo y el 12.1% de estudiantes está totalmente desacuerdo con este tema. En base a esto se observa que un gran porcentaje de igual manera tiene el conocimiento correcto de que la información del usuario y sus credenciales son sumamente importantes, y se deben resguardar y no transmitirlas en entornos no seguros, se logra afectar a ese usuario y sus datos en sí.

Pregunta 3. ¿Piensa que su contraseña debe estar bien estructurada para tener una buena seguridad al acceso de sus cuentas?

Gráfico 5. ¿Piensa que su contraseña debe estar bien estructurada para tener una buena seguridad al acceso de sus cuentas?



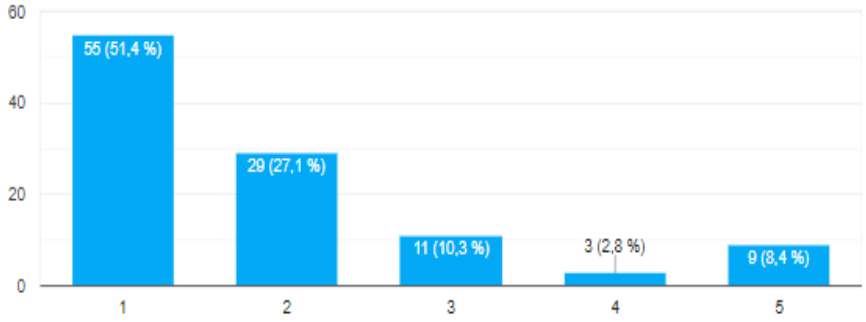
Fuente: elaboración propia

- **Interpretación**

  Se observa que el 61.7% de los estudiantes encuestados están totalmente de acuerdo en que la contraseña debe estar bien estructurada para tener una buena seguridad en los sitios *web* y plataformas educativas, mientras que el 16.8% está de acuerdo, el 7.5% indeciso, el 2.8% desacuerdo y el 11.2% de estudiantes está totalmente desacuerdo con este tema. En base a esto se observa de igual manera que un gran porcentaje de estudiantes ve la importancia de que la contraseña tiene ser bien estructurada para así protegerse de ataques de fuerza bruta o robo de credenciales.

Pregunta 4. ¿Cree que si le roban información personal presentará riesgos cibernéticos?

Gráfico 6. ¿Cree que si le roban información personal presentara riesgos cibernéticos?



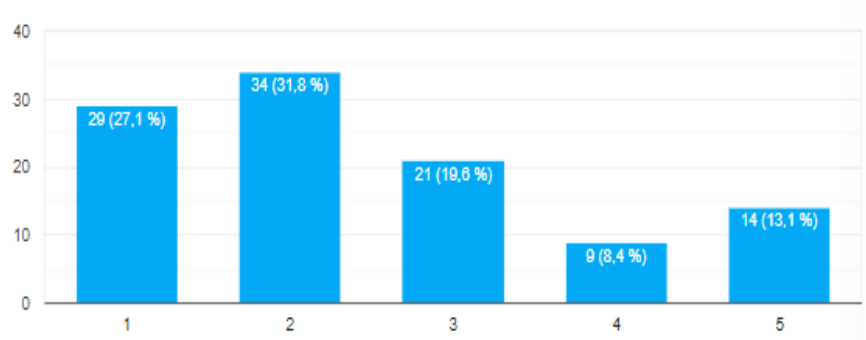
Fuente: elaboración propia

- **Interpretación**

  Se observa que el 51.4% de los estudiantes encuestados están totalmente de acuerdo en que si sufren un robo o ataque de ciberseguridad se presentará riesgos cibernéticos, mientras que de igual manera se ve un porcentaje alto del 27.1% está de acuerdo, el 10.3% indeciso, el 2.8% desacuerdo y el 8.4% de estudiantes está totalmente desacuerdo con este tema. En base a esto se observa que un gran porcentaje de igual manera está consciente de que su información personal al ser robada presenta riesgos los cuales perjudican a los usuarios a futuro.

Pregunta 5. ¿Sabe usted que, si su información ha sido cambiada o alterada, es específicamente por ataques o por descuidos personales?

Gráfico 7. ¿Sabe usted que, si su información ha sido cambiada o alterada, es específicamente por ataques o por descuidos personales?



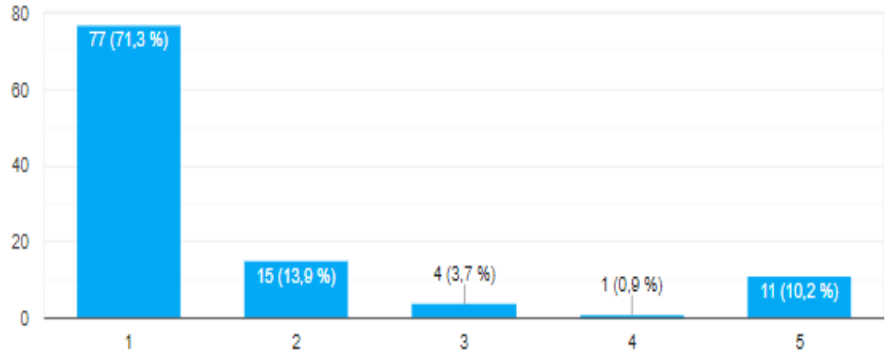
Fuente: elaboración propia

- **Interpretación**

  Se observa que el porcentaje mayor aquí es el número 2 con un 31.8% de los estudiantes encuestados están de acuerdo con la pregunta de conocimiento al saber si la información personal ha sido alterada y si esta es específicamente por ataques o descuidos personales, mientras que el 29.1% está totalmente de acuerdo, el 19.6% indeciso, el 8.4% desacuerdo y el 13.1% de estudiantes está totalmente desacuerdo con este tema. En base a esto se observa que un gran porcentaje se encuentra de acuerdo con que la información que sea alterada es específicamente por ataques cibernéticos o por descuidos personales ya sean estos como dejar sesiones iniciadas o compartidas sin el debido cuidado.

Pregunta 6. ¿Piensa que su información deberá estar siempre protegida en su Plataforma Educativa?

Gráfico 8. ¿Piensa que su información deberá estar siempre protegida en su Plataforma Educativa?



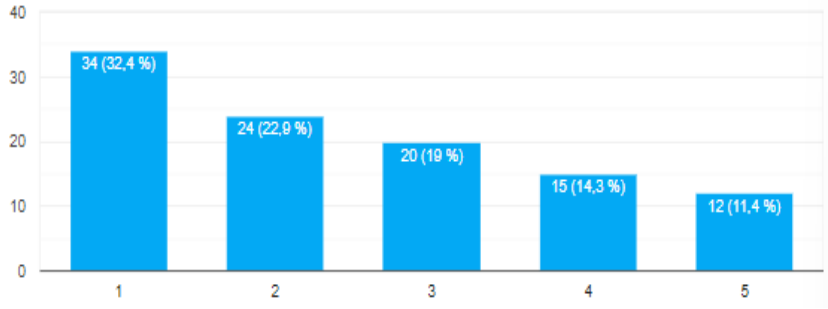
Fuente: elaboración propia

- **Interpretación**

  En este estudio se nota un porcentaje claramente mayor al tener el 71.3% de los estudiantes encuestados están totalmente de acuerdo con que su información debe estar protegida en la Plataforma Educativa, mientras que el 13.9% está de acuerdo, el 3.7% indeciso, el 0.9% desacuerdo y el 10.2% de estudiantes está totalmente desacuerdo con este tema. En base a esto se menciona como los estudiantes están preocupados con su información y como esta tiene que estar bien resguarda dentro de los recursos educativos.

Pregunta 7. ¿Al momento de utilizar su Plataforma Educativa ha percibido errores de carga?

Gráfico 9. ¿Al momento de utilizar su Plataforma Educativa ha percibido errores de carga?



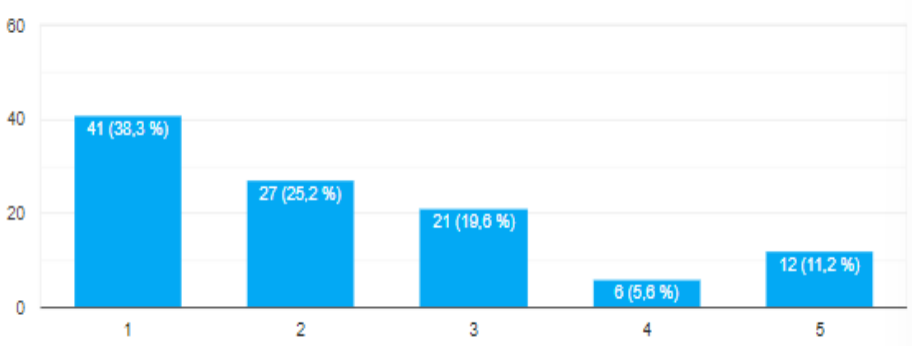
Fuente: elaboración propia

- **Interpretación**

  Se observa un 34.4% de los estudiantes encuestados están totalmente de acuerdo que cuando utilizan la plataforma educativa se ha percibido errores de carga, mientras que el 22.9% está de acuerdo, el 19% indeciso, el 14.3% desacuerdo y el 11.4% de estudiantes está totalmente desacuerdo con este tema. En base a esto se menciona que no es tanta la diferencia entre las opciones, pero de igual manera existe un gran porcentaje el cual nota que al momento de utilizar la plataforma educativa, ya sea para cargar datos o visualizar información, se note fallos de carga.

Pregunta 8. ¿Conoce que los ataques cibernéticos son los causantes de perjudicar la presentación de la información dentro de una Plataforma Educativa?

Gráfico 10. ¿Conoce que los ataques cibernéticos son los causantes de perjudicar la presentación de la información dentro de una Plataforma Educativa?



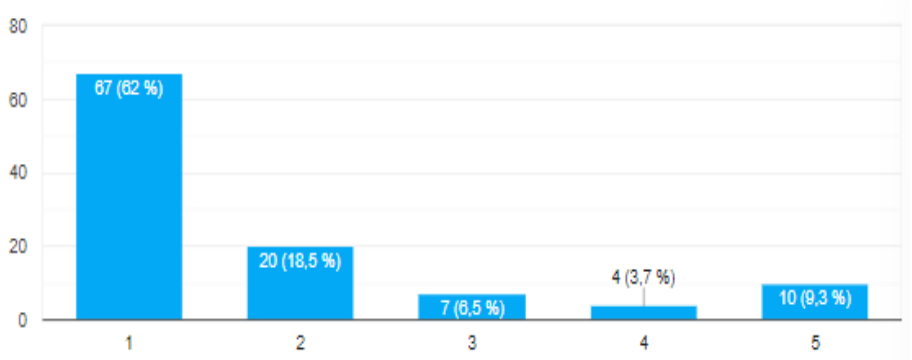
Fuente: elaboración propia

- **Interpretación**

  Se observa que el 38.3% de los estudiantes encuestados están totalmente de acuerdo en que los ataques cibernéticos son los causantes de fallos en las plataformas educativas, mientras que el 25.2% está de acuerdo, el 19.6% indeciso, el 5.6% desacuerdo y el 11.2% de estudiantes está totalmente desacuerdo con este tema. En base a esto se observa de igual manera que los estudiantes reconocen a los ciber atacantes como perjudiciales en la disponibilidad de la información dentro de las plataformas educativas.

Pregunta 9. ¿Piensa que se deben implementar medidas de seguridad para proteger la información dentro de su Plataforma Educativa?

Gráfico 11. ¿Piensa que se deben implementar medidas de seguridad para proteger la información dentro de su Plataforma Educativa?



Fuente: elaboración propia

- **Interpretación**

  En base a la última pregunta se observa que el porcentaje con mayor diferencia del 62% de los estudiantes encuestados están totalmente de acuerdo en que se debe tener medidas de seguridad en las plataformas educativas, mientras que el 18.5% está de acuerdo, el 6.5% indeciso, el 3.7% desacuerdo y el 9.3% de estudiantes está totalmente desacuerdo con este tema. En base a esto se menciona que los estudiantes piensan que es necesario implementar medidas de seguridad para proteger la información dentro de su plataforma educativa, para así sentirse resguardados en un entorno cibernético.

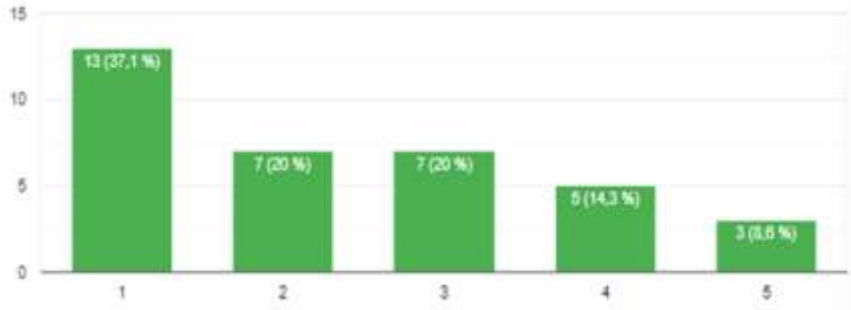
Encuesta realizada a los docentes del Instituto Superior Tecnológico Pelileo

Dentro de la recopilación de datos centrado en los docentes del Instituto Superior Tecnológico Pelileo se muestra las respuestas de cada pregunta planteada a continuación:

Pregunta 1. ¿Cree que la información o material que sube en su Plataforma Educativa está completamente seguro?

1. Totalmente de acuerdo
2. De acuerdo
3. Indeciso
4. En desacuerdo
5. Totalmente desacuerdo

Gráfico 12. ¿Cree que la información o material que sube en su Plataforma Educativa está completamente seguro?



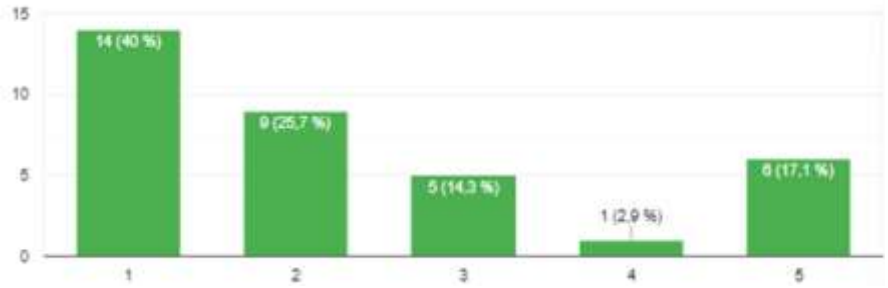
Fuente: elaboración propia

- **Interpretación**

  En este caso los resultados se observan que el 37.1% de los docentes encuestados están totalmente de acuerdo en que la información o material cargado a la plataforma educativa está totalmente segura, mientras que el 20% está de acuerdo, el 20% indeciso, el 14.3% desacuerdo y el 8.6% de docentes está totalmente desacuerdo con este tema. En base a esto se hay que mencionar que ese porcentaje no es tan lejano a los dos siguientes, para tener en cuenta que la mayoría de los docentes sienten que su información y material que suben ya sea notas, trabajos o actividades para los estudiantes, está completamente seguro.

Pregunta 2. ¿Considera importante implementar seguridad en el material y links que utiliza en actividades educativas?

Gráfico 13. ¿Considera importante implementar seguridad en el material y links que utiliza en actividades educativas?



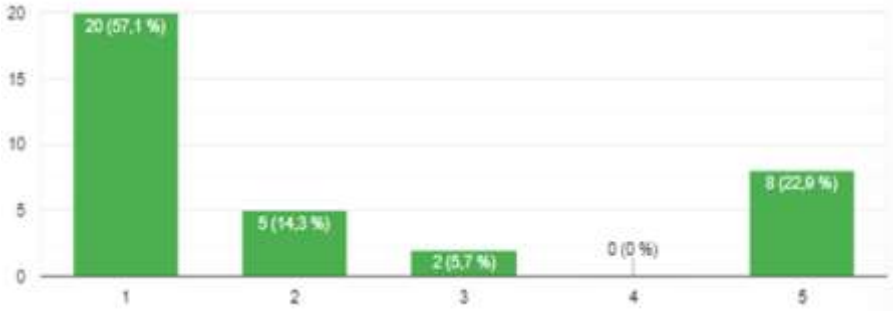
Fuente: elaboración propia

- **Interpretación**

  Se nota que el 57.1% de los docentes encuestados están totalmente de acuerdo en considerar implementar seguridad en el material y links que se utilicen en los recursos educativos, mientras que el 25.7% está de acuerdo, el 14.3% indeciso, el 2.9% desacuerdo y el 17.1% de docentes está totalmente desacuerdo con este tema. Se define de esta manera que un gran porcentaje de docentes considera sumamente importante implementar seguridad en la información que se cargue en la plataforma educativa ya sea links o el material en sí, al llevar que se sientan seguros de que ninguna de esta información logre ser perjudicada.

Pregunta 3. ¿Considera que su contraseña debe estar bien estructurada para tener una buena seguridad al acceso de sus cuentas?

Gráfico 14. ¿Considera que su contraseña debe estar bien estructurada para tener una buena seguridad al acceso de sus cuentas?



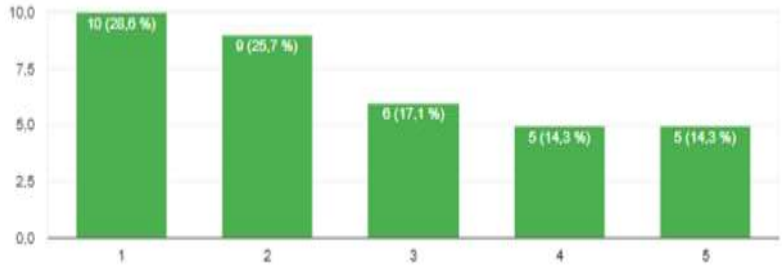
Fuente: elaboración propia

- **Interpretación**

  Se observa que el 57.1% de los docentes encuestados están totalmente de acuerdo en tener una contraseña bien estructurada, mientras que el 14.3% está de acuerdo, el 5.7% indeciso, el 0% desacuerdo y el 22.9% de docentes está totalmente desacuerdo con este tema. Se observa como la mayoría de los docentes al saber la importancia de los datos personales que tienen en sus cuentas y los permisos para modificar información, consideran que la contraseña debe estar bien estructurada para tener mayor seguridad al acceso de sus cuentas.

Pregunta 4 ¿Cree que toda su información dentro de la plataforma Educativa institucional está totalmente correcta y segura?

Figura 1: ¿Cree que toda su información dentro de la plataforma Educativa Institucional está totalmente correcta y segura?



Fuente: elaboración propia

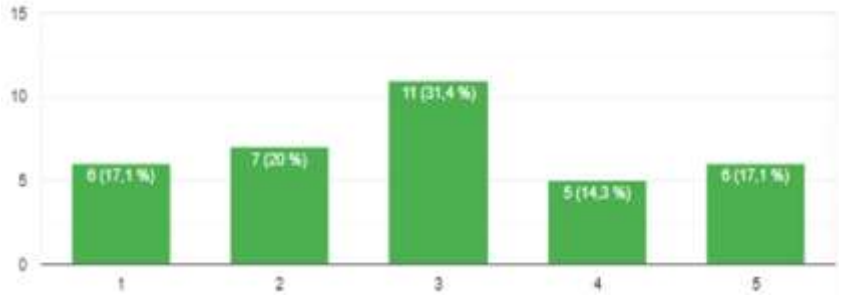
- **Interpretación**

  En esta pregunta se observa que no existe tanta diferencia entre los resultados de las respuestas, se superan por pocas cifras para empezar con el 28.6% de los docentes encuestados están totalmente de acuerdo en que la información que está dentro de la plataforma educativa está resguardada, mientras que el 25.7% está de acuerdo, el 17.1% indeciso, el 14.3% desacuerdo y el 14.3% de docentes está totalmente desacuerdo con este. tema. Se observa claramente que no existe tanta discrepancia en cuanto a resultados de estar o no de acuerdo en creer que la información dentro de la plataforma educativa institucional permanece correcta y segura. Al notar que la primera opción tiene el mayor porcentaje de conformidad, los demás resultados muestran una diferencia no tan mayor y se cuestiona sobre si de

verdad se encuentra resguardada y en términos correctos la información dentro de las plataformas educativas.

Pregunta 5. ¿Sabe usted que cuando su información ha sido cambiada o alterada, es específicamente por ataques o por descuidos personales?

Gráfico 15. ¿Sabe usted que cuando su información ha sido cambiada o alterada, es específicamente por ataques o por descuidos personales?



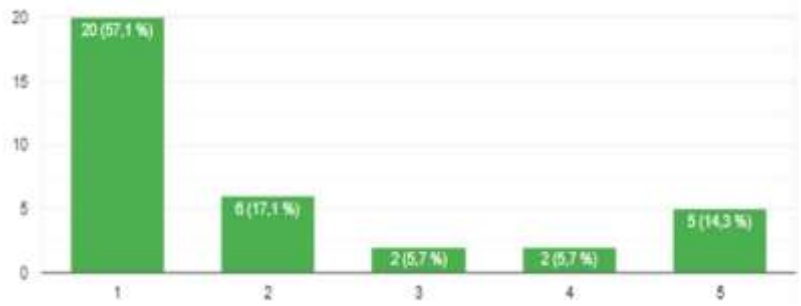
Fuente: elaboración propia

- **Interpretación**

  En este caso la cifra respuesta con mayor porcentaje es el de 31.4% de los docentes encuestados están indecisos en que la información cuando es alterada específicamente es por atacantes o descuidos personales, mientras que el 17.1% está de totalmente de acuerdo, el 20% de acuerdo, el 14.3% desacuerdo y el 17.1% de docentes está totalmente desacuerdo con este. tema. Se observa una respuesta la cual es muy cuestionada en parte de los docentes, es o no que la información que se haya alterado sea responsable directo de los atacantes cibernéticos o por descuidos personales que lleven a una infiltración a datos restringidos que perjudique así al usuario y su información.

Pregunta 6. ¿Considera que su información y material de trabajo deberá estar siempre protegido en la Plataforma Educativa?

Gráfico 16. ¿Considera que su información y material de trabajo deberá estar siempre protegido en la Plataforma Educativa?



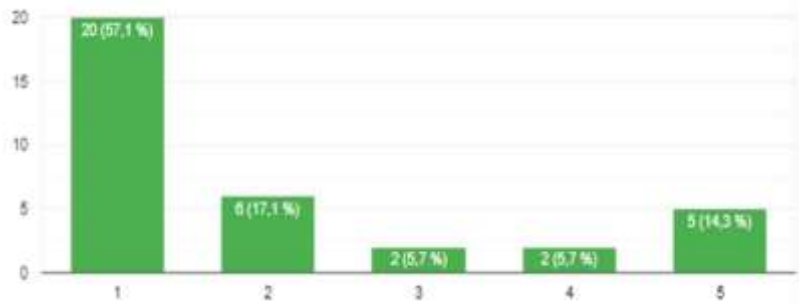
Fuente: elaboración propia

- **Interpretación**

  Se observa que el 57.1% de los docentes encuestados están totalmente de acuerdo en que la información que suben y se presenta en las plataformas educativas deberá permanecer segura, mientras que el 17.1% está de acuerdo, el 5.7% indeciso, el 5.7% desacuerdo y el 14.3% de docentes está totalmente desacuerdo con este tema. Con estos datos se observa como la mayoría de los docentes reconocen que los materiales e información en general que se sube a la plataforma educativa deberá ser resguardada de forma educada para que no existan fallos o cambios en ella.

Pregunta 7. ¿Al momento de utilizar su Plataforma Educativa ha percibido errores de carga o caída del sistema?

Gráfico 17.¿Al momento de utilizar su Plataforma Educativa ha percibido errores de carga o caída del sistema?



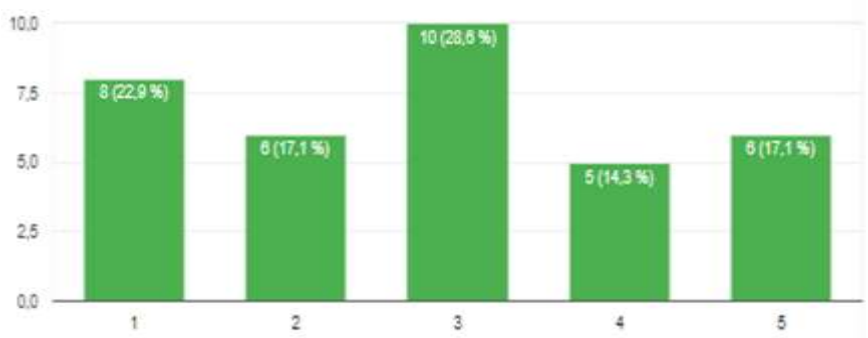
Fuente: elaboración propia

- **Interpretación**

  Se observa que el porcentaje más alto con 34.3% de estar totalmente de acuerdo, pero con no tanta diferencia del 31.4% de indecisos, detalla cómo los docentes encuestados están en su mayoría totalmente de acuerdo en al momento de utilizar la plataforma educativa ha ocurrido algún error o fallo de este, mientras que el 5.7% está de acuerdo, el 14.3% desacuerdo y de la misma manera con 14.3% de docentes está totalmente desacuerdo con este tema. En base a estos resultados se observa cómo en gran mayoría los docentes se enfrentan a fallos o errores dentro de la plataforma educativa ya sea que no se cargue la página o esté mal configurada, lo que causa inconvenientes al momento de manejar esta herramienta.

Pregunta 8 ¿Cree que los ataques cibernéticos son los causantes de perjudicar la presentación de la información dentro de la Plataforma Educativa?

Gráfico 18. ¿Cree que los ataques cibernéticos son los causantes de perjudicar la presentación de la información dentro de la Plataforma Educativa?



Fuente: elaboración propia

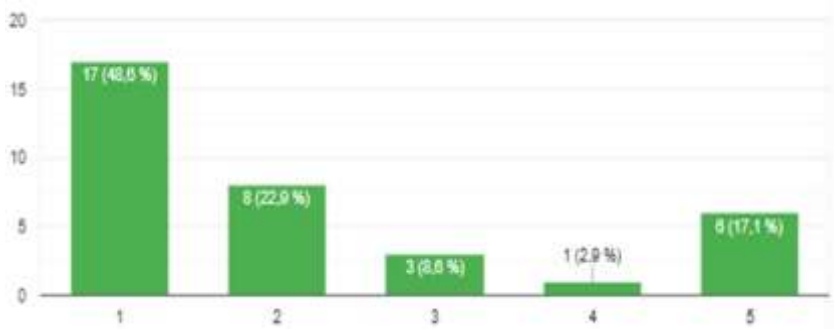
- **Interpretación**

  Se observa en esta pregunta como la predominante es la respuesta tres con un 28.6% de los docentes encuestados están indecisos en saber si los ataques cibernéticos son los causantes de perjudicar la disponibilidad de la información, mientras que el 22.9% está totalmente de acuerdo, el 17.1% de acuerdo, el 14.3% desacuerdo y el 17.1% de docentes está totalmente desacuerdo con este tema. Donde se considera así a que los docentes no sepan exactamente por qué la información que no se presente o tenga fallos

dentro de la plataforma educativa, no sea específicamente por ataques cibernéticos si no para considerar otros factores para que esto ocurra.

Pregunta 9. ¿Piensa que se deben implementar medidas de seguridad para proteger la información dentro de su Plataforma Educativa?

Gráfico 19. ¿Piensa que se deben implementar medidas de seguridad para proteger la información dentro de su Plataforma Educativa?



Fuente: elaboración propia

- **Interpretación**

  En esta última pregunta se observa que el 48.6% de los docentes encuestados están totalmente de acuerdo en que se debe implementar medidas de seguridad en las plataformas educativas, mientras que el 22.9% está de acuerdo, el 8.6% indeciso, el 2.9% desacuerdo y el 17.1% de docentes está totalmente desacuerdo con este tema. Con estos datos se observa como la mayoría de los docentes piensa que si es necesario completamente una implementación de medidas y normas que ayuden a resguardar la información dentro de las plataformas educativas.

2.3. Metodología de desarrollo

En base a los objetivos planteados y la importancia de que exista un control para gestionar riesgos de ciberseguridad dentro de institutos educativos. Según Morales & Medina (2021), se plantea una metodología para la Gestión de riesgos de ciberseguridad dentro de IST.

Figura 6. Fases de Procedimiento Gestión de Ciberseguridad para plataformas educativas.

Fuente: Morales & Medina (2021)

El siguiente proceso de gestión contiene 6 fases, las cuales, se inician desde definir objetivos de seguridad hasta identificarlos, seleccionarlos y generar sus respectivas salvaguardas o procedimientos de mitigación a ataques o políticas mal estructuradas dentro de una institución educativa.

De acuerdo con el análisis de la metodología de gestión del control de ciberseguridad, se opta por la implementación de esta metodología en el Instituto Superior Tecnológico Pelileo, se estructura un plan específicamente en sus plataformas educativas a través de objetivos y fases generales que permitan resguardar información y tener un buen control de seguridad en sí de la institución.

Fase 1: DEFINIR OBJETIVOS DE CIBERSEGURIDAD

Para esta definición de objetivos se lleva a cabo como partida la conceptualización de términos de ciberseguridad, se detalla de manera primordial a los datos institucionales como datos sensibles que se deben proteger y resguardar. Esta fase se empieza desde el contexto de la unidad de TIC, el cual define lineamientos y permisos que permitan resguardar la información y resolver problemas de seguridad dentro de la infraestructura.

De acuerdo con la metodología utilizada, los autores determinan el desarrollo de los siguientes procesos en esta fase:

1. **Implementar la Unidad de Gestión de Ciberseguridad dentro de la Institución**

Este primer punto es importante, por cuanto el contar dentro de una organización con la Unidad de gestión de ciberseguridad, la cual permita mitigar varios procedimientos de amenazas cibernéticas, para tener en cuenta a un equipo especializado en esta área de protección de información que se genera y procesa a través de ordenadores y sistemas que posee el Instituto.

Se toma como base lo anterior, para el desarrollo de este punto se han considerado como insumos:

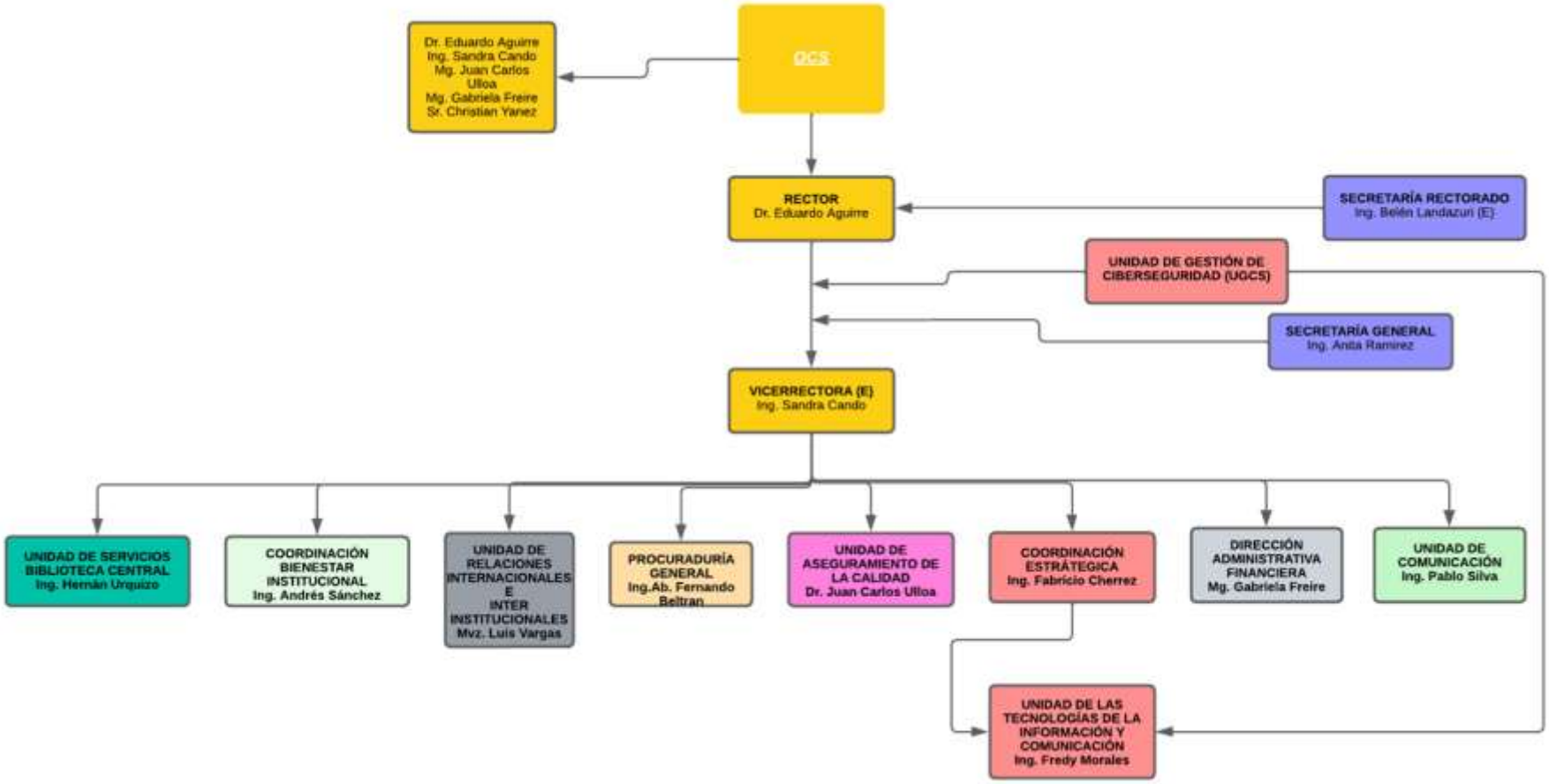
1. El Organigrama estructural del Instituto el mismo que está disponible en el anexo 5, y que muestra que, dentro de la estructura de la institución, existe la unidad de las Tecnologías de la Información y Comunicación dentro de la Coordinación estratégica, lo cual evidencia que el desarrollo de las TIC y su gestión tiene injerencia a nivel estratégico en la organización.
2. Si bien no existe un organigrama de la Unidad de Tecnologías de la Información y Comunicación, sí se cuenta con el Estatuto para el Instituto Superior Tecnológico Pelileo (Morales & Lezano 2019), dentro del cual el Artículo 62 y el Artículo 63 establecen la estructura y funciones de la Coordinación Estratégica en donde se resalta que la Unidad de Tecnología tiene que tener varias atribuciones, de las cuales se resaltan los siguientes literales que tienen relación con la seguridad de la información y la gestión de plataformas educativas:
    - Literal i) Asesorar y capacitar a las áreas académicas, administrativas y de apoyo y asesoría en temas relacionados a tecnologías de la información y comunicación;
    - Literal m) Velar por la seguridad y disponibilidad de la información generada por el Instituto;
    - Literal o) Crear y administrar entornos virtuales de aprendizaje según las necesidades de los procesos sustantivos de la formación técnica y tecnológica;

Con estos antecedentes, y al tomar como base los sustentos teóricos referentes a la importancia de la Ciberseguridad dentro de las organizaciones, se propone la creación de la Unidad de Gestión de Ciberseguridad (UGCS), la misma que a nivel estructural y funcional tiene las siguientes características:

1. La UGCS depende estructuralmente de la máxima autoridad de la Institución, que en este caso es el Rector del IST Pelileo, esto debido a que se requiere de la toma de decisiones importantes con un alto nivel de confidencialidad por lo que es importante contar directamente con el apoyo directivo. Si bien anteriormente se había manifestado que la metodología recomienda que la UGCS forme parte de la unidad de TIC Institucional, para la investigación no se considera ésta como la mejor opción debido a que la Unidad de Tecnologías de la Información y Comunicación está descentralizada en distintas instituciones que forman parte del grupo académico del Instituto.
2. Está integrado por: el Rector del Instituto y el jefe de la Unidad de Tecnologías de la Información y Comunicación, además se contempla la posible participación de asesores externos en áreas específicas de Ciberseguridad que fueran requeridos, esto por cuanto la institución no dispone de los recursos estatales para crear una unidad como tal con personal especializado de planta.

Gráfico Del Organigrama con la UGCS

Figura 7. Organigrama con la Implementación del UGCS



Fuente: elaboración propia

3. Las funciones que cumple la UGCS están enmarcadas en los siguientes aspectos en concordancia con las atribuciones mencionadas anteriormente del Estatuto, además toman como base los lineamientos establecidos por la ISO27032 y Magerit que fueron el sustento de la Metodología utilizada:

    a. **Prevención de incidentes informáticos:** Implementar políticas, normas programas y softwares que prevengan diferentes amenazas existentes, las cuales perjudican al IST.
    b. **Identificación de recursos de sistemas informáticos**: Proteger los recursos o activos de información del IST
    c. **Detección de la información**: Identificar los riesgos asociados a los activos de información críticos para la implementación de controles destinados a la gestión de ciberseguridad.
    d. **Protección de la Información**: Implementar salvaguardas para protección de la información ante ciberamenazas; monitorear eventos inusuales que dañen los sistemas, para identificarlos y solventarlos.
    e. **Respuesta y Aviso de incidentes:** Implementar medidas que reduzcan el impacto de amenazas y ayuden a tener un entorno seguro.
    f. **Recuperación y Aprendizaje:** Tomar acciones correctas y seguras para restaurar los sistemas informáticos o servicios tecnológicos que pudieran ser afectados, definir procedimientos para reducir la probabilidad de incidentes los cuales dañan estos sistemas.

2. Crear una Norma de Ciberseguridad Institucional

Para la creación de la Norma de Ciberseguridad del IST, se han tomado como base los lineamientos establecidos en la Norma ISO 27032 y en Magerit V3.0; además, es importante contemplar la misión y visión institucionales para que la norma aporte de manera estratégica a su cumplimiento y desarrollo.

El documento se refiere en el Anexo 6, el mismo que ha sido estructurado en base a los siguientes aspectos:

- Antecedentes
- Objetivos
- Importancia
- Contexto Normativo
- Seguridad de la información
- Responsabilidades
- Políticas, normas y procesos de la seguridad de la información
- Glosario de términos y definiciones

3. Alinear los Procesos de Gestión de Seguridad Dentro del Plan Operativo Anual

El Plan Operativo del IST Pelileo que se encuentra en ejecución actualmente corresponde al año 2022, y fue proporcionado por funcionarios de la institución, contempla funciones, objetivos, criterios, subcriterios, indicadores, planes de proyectos / actividades y porcentajes de cumplimiento.

Por otra parte, dentro de la Norma de Ciberseguridad Institucional presentada en el punto anterior, se consideraron los distintos procesos que permiten el cumplimiento de las políticas y normas definidas.

Se toma como base los Procesos detallados; en este apartado, se desarrolla una matriz que permite evidenciar cómo dichos procesos de la Política de Ciberseguridad deben estar alineados con el POA del IST “Pelileo”, para identificar los diferentes recursos de ciberseguridad necesarios en la institución, además de establecer buenas prácticas de ciberseguridad.

El POA cuenta con 6 funciones sustantivas las cuales tienen indicadores específicos de sus áreas y muestran cómo son ejecutadas. Para la unión de los procesos con los indicadores del POA se consideraron los 9 procesos definidos, los cuales se evalúan según una escala de Likert que valora el nivel de importancia dentro del ámbito de ciberseguridad. La escala usada es la siguiente:

0. No aplica
1. No es importante
2. Poco importante
3. Algo importante
4. Importante
5. Muy importante

A continuación de muestra la matriz resultante:

Figura 8. Matriz de Procesos de Gestión de Seguridad dentro del POA

Procesos de Gestión de Seguridad dentro del POA	Procesos	Proceso Control de Cuentas de Usuarios	Proceso Control de Permisos en Dispositivos	Proceso Control de Contraseñas	Proceso Control de Dispositivos Externos	Proceso Control de Conexiones	Proceso Control de Información	Proceso Control de Firewall	Proceso Control de Navegación en Internet	Proceso Control de Hardware y Software
POA										
Selección de docentes y personal administrativo		4	5	5	2	5	5	2	4	3
Entorno Virtual de Aprendizaje (EVA)		4	3	4	4	3	5	2	5	4
Informe estadístico del uso de la plataforma virtual (SIGA)		5	3	5	2	4	4	3	4	3
Aplicaciones y paquetes informáticos generales y específicos.		3	0	0	0	2	3	4	3	2
Actualización del sistema informático		2	2	1	1	3	4	2	5	3
Web institucional		5	4	5	3	3	4	4	4	2
Código de ética de la institución		5	5	4	3	3	5	2	3	2
Captación de información sobre apreciaciones de los integrantes de la comunidad educativa		4	3	3	2	1	3	0	3	0
Registros de inspecciones de seguridad (captados a través del aplicativo SIIES)		4	4	3	4	4	5	3	5	4

Fuente: elaboración propia

Se interpreta que dentro de los Procesos Operativos el que tiene mayor importancia es el de “Registros de inspecciones de seguridad (captados a través del aplicativo SIIES)”, cuenta con un nivel de importancia alto en cuanto a relación de los procesos en general, como siguiente resultado en cuanto a los procesos, se tiene al más importante el de “Control de información”, que se obtiene como resultado, que dentro de estos alineamientos el enfoque de la información y su control son fundamentales en el IST para tener una buena ciberseguridad.

4. **Permitir procesos de autogestión para resolver problemas de seguridad en las infraestructuras tecnológicas.**

Frente al análisis realizado en el punto anterior, y con base en la estructura y normativa propuesta para la gestión de ciberseguridad institucional, se establece que la mejora manera de cumplir los objetivos propuestos es a través de procesos de capacitación dentro del IST Pelileo, los cuales sirven a futuro para concientizar a docentes, estudiantes y personal administrativo para tener un enfoque amplio y preciso sobre lo que involucra la seguridad de la información y de los datos en sí.
Al respecto, mediante la gestión y convenios con instituciones públicas y privadas se logra la participación de capacitadores en áreas como:

- Seguridad y protección de datos personales: dirigido a docentes, estudiantes y personal administrativo
- Ingeniería Social: dirigido a docentes, estudiantes y personal administrativo
- Buenas prácticas de ciberseguridad en instituciones educativas: dirigido a docentes, estudiantes y personal administrativo.
- Seguridad en redes e infraestructura: dirigido a personal del departamento administrativo y de tecnología
- Seguridad en aplicaciones y sitios *web*: dirigido a docentes, estudiantes y personal administrativo
- Seguridad en el uso de dispositivos móviles: dirigido a docentes, estudiantes y personal administrativo
- Entre otras temáticas

Además, es necesario el desarrollo por parte del departamento de tecnología, de una guía de buenas prácticas para los usuarios y que dentro de la plataforma educativa no exista inconvenientes en cuanto a ataques cibernéticos, para esto las personas estarán capacitadas para el uso y funcionamiento de sus procesos dentro de este sistema y cualquier otro dentro de la institución.

Fase 2: IDENTIFICAR INFRAESTRUCTURA TECNOLÓGICA A PROTEGER

En cuanto a la infraestructura, se identifican los activos de información y se clasifican en tangibles e intangibles; además, se realiza un Análisis de Riesgos, en donde se valoran los activos de información. Para ello, se toma como base la ISO 27000:2013, se considera la Triada CID, para el análisis de los activos de información, de tal manera que:

- La Confidencialidad, clasifica a la información en: reservada, clasificada o pública;
- La Integridad se valora como alta, media y baja;
- La Disponibilidad de igual manera que en la Integridad se valora como alta, media y baja.

En base a estos tres parámetros, se valora la información de tal manera que si existe un ítem que no clasifica, hace referencia a aquel que no pertenece o se asocia a estos términos.

Cuadro 7. Clasificación de activos

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Tomado a partir de la Norma ISO27000:2013

Luego del análisis de los factores de la triada CID frente a los activos de información, se define el nivel de riesgo, de tal manera que se considera que el riesgo es Alto, cuando los activos tienen una clasificación alta en 2 o más propiedades del CID; el riesgo es Medio cuando los activos informáticos se clasifiquen como Media, en 1 o menos elementos de la triada; y por último el riesgo es Bajo cuando todas las valoraciones en todos sus niveles sean bajos.

En base a lo mencionado, se valora como riesgo alto en aquellos activos de información que al no estar operativos de una manera adecuada, la institución corre el riesgo de suspender sus servicios académicos y por tanto no funcionar de

manera correcta; cuando el riesgo es medio, se verían afectadas ciertas operaciones importantes pero no necesariamente implica una suspensión total del funcionamiento de la institución; cuando el riesgo es bajo, los activos afectados tienen relación con operaciones que se desarrolla sin problema una vez se restauran los servicios. Este análisis pretende aclarar la valoración de riesgo sin restar importancia a todos los procesos vinculados a todos los activos de información identificada.

En base a lo mencionado anteriormente, se crea a continuación un cuadro el cual se enfoca en identificar infraestructuras tecnológicas a proteger su clasificación correspondiente:

Cuadro 8. Identificación de Infraestructuras Tecnológicas a Proteger

Activo de Información	Descripción	Tipo	Clasificación
Plataforma Moodle	En el IST Pelileo**,** la plataforma que utilizan es Moodle 3.8, la cual trata de una plataforma de gestión de aprendizaje que se utiliza en todo el mundo con fines educativos.	Intangible	Alta
SIGA Institucional	Existe el Sistema Integrado de Gestión Administrativa- por sus siglas (SIGA), que es una "herramienta que simplifica y automatiza los procesos administrativos en una entidad y sigue las normas establecidas por los Órganos Rectores de los Sistemas Administrativos del Estado", según Chicoma Palacios (2019)	Intangible	Media
Página Web Institucional	La página *web* Institucional cuenta con un hostin ilimitado que les provee ecuahostin.	Intangible	Media
Servidor Web	A lo que se refiere Infraestructura dentro del Instituto cuentan con un servidor *web* de sistema operativo Linux, CentOS 7, este servidor está específicamente destinado a las aulas virtuales. Dentro de él se manejan aproximadamente 800 usuarios.	Tangible	Alta
Servidor de aplicaciones	En este servidor físico maneja el mismo sistema operativo que es CentOS, y dentro de este servidor se implementa el repositorio de la biblioteca institucional.	Tangible	Media
WLan Controler	Este controlador de red que tiene la institución soporta 16 antenas inalámbricas y tiene un servidor mikrotik es cual es un *software* que trabaja como sistema operativo.	Tangible	Media
Nube Siga	Dentro de lo que compone el sistema SIGA, dentro del instituto se tiene un servidor en la nube que provee CNT y el SENESCYT.	Intangible	Media
Nube Página Web	La página *web* del IST tiene su información dentro de la nube en acuahostin el cual se da espacio para sus datos.	Intangible	Media

Fuente: elaboración propia

Como se observa las infraestructuras con mayor grado de clasificación, son las que muestran, guardan y suben información del IST, estos datos que son manejados por estos servidores físicos y en la nube, son los que deben tener alta disponibilidad, integridad y confiabilidad, es la que los usuarios manejan siempre y tanto docentes como estudiantes y personal administrativo estarán en dependencia de esta información en todo momento.

Fase 3: SELECCIONAR INCIDENTES DE SEGURIDAD MÁS COMUNES EN LAS APLICACIONES WEB

Dentro de lo que conlleva la selección de incidentes de ciberseguridad más comunes en las aplicaciones *web* dentro del IST “Pelileo”, por medio de una entrevista a Morales (2022), se detalla los siguientes aspectos; incidentes en el cual se detalla los más comunes, continuamente de la descripción de este y la frecuencia la cual con una escala de Likert se mide si es Muy Frecuente, Frecuentemente, Ocasionalmente, Raramente y Nunca. Mientras que el impacto se mide en Alto, Medio y Bajo:

Cuadro 9: Incidentes de Seguridad más Comunes

Incidente	Descripción	Frecuencia	Impacto
Disponibilidad en SIGA	De acuerdo con la evidencia existente en la unidad de TI del IST Pelileo, han existido reportes de usuarios respecto a eventos en los cuales el sistema SIGA se cuelga y no está disponible. Si bien se han tomado correctivos las fallas se mantienen.	Frecuentemente	Medio
Página Web	Se han registrado en la unidad de TI ataques DDoS a la página *web* institucional, lo que ha ocasionado pérdida del servicio.	Frecuentemente	Alta
Plataforma Virtual	Existen frecuentes reportes de usuarios de ingresos no deseados y de vulneración de la integridad de la información de algunos de ellos, situación que se da debido al incumplimiento de la política de gestión y manejo de contraseñas, que establece que los usuarios deben actualizarla una vez que se les asigne una contraseña genérica.	Ocasionalmente	Media

Fuente: elaboración propia

Fase 4: IDENTIFICAR LAS VULNERABILIDADES DEL IST

Para la siguiente fase en donde se va a identificar vulnerabilidades dentro del sistema del IST Pelileo, se procedió a solicitar permisos a la unidad de TIC del instituto, el cual permitió que se gestionen estos ataques de hackeo ético para comprobar las vulnerabilidades de cada página *web* y sistema que se ocupe dentro del instituto. Estas vulneraciones se basan como principio las fases del Hacking Ético las cuales detalla EHACK (2022), como 5 fases las cuales un hacker de sombrero blanco tiene que realizar para comprobar vulnerabilidades de algún sistema informático.

Como Primera parte se utilizó Kali Linux el cual trata de un sistema operativo utilizado para los ataques cibernéticos y se especifica en temas de seguridad. Este sistema se instaló en una máquina virtual y se utilizó la terminal para ingresar el comando UNISCAN, esta herramienta ayuda con pruebas de seguridad sobre aplicaciones *web* y direcciones Ip externas, las mismas que comprueban vulnerabilidades como secuencias de comandos de sitios cruzados y otras vulnerabilidades explotables. Esta rastrea automáticamente páginas en internet y realiza una técnica de hacking considerada como caja gris la cual revela riesgos que comprometan el sitio *web* y su información.

Se usó una herramienta llamada Legion que es muy conocida por la forma de auditar alguna página o sitio *web*, Legion enumera puertos y servicios que estén abiertos para realizar un *pentesting* de todo el sistema.

De igual manera se usó una herramienta *web* gratuita la cual se llama SUCURI, consiste en un sitio de escáner de seguridad y *malware* de páginas *web*, se realiza pruebas de SPAM inyectado, desconfiguraciones, y ataques a fuerza bruta, donde se muestra un listado de vulnerabilidades.

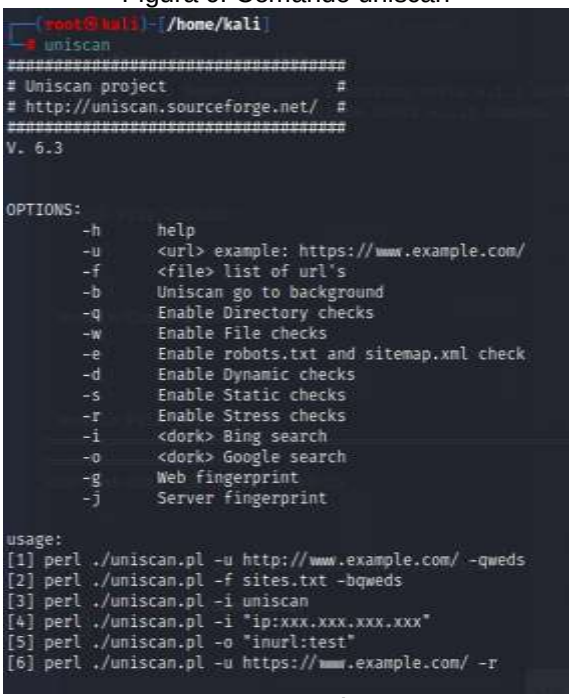
Para el primer caso se va a vulnerar La Plataforma Web Institucional, esta muestra datos del instituto como; las carreras y áreas que tienen, la redirección a aulas virtuales, bibliotecas y matrículas que son procesos que mediante esta página se

gestiona y de igual manera cuenta con enlaces secundarios que llevan a otros servicios institucionales como son el del Aula Virtual (Moodle) y el SIGA, los cuales serán vulnerados posteriormente.

PRIMERA PARTE: Análisis comando uniscan en Kali Linux

Para este proceso se ingresó a la máquina virtual donde se tiene instalado la imagen del sistema operativo de Kali Linux, posteriormente se abre la terminal y se ingresa el comando uniscan, el cual muestra las opciones que este tiene y la manera en la que se tiene que escribir el comando siguiente para que comience el análisis de vulnerabilidades.

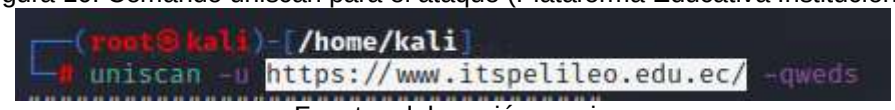
Figura 9. Comando uniscan



Fuente: elaboración propia

Una vez ingresado el comando anterior, se escoge la opción 1 el cual muestra como es el comando para el análisis de vulnerabilidades. Para esto se pone el primer sitio *web* http://www.itspelileo.edu.ec que pertenece a la Plataforma Educativa Institucional. Se pone el comando uniscan -u http://www.itspelileo.edu.ec -qweds

Figura 10. Comando uniscan para el ataque (Plataforma Educativa Institucional)



Fuente: elaboración propia

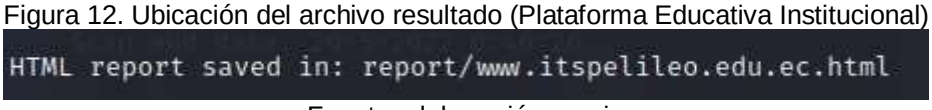
Como se muestra a continuación se realiza el análisis entero del sitio *web* y se observa las inyecciones SQL que se implementan para esto y de igual manera *los test* y spam que se llevan a cabo.

Figura 11. Análisis uniscan Plataforma Educativa Institucional

Fuente: elaboración propia

Una vez acabado el análisis, se entrega un directorio el cual dentro del ordenador de Kali Linux se busca y esto permite observar un archivo html con los resultados del test de seguridad.

Figura 12. Ubicación del archivo resultado (Plataforma Educativa Institucional)

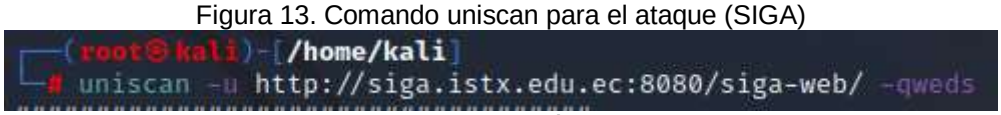


Fuente: elaboración propia

Dentro del anexo 7, resultado 1 se observa que no posee vulnerabilidades en referencia al escaneo realizado con esta herramienta *web*.

Para el siguiente enlace el cual es http://siga.istx.edu.ec:8080/siga-web/ que pertenece a la Plataforma Web SIGA. A continuación, se pone de igual manera el comando uniscan -u http://siga.istx.edu.ec:8080/siga-web/ -qweds, como se muestra en la siguiente imagen.

Figura 13. Comando uniscan para el ataque (SIGA)



Fuente: elaboración propia

Como se muestra a continuación se realiza el análisis entero del sitio *web* y se observa las inyecciones SQL que se implementan para esto y de igual manera los *test* y *spam* que se llevan a cabo.

Figura 2: Análisis uniscan Plataforma Web SIGA

Fuente: elaboración propia

Ya analizado el sitio *web*, el comando entrega un directorio el cual dentro del ordenador de Kali Linux se busca y este permite observar un archivo html con los resultados de la prueba de seguridad.

Figura 14. Ubicación del archivo resultado (Plataforma Web SIGA)

Fuente: elaboración propia

Dentro del anexo 7, resultado 2 se observa de igual manera que es una página que no tiene vulnerabilidades *web*, estudiada y analizada desde la perspectiva de esta herramienta *web*.

Para el ultimo enlace el cual es http://181.211.10.243/aulapelileo/ que pertenece al Aula Virtual Moodle del IST Pelileo. A continuación, se pone de igual manera el comando uniscan -u http://181.211.10.243/aulapelileo/login/ -qweds, como se muestra en la siguiente imagen.

Figura 15. Comando uniscan para el ataque (Moodle)

Fuente: elaboración propia

Como se muestra de igual manera, se realiza el análisis entero del sitio *web* y se observa las inyecciones SQL que se implementan para esto y de igual manera los *test* y spam que se llevan a cabo.

Figura 3: Análisis uniscan Moodle

Fuente: elaboración propia

Ya analizado el sitio *web*, el comando entrega un directorio el cual dentro del ordenador de Kali Linux se busca y este permite observar un archivo html con los resultados de la prueba de seguridad.

Figura 16. Ubicación del archivo resultado (Moodle)

```
HTML report saved in: report/181.211.10.243.html
```

Fuente: elaboración propia

Dentro del Anexo 7, resultado 3 se observa que con la auditoría *web* denominada Crawling, se evidencia que dispone de una versión php 7.1.33 que tiene vulnerabilidades *web* conocidas acorde a CVE-2019-11043. También se aplica que la versión de Apache/2.4.41 urge ser actualizada de acuerdo con las Vulnerabilidades y exposiciones comunes (CVE) (CVE-2019-10092) y (CVE-2019-10081).

SEGUNDA PARTE: Análisis de vulnerabilidades mediante Hacking Ético

Plataforma Web Institucional

A continuación, se realizó el ataque a la Plataforma Web Institucional, mediante fases distintas de hackeo ético.

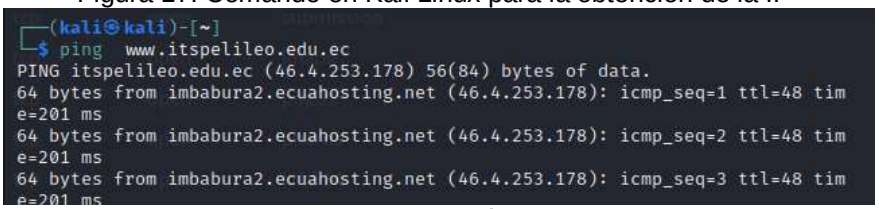
Fase 1: Reconocimiento Pasivo y Activo

Esta fase trata del reconocimiento pasivo o activo que se toma, para el pasivo envuelve la selección de información y datos sin el conocimiento de la empresa o del individuo al que se lo vulnere, mientras que el activo trata de explorar la red más ampliamente para obtener como resultado el descubrimiento de dispositivos individuales en la red, direcciones IP de ordenadores y servicios de red que este sistema posee. Este proceso implica mayor facilidad para localizar que es lo que tiene el reconocimiento pasivo y se le conoce como *rattling the doorknobs.*

Como se menciona el reconocimiento pasivo y de igual manera el activo se lleva al hallazgo de información ventajosa que se utilice para el ataque. Esta información permite a un hacker encontrar vulnerabilidades dentro del sistema y aprovechar estas para obtener más acceso a esta información y datos en sí.

Para la Plataforma Web Institucional se Reconoció a la página como la principal que utilizan los estudiantes y como mediante esta se redirecciona a otras secundarias que sirven dentro de la institución. Esta plataforma Web cuenta con el siguiente enlace https://www.itspelileo.edu.ec el cual se pudo averiguar mediante una máquina virtual instalada y creado la imagen de Kali Linux, donde dentro de la terminal por el comando ping, seguido del enlace se obtiene la IP 46.4.253.178 con la que esta trabaja.

Figura 17. Comando en Kali Linux para la obtención de la IP



Fuente: elaboración propia

Fase 2: Escaneo

Dentro de lo que trata el escaneo es tomar información que se estudió previamente durante el reconocimiento y utilizarlo para vulnerar la red. Una de las herramientas que de uso para vulnerar este sistema es el de LEGION, esta es una herramienta de penetración de red, la cual utiliza otros instrumentos de open-source que ayudan a la obtención automática de puertos de red abiertos que en este caso se especificó en identificarlos.

Una vez realizada la fase 1 que es el reconocimiento y se obtuvo la dirección IP, se procede dentro de la herramienta LEGION a indicar que dirección se va a vulnerar que en este caso es de la Plataforma Web Institucional.

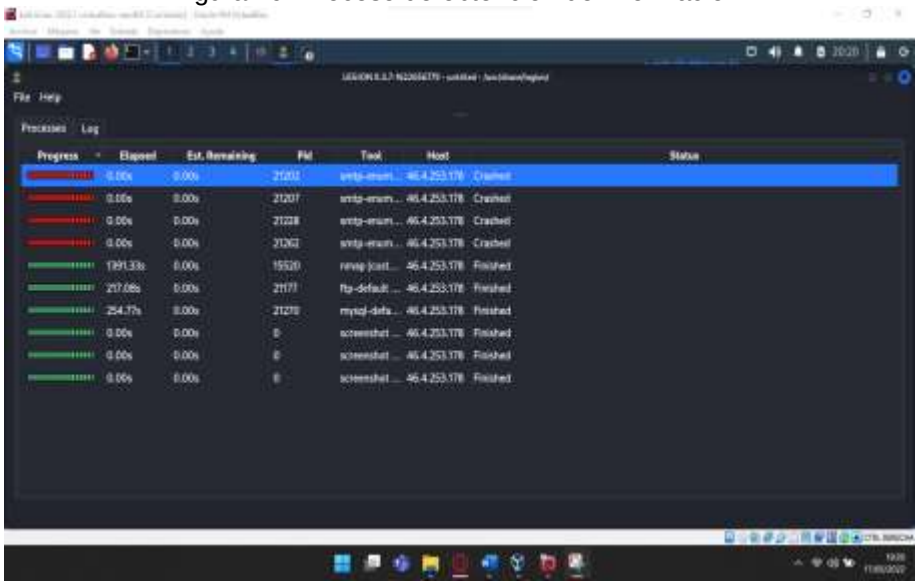
Figura 18. Colocación de IP en LEGION

Fuente: elaboración propia

Se tiene que poner en modo de selección Hard, lo cual ayuda a tener una mejor obtención de puertos que estén abiertos, y en Opción de Tiempo y rendimiento ponerlo en el penúltimo nivel de Agresivo el cual ayuda de igual manera para la obtención más precisa de lo que se requiere.

Una vez ingresada la IP, el programa comienza de manera automática a atacar el sitio *web* y calcula el tiempo que va a durar el ataque hasta que se concluya la operación para mostrar todos los puertos vulnerables.

Figura 19. Proceso de obtención de información



Fuente: elaboración propia

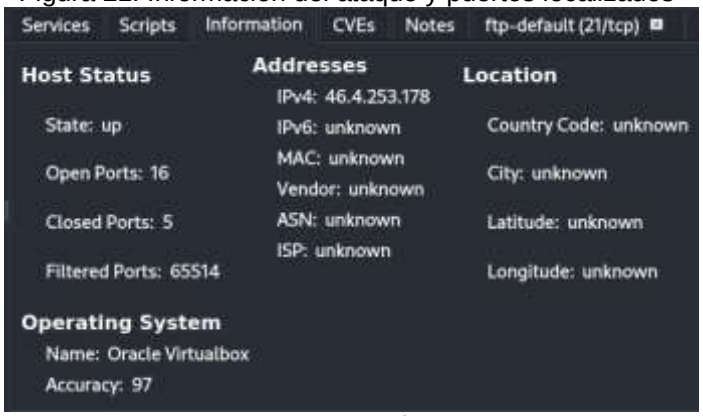
Dentro de la dirección IP 46.4.253.178 que pertenece al enlace de https://www.itspelileo.edu.ec que es la Plataforma Web Institucional. El programa acaba de analizar todos los puertos abiertos los cuales se muestra a continuación el número de puerto el cual está abierto, el protocolo de este, su estado, nombre y versión que este tenga.

Figura 20. Puertos abiertos

Fuente: elaboración propia

En el apartado de información se encontró los 16 puertos abiertos, 5 puestos cerrados y 65514 puertos filtrados, como se muestra a continuación.

Figura 21. Información del ataque y puertos localizados



Fuente: elaboración propia

Fase 3: Obtener Acceso

Una vez obtenidos los puertos abiertos y las vulnerabilidades expuestas que se lograron identificar durante el reconocimiento y la fase de exploración se puede mencionar los siguientes puertos abiertos que son:

Cuadro 10. Descripción de Puertos Abiertos

Puerto	Descripción	Riesgo
Puerto 21:	Este puerto 21 se usa para las conexiones a servidores FTP, permite a los ordenadores el intercambio de archivos en la red de forma masiva.	Al tener estos puertos abiertos se los cataloga como peligro considerable, tiene capacidades de autenticación anónima sin permisos de acceso, de igual manera los recorridos de directorios y scripts entre sitios *web* los cuales son muy convenientes de quebrantar.
Puerto 25:	El puerto 25 se usa por el protocolo SMTP que da permiso a los ordenadores del envío de correos electrónicos.	Con este puerto abierto se infecte los ordenadores con *malwares* que sin consentimiento alguno se envíe correos basura por personales de la organización
Puerto 26:	Este puerto 26 usa el Protocolo TCP el cual es orientado a la conexión y comunicaciones, en donde los datos del usuario se mandan de manera bidireccional y garantiza el orden de entrega de paquetes.	El riesgo que se tiene en este puerto abierto es el de alterar la información u ocupar para fines propios maliciosos de los atacantes, al tener acceso a toda la información que viaja por la red mediante este puerto.
Puerto 53:	El protocolo 53 es utilizado para servicios DNS, este protocolo permite el uso de TCP y UDP que permite la comunicación con servidores DNS.	Si este puerto es vulnerado se utiliza como minería de datos la cual controla el tráfico de datos a través del Sistema de nombres de dominio. Esto sirve para que el atacante libremente los datos robados como tráfico DNS, que redirecciona a un propio servidor DNS falso.
Puerto 80:	Este puerto es utilizado para la navegación *web* HTTP de forma no segura.	Tener este puerto abierto, sirve como puerta de enlace de alojamiento de interfaz *web*, es vulnerable a ataques DoS, envía spam y bloquea el acceso a la plataforma.
Puerto 110:	Este puerto 110 usa gestores para el correo electrónico y establece conexión con el protocolo POP3.	Al tener este puerto abierto es vulnerable a ataques sniffer los cuales interfieren en el tráfico de red.
Puerto 119:	El puerto 119 usa el protocolo TCP/IP, el cual está orientado en la conexión de datos de usuario que se envían bidireccional.	El riesgo sería complejo, la información no se registra de manera correcta y todo lo que se envié no llegue de manera correcta al remitente.
Puerto 143:	El puerto 143 tiene como Protocolo de acceso a mensajes de Internet (IMAP).	Al ser un puerto que recibe solicitudes de clientes, se deniegue el servicio y perjudicar el acceso a la conexión dentro de servidores sin permisos requeridos.
Puerto 443:	Este puerto 443 sirve para la navegación *web*, y utiliza el protocolo HTTPS el cual asegura la navegación dentro de un ordenador y de igual manera utiliza el protocolo TLS por debajo del protocolo anterior.	Afecta prácticamente a la integridad del sistema, si se vulnera este puerto abierto se logra afectar parcialmente la confidencialidad del sistema y su disponibilidad.
Puerto 456:	El puerto 456 usa un protocolo TCP y está orientado en la conexión de forma íntegra.	
Puerto 563:	El puerto 563 utiliza de igual manera el protocolo TCP/IP el cual orienta a la comunicación dentro de la red para garantizar él envió de paquetes de datos de forma ordenada.	Al tener este puerto abierto, se interfiere con la información que se transmite dentro de la red y los datos como se alterarán o roban para fines maliciosos.

Puerto 587:	Este puerto 587 se especifica en el envío de mensajes de email y que estos se transmitan de forma segura y garantizar hasta llegar a su destino.	Si se vulnera este puerto abierto el atacante tendria acceso total a la red en donde se envían específicamente los emails de cada usuario.
Puerto 993:	El puerto 993 utiliza el protocolo IMAP y función SSL que habilita la conexión segura al usar gestores de correo electrónico.	Estos puertos al estar abiertos perjudican a la conexión y envío de correos electrónicos, se interrumpen estos gestores de conexión y no se logra trabajar de manera correcta lo que afecta la legitimidad y disponibilidad de estos servicios.
Puerto 995:	Tiene la misma función que el puerto 993 de gestionar correos electrónicos al establecer una conexión segura junto al protocolo POP3 SSL.	
Puerto 3306:	Este puerto 3306 es utilizado por defecto como protocolo de bases de datos MySQL.	Al vulnerar este puerto abierto se logra fijar en la base de datos de la institución u organización, que pone en riesgo los datos y la gestión de servicios.
Puerto 8008:	Este puerto 8008 tiene un protocolo de TCP para servidores *web* y está orientado a la conexión segura de datos de principio a fin.	La vulneración y riesgos que tiene este puerto al estar abierto es el de conseguir los datos e información en medida que este se transmita al robar o modificar esto.

Fuente: elaboración propia

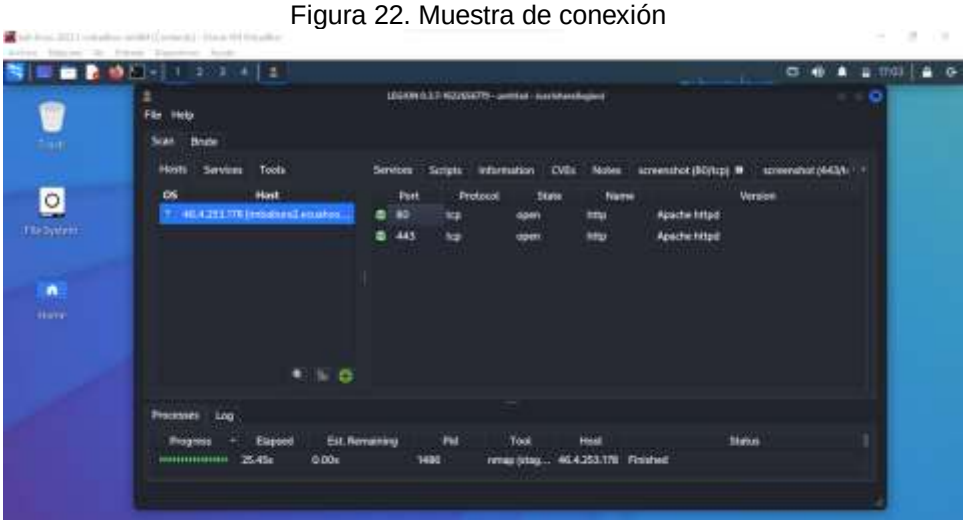
Al analizar todos los puertos abiertos se destaca el puerto 443, al estar este puerto abierto se vulneran o reciben ataques externos como el de DDoS, el cual deniega servicios y un ciber atacante logra llevarlo a cabo y alterar la página para poner en riesgo la disponibilidad de la información, de igual manera se logra llevar ataques de legitimidad en donde se pone en peligro el acceso a la información.

Fase 4: Mantener el Acceso

Una vez realizado el ataque y observado los puertos que se han abierto, uno como hacker ético ha demostrado que logra conseguir y acceder a un sistema o en este caso plataforma *web*. Para esto es muy bueno demostrar que el acceso se mantiene para futuras investigaciones y reconocimientos de vulnerabilidades.

Como se muestra a continuación, se mantiene en conexión con el programa y la dirección IP que se ejecutó para encontrar los puertos abiertos.

Figura 22. Muestra de conexión



Fuente: elaboración propia

Fase 5: Cubrir los pasos

Una vez que se haya realizado el ataque y vulnerado los sistemas requeridos, es muy prudente cubrir los pasos y mediante el ataque de igual manera ocultar evidencias de cómo o donde se realizó estos ataques, para esto la mayoría de los hackers ocultan sus direcciones IP al usar VPN lo cual ayuda al cifrado de datos y

mantener una velocidad alta, esta herramienta VPN ofrece funciones de privacidad y seguridad para las conexiones. Para esta práctica de igual manera se ocupó una máquina virtual la cual ayuda a que no sea directa la conexión con el ordenador si no existe más pasos para localizarlo.

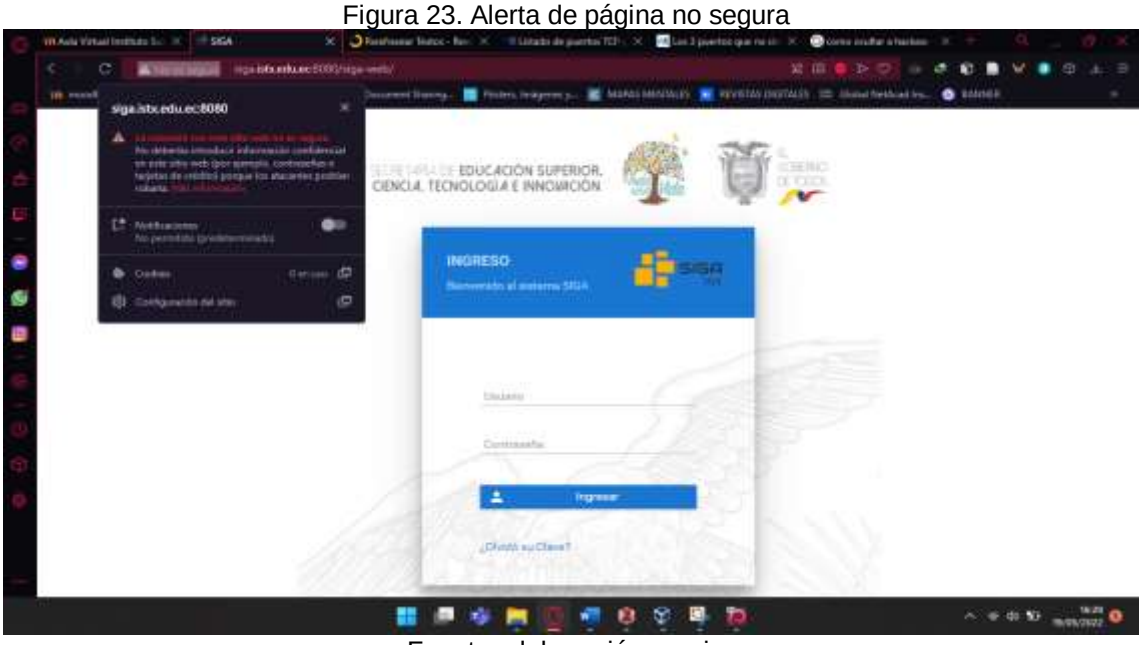
Plataforma Web SIGA

Como segundo punto, se realiza el ataque a la Plataforma Web SIGA, esta plataforma esta de la mano con la secretaria de educación superior del ecuador, para vulnerar y estudiar esta plataforma que usa las mismas fases del hackeo ético anterior.

Fase 1: Reconocimiento Pasivo y Activo

En esta fase se observa ya lo mencionado anteriormente, como se reconoce como primer punto a la página *web* que se atacara y ni bien al momento de entrar en este sitio *web*, se observa en la parte de arriba un mensaje de que no es segura esta página y que un hacker obtenga tu contraseña y datos que se logre ingresar aquí.

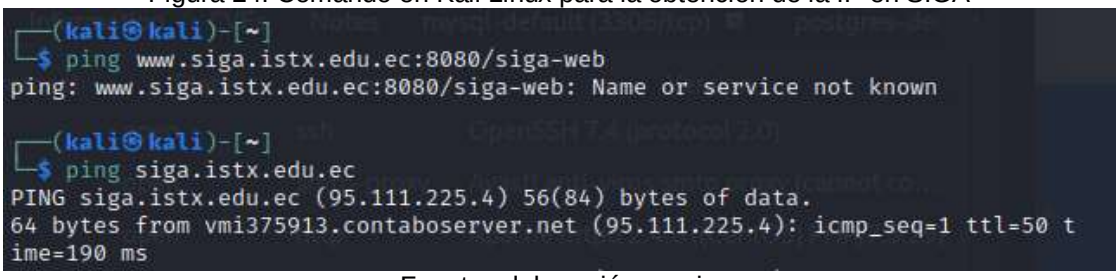
Figura 23. Alerta de página no segura



Fuente: elaboración propia

Para la Plataforma Web SIGA se reconoció a la página como secundaria en la que los usuarios del IST utilizan. Esta plataforma SIGA cuenta con el siguiente enlace http://siga.istx.edu.ec:8080/siga-web/ el cual se pudo averiguar mediante una máquina virtual instalada y creado la imagen de Kali Linux, donde dentro de la terminal por el comando ping, seguido del enlace se obtiene la IP 95.11.255.4 con la que esta trabaja.

Figura 24. Comando en Kali Linux para la obtención de la IP en SIGA



Fuente: elaboración propia

Fase 2: Escaneo

De igual manera se usó la herramienta LEGION, la cual ayuda a la penetración de red, y cuenta con instrumentos de open-source que ayudan a la obtención automática de puertos de red abiertos que en este caso se especificó en identificarlos.

Una vez realizada la fase 1 que es el reconocimiento y se obtuvo la dirección IP de la plataforma *web* SIGA, se procede dentro de la herramienta LEGION a indicar que dirección se va a vulnerar.

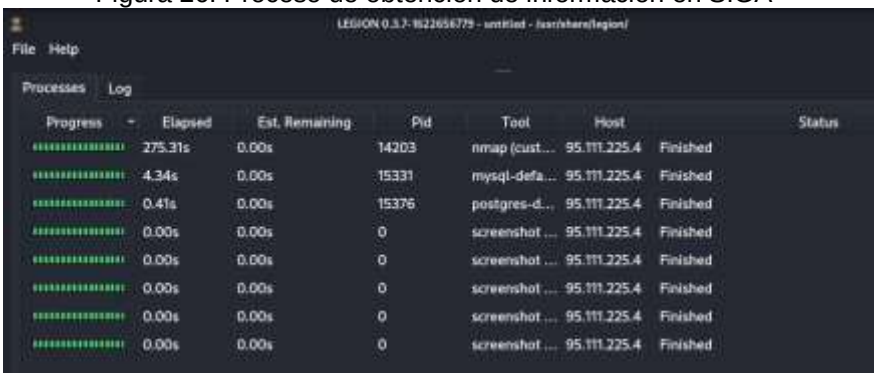
Figura 25. Colocación de IP en LEGION para SIGA

Fuente: elaboración propia

Se tiene que poner de igual manera, en modo de selección *Hard*, lo cual ayuda a tener una mejor obtención de puertos que estén abiertos, y en Opción de Tiempo y rendimiento ponerlo en el penúltimo nivel de Agresivo el cual ayuda de igual manera para la obtención más precisa de lo que se requiere.

Una vez ingresada la IP, el programa comienza de manera automática a atacar el sitio *web* y calcula el tiempo que va a durar el ataque hasta que se concluya la operación para mostrar todos los puertos vulnerables.

Figura 26. Proceso de obtención de información en SIGA



Fuente: elaboración propia

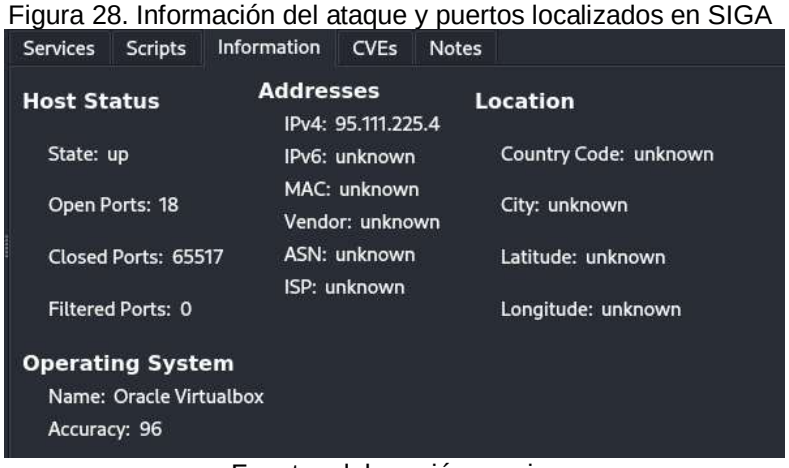
El programa acaba de analizar todos los puertos abiertos los cuales se muestra a continuación el número de puerto el cual está abierto, el protocolo de este, su estado, nombre y versión que este tenga.

Figura 27. Puertos abiertos en SIGA

Fuente: elaboración propia

En el apartado de información se encontró los 18 puertos abiertos, 65517 puestos cerrados y 0 puertos filtrados, como se muestra a continuación.

Figura 28. Información del ataque y puertos localizados en SIGA



Fuente: elaboración propia

Fase 3: Obtener Acceso

Una vez obtenidos los puertos abiertos 25, 80, 110, 119,143,443, 563, 587, 993, 995, 3306 y 8008 ya mencionados en el cuadro anterior y las vulnerabilidades

expuestas que se lograron identificar durante el reconocimiento y la fase de exploración se menciona en los siguientes puertos abiertos que son:

Cuadro 11. Descripción de Puertos Abiertos SIGA

Puerto	Descripción	Riesgo
Puerto 22:	Este puerto 21 se usa para las conexiones a servidores FTP, permite a los ordenadores el intercambio de archivos en la red de forma masiva.	Al tener estos puertos abiertos se los cataloga como peligro considerable, tiene capacidades de autenticación anónima sin permisos de acceso, de igual manera los recorridos de directorios y scripts entre sitios *web* los cuales son muy convenientes de quebrantar.
Puerto 465:	Este puerto 465 contiene un protocolo SMTP el cual opera con capas de seguridad en red, para cifrar las comunicaciones.	Si este protocolo se ve vulnerado mediante el puerto abierto, se logra acceder a la red y lo cifrado con hackeo a fuerza bruta o herramientas de descifrado, encontrar información valiosa y alterarla para beneficios no éticos.
Puerto 5432:	El puerto 5432 garantiza la comunicación y entrega de paquetes en la red, estos están ordenadamente enviados y va de la mano con el protocolo TCP.	El puerto al estar abierto perjudica a la información que se transmite dentro de la red y se perjudica los datos enviados en esta.
Puerto 8080:	El puerto 8080 es un puerto alternativo del 80 TCP que se enfoca en servidores *web*, sirve para la descarga de archivos y es utilizado más para pruebas.	Este puerto al estar abierto da como posible riesgo el de perjudicar archivos de descarga que afecte a los ordenadores.
Puerto 8443:	Al igual que el puerto 8080 una vez implementado se utiliza el puerto 8443 cuando se ha asegurado la conexión en base de SSL.	Si este puerto que ofrece seguridad mediante un puerto ya seguro está vulnerado, no se encuentra con una buena seguridad para la plataforma *web*.
Puerto 10000:	El puerto 10000 usa un protocolo TCP y garantiza la entrega ordenada de paquetes y datos dentro de la red,	Si este puerto se vulnera, se ve riesgos de veracidad de información, en donde no se cumplan las normas de integridad de datos y perjudique a la institución u organización.

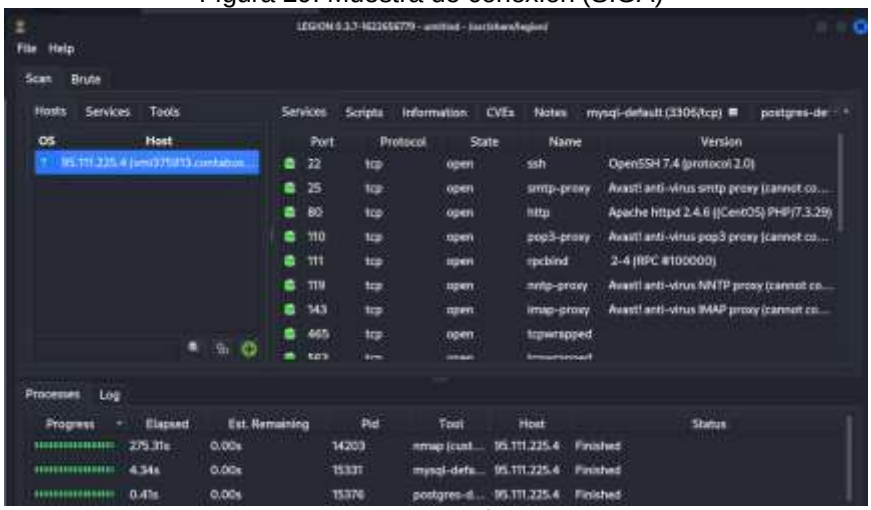
Fuente: elaboración propia

Al analizar todos los puertos abiertos se destaca el puerto 80, al estar este puerto enfocado en los servicios *web*, se vulnera y recibe ataques cibernéticos los cuales saturen un servicio o muchas veces de acceso no autorizado a usuarios externos maliciosos.

Fase 4: Mantener el Acceso

Como se muestra a continuación, se mantiene la conexión con el programa y la dirección IP que se ejecutó para encontrar los puertos abiertos.

Figura 29. Muestra de conexión (SIGA)



Fuente: elaboración propia

Fase 5: Cubrir los pasos

De igual manera se menciona que el ataque se sigue dentro de una máquina virtual la cual de igual manera se usa programas VPN para resguardar la dirección IP y que, aunque cuente con permisos no sea posible el rastreo de estos ataques.

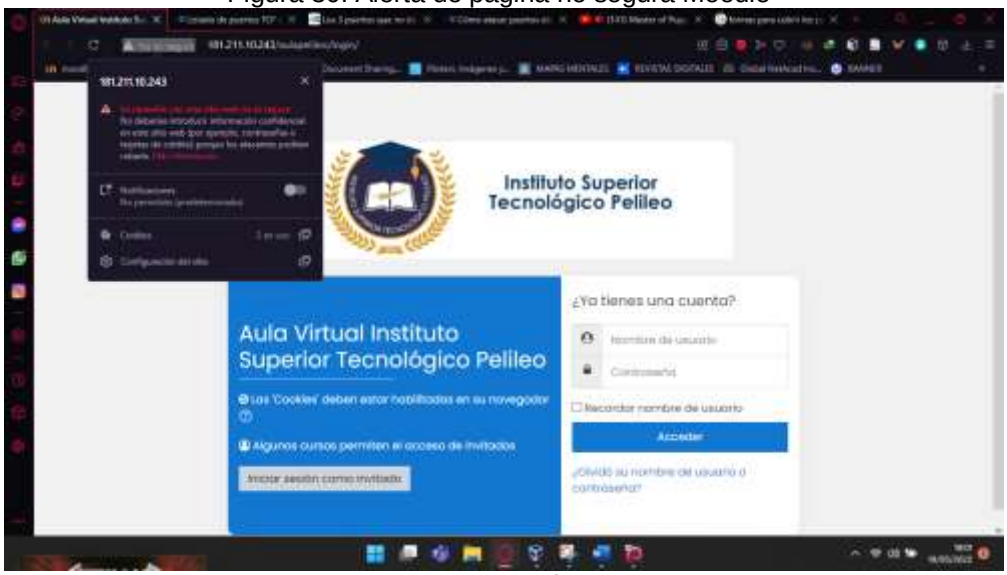
Plataforma Moodle del IST Pelileo

Como último punto, se realiza el ataque a la Plataforma Moodle de la institución, esta plataforma, ocupan tanto los estudiantes como docentes para la interacción con material educativo, para vulnerar y estudiar esta plataforma se usa las mismas fases del hackeo ético ya mencionado.

Fase 1: Reconocimiento Pasivo y Activo

Esta fase se observa ya lo mencionado anteriormente, como se reconoce como primer punto a la página *web* que se atacara y ni bien al momento de entrar en este sitio *web*, se observa en la parte de arriba un mensaje de que no es segura esta página y que un hacker logra obtener tu contraseña y datos que se logre ingresar aquí.

Figura 30. Alerta de página no segura Moodle



Fuente: elaboración propia

Para la Plataforma Web Moodle se reconoció a la página como principal para la subida de deberes y materiales educativos que se presenta a los estudiantes. El URL es http://181.211.10.243/aulapelileo/login/ el cual se accede desde cualquier navegador *web*. En Kali Linux, dentro de la terminal por el comando ping, seguido del enlace se obtiene la IP 181.211.10.243 con la que esta trabaja.

Figura 31. Comando en Kali Linux para la obtención de la IP en Moodle

```
┌──(kali㉿kali)-[~]
└─$ ping 181.211.10.243
PING 181.211.10.243 (181.211.10.243) 56(84) bytes of data.
64 bytes from 181.211.10.243: icmp_seq=1 ttl=54 time=12.6 ms
64 bytes from 181.211.10.243: icmp_seq=2 ttl=54 time=15.8 ms
64 bytes from 181.211.10.243: icmp_seq=3 ttl=54 time=12.9 ms
```

Fuente: elaboración propia

Fase 2: Escaneo

De igual manera se usó la herramienta LEGION, la cual ayuda a la penetración de red, y cuenta con instrumentos de *open-source* que ayudan a la obtención automática de puertos de red abiertos que en este caso se especificó en identificarlos.

Una vez realizada la fase 1 que es el reconocimiento y se obtuvo la dirección IP de la plataforma *web* Moodle, se procede dentro de la herramienta LEGION a indicar que dirección se va a vulnerar.

Figura 32. Colocación de IP en LEGION para Moodle

Fuente: elaboración propia

Se tiene que poner de igual manera, en modo de selección *Hard*, lo cual ayuda a tener una mejor obtención de puertos que estén abiertos, y en Opción de Tiempo y rendimiento ponerlo en el penúltimo nivel de Agresivo el cual ayuda de igual manera para la obtención más precisa de lo que se requiere.

Una vez ingresada la IP, el programa comienza de manera automática a atacar el sitio *web* y calcula el tiempo que va a durar el ataque hasta que se concluya la operación para mostrar todos los puertos vulnerables.

Figura 33. Proceso de obtención de información en Moodle

Fuente: elaboración propia

El programa acaba de realizar un proceso de ver todos los puertos abiertos los cuales se muestra a continuación el número de puerto el cual está abierto, el protocolo de este, su estado, nombre y versión que este tenga.

Figura 34. Puertos abiertos en SIGA

Fuente: elaboración propia

En el apartado de información se encontró los 17 puertos abiertos, 0 puertos cerrados y 65518 puertos filtrados, como se muestra a continuación.

Figura 35. Información del ataque y puertos localizados en Moodle

Fuente: elaboración propia

Fase 3: Obtener Acceso

Una vez obtenidos los puertos abiertos los cuales son el 22, 25, 80, 110, 119, 143, 465, 563, 587, 993, 995 y 8008 ya mencionados en los cuadros anteriores y las

vulnerabilidades expuestas que se lograron identificar durante el reconocimiento y la fase de exploración se menciona los siguientes puertos abiertos que son:

Cuadro 12. Descripción de Puertos Abiertos Moodle

Puerto	Descripción	Riesgo
Puerto 4443:	Este puerto 4443 utiliza un protocolo TCP/IP que ayuda a la conexión de información y determina la comunicación bidireccional.	Si este puerto está abierto y es vulnerado se logra intervenir en los datos y pone en riesgo la información que se presente en la red.
Puerto 4444:	El puerto 4444 usa un protocolo de control de transporte el cual maneja el tráfico de comunicaciones y exfiltra los datos de los ordenadores comprometidos.	Este puerto al estar abierto es sumamente perjudicial, se espía el tráfico en la red y descargarlos para utilidades maliciosas.
Puerto 8081:	El puerto 8081 utiliza el protocolo de transmisión TCP/IP que está orientado a la conexión y envío de datos seguros	Estos dos puertos al estar abiertos se redireccionan información a servidores maliciosos, que toman estos datos para usos ilegales e infiltrarse con información confidencial.
Puerto 8082:	El puerto 8082 se configura de manera predeterminada con el puerto 8081, este puerto retransmite datos por el protocolo UDP y TCP de igual manera.	
Puerto 8443:	El puerto 8443 al ya ver configurado el puerto 8080 se utiliza como respaldo de resguardo de conexiones para obtener un certificado SSL.	Este puerto al estar en un plano de aseguramiento de otro si es vulnerado se pierde dos puertos al mismo tiempo lo que perjudica la información que se transmite dentro de la red.

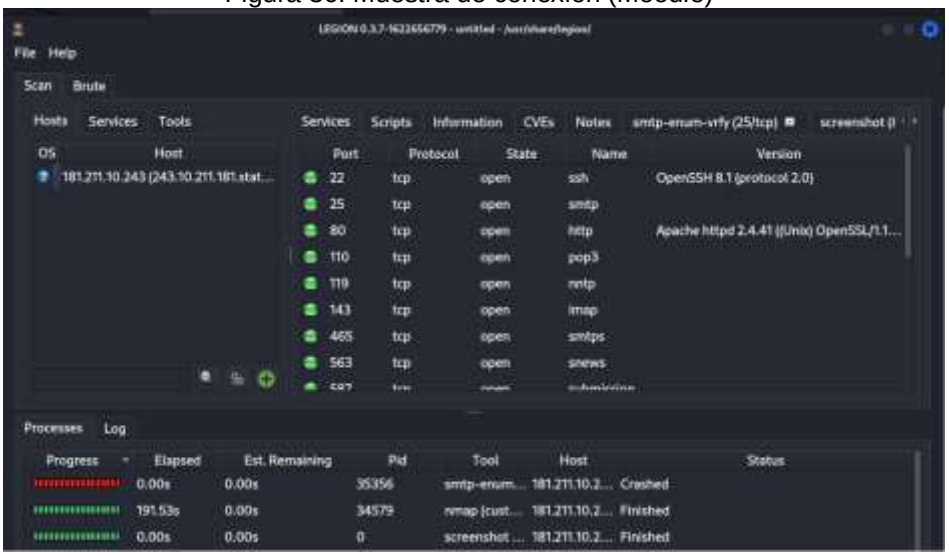
Fuente: elaboración propia

Al analizar todos los puertos abiertos se destacan que la mayoría de los puertos se repiten en los 3 ataques y que en su mayoría los de páginas *web* como el puerto 80, 443, 8081 y entre otros deberán ser los principales en resguardarse y protegerse, para evitar la pérdida de información y la manipulación no autorizada por atacantes maliciosos.

Fase 4: Mantener el Acceso

Como se muestra a continuación, se mantiene en conexión con el programa y la dirección IP que se ejecutó para encontrar los puertos abiertos.

Figura 36. Muestra de conexión (Moodle)



Fuente: elaboración propia

Fase 5: Cubrir los pasos

Como se menciona anteriormente los pasos que se siguieron para cubrir los ataques son dentro de la máquina virtual la cual ayuda en gran cantidad a protegerse de ser rastreado.

TERCERA PARTE: Análisis de vulnerabilidades mediante Herramientas Web

La herramienta SUCURI la cual permite una supervisión y escaneo de sitios *web*, ayuda a protegerse de ataques cibernéticos los cuales distintos sitios tienen, esta herramienta al ingresar el URL de un análisis mediante inyecciones SQL y Spam, de varios riesgos que este sitio *web* posee y ayuda a la limpieza de amenazas en línea que tiene un sitio *web*.

Como primer paso se entra al Sitio Web SECURI, el cual permite poner un URL que es el analizado, para este punto se pone el siguiente https://itspelileo.edu.ec/virtual/ que pertenece a la plataforma institucional del IST Pelileo.

Figura 37. SECURI URL (Plataforma Web Institucional)

Fuente: elaboración propia

Una vez analizado todos los datos, información y vulnerabilidades, a continuación, se resumen los hallazgos:

Figura 38. Información Plataforma Web Institucional

Fuente: elaboración propia

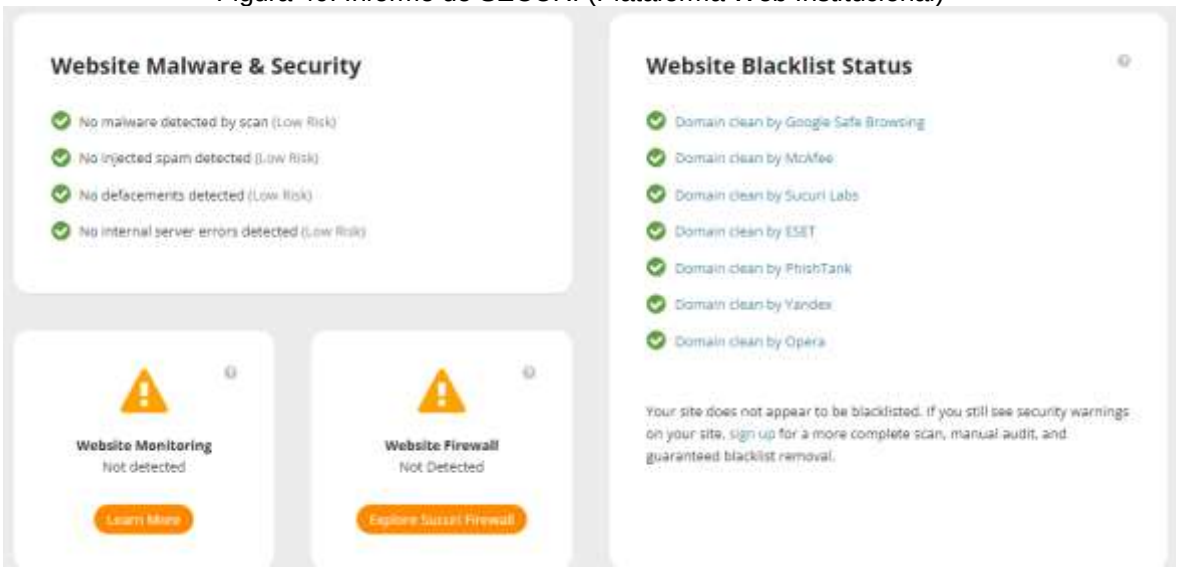
En esta imagen se observa que la clasificación que le ha puesto a este sitio *web* es de Medio Riesgo de Seguridad, donde no se ha encontrado *Malware* y es un sitio que no está en lista negra.

Figura 39. Recomendaciones Plataforma Web Institucional

Fuente: elaboración propia

En este apartado se da una recomendación TLS, la cual informa que al ser un sitio no tan seguro. Se recomienda pasar de http a https, en donde los visitantes al momento de acceder no se muestre la advertencia de navegador no seguro.

Figura 40. Informe de SECURI (Plataforma Web Institucional)



Fuente: elaboración propia

En el apartado de sitio *web* y *malware* detalla de manera más precisa lo hallado a continuación:

- No se ha detectado *malware* en el análisis (Riesgo bajo)
- No se ha detectado spam inyectado (Riesgo bajo)
- No se han detectado desfiguraciones (Riesgo bajo)

- No se han detectado errores internos del servidor (Riesgo bajo)

Se nota de igual manera que no se ha detectado un firewall del sitio *web* y que esté con supervisión.

En la parte de reconocer si es un sitio en lista negra, ofrece la siguiente información:

- Dominio limpio por Google Safe Browsing
- Dominio limpio por McAfee
- Dominio limpio por Sucuri Labs
- Dominio limpio por ESET
- Dominio limpio por PhishTank
- Dominio limpio de Yandex
- Dominio limpio por Opera

Como segundo objetivo se analizó el siguiente enlace http://siga.istx.edu.ec:8080/siga-web/ que pertenece a la plataforma web SIGA del IST Pelileo.

Figura 41. SECURI URL (Plataforma Web SIGA)

Fuente: elaboración propia

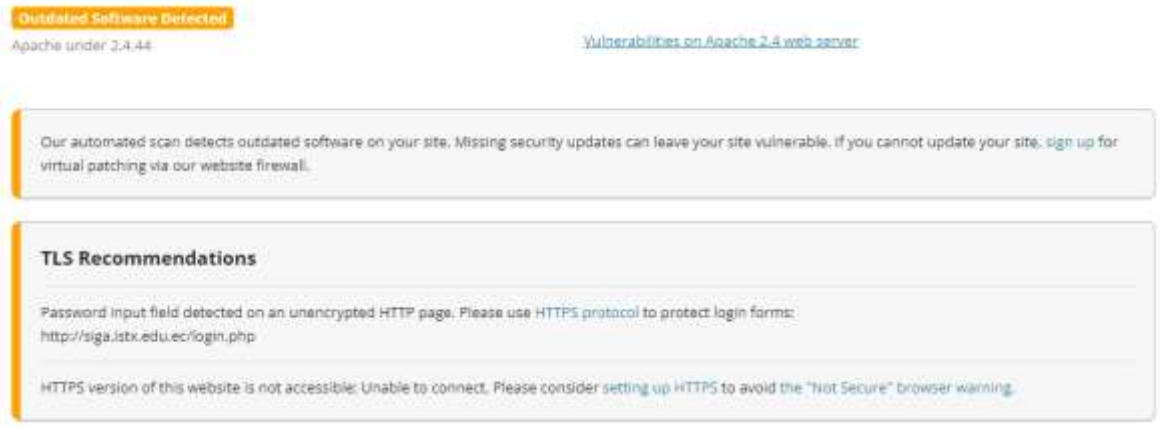
Una vez analizado todos los datos, información y vulnerabilidades, a continuación, se resumen los hallazgos:

Figura 42. Información Plataforma Web SIGA

Fuente: elaboración propia

En esta imagen se observa que la clasificación que le ha puesto a este sitio *web* es de Medio Riesgo de Seguridad, donde no se ha encontrado *Malware* y es un sitio que no está en lista negra de igual manera que el anterior.

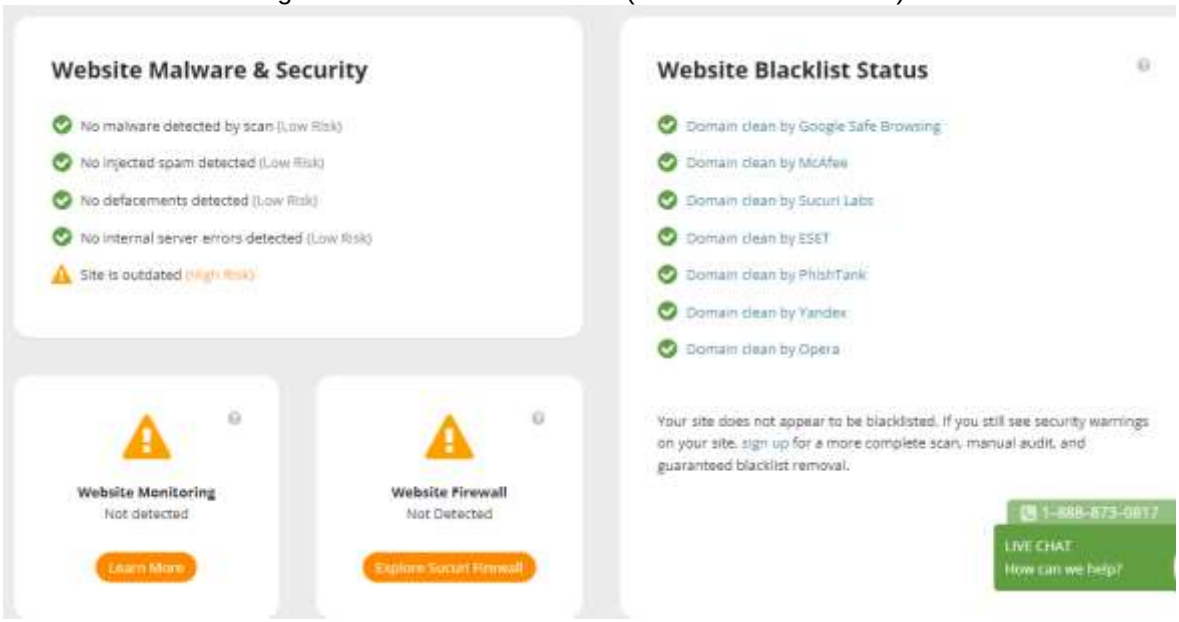
Figura 43. Recomendaciones Plataforma Web SIGA



Fuente: elaboración propia

En este apartado se observa que da una recomendación de un Apache obsoleto, se da una recomendación TLS, la cual informa que se escaneó un *software* desactualizado en su sitio, esta falta de actualizaciones de seguridad deja su sitio vulnerable.

Figura 44. Informe de SECURI (Plataforma Web SIGA)



Fuente: elaboración propia

En el apartado de sitio *web* y *malware* detalla de manera más precisa lo hallado a continuación:

- No se ha detectado *malware* en el análisis (Riesgo bajo)
- No se ha detectado spam inyectado (Riesgo bajo)
- No se han detectado desfiguraciones (Riesgo bajo)
- No se han detectado errores internos del servidor (Riesgo bajo)
- El sitio está obsoleto (Riesgo alto)

De igual manera se muestra que no se ha detectado un firewall del sitio *web* y que este con supervisión.

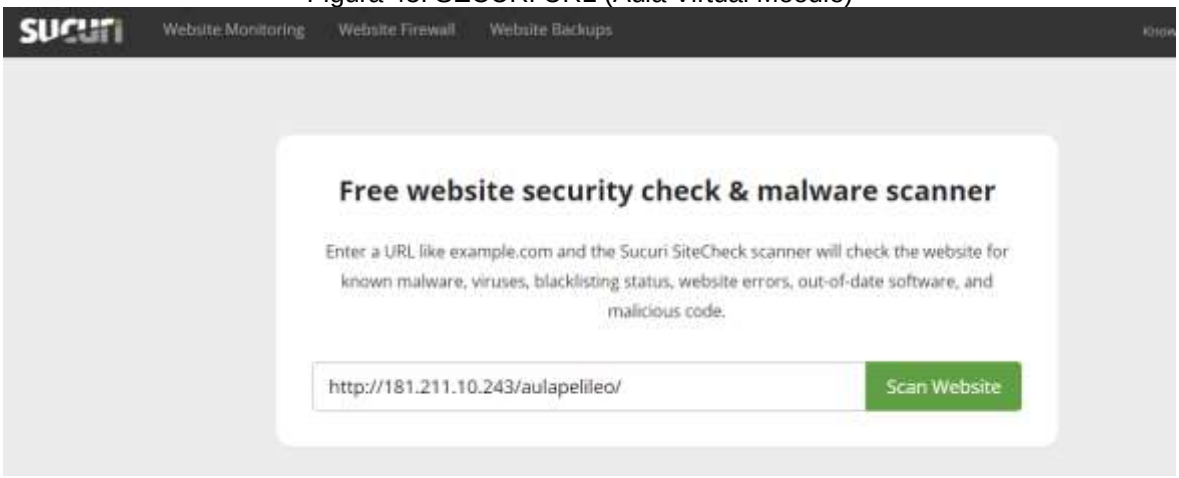
En la parte de reconocer si es un sitio en lista negra, ofrece la siguiente información:

- Dominio limpio por Google Safe Browsing
- Dominio limpio por McAfee
- Dominio limpio por Sucuri Labs
- Dominio limpio por ESET
- Dominio limpio por PhishTank
- Dominio limpio de Yandex

- Dominio limpio por Opera

Como último punto se analizó el siguiente enlace http://181.211.10.243/aulapelileo/ que pertenece al Aula Virtual del IST Pelileo.

Figura 45. SECURI URL (Aula Virtual Moodle)



Fuente: elaboración propia

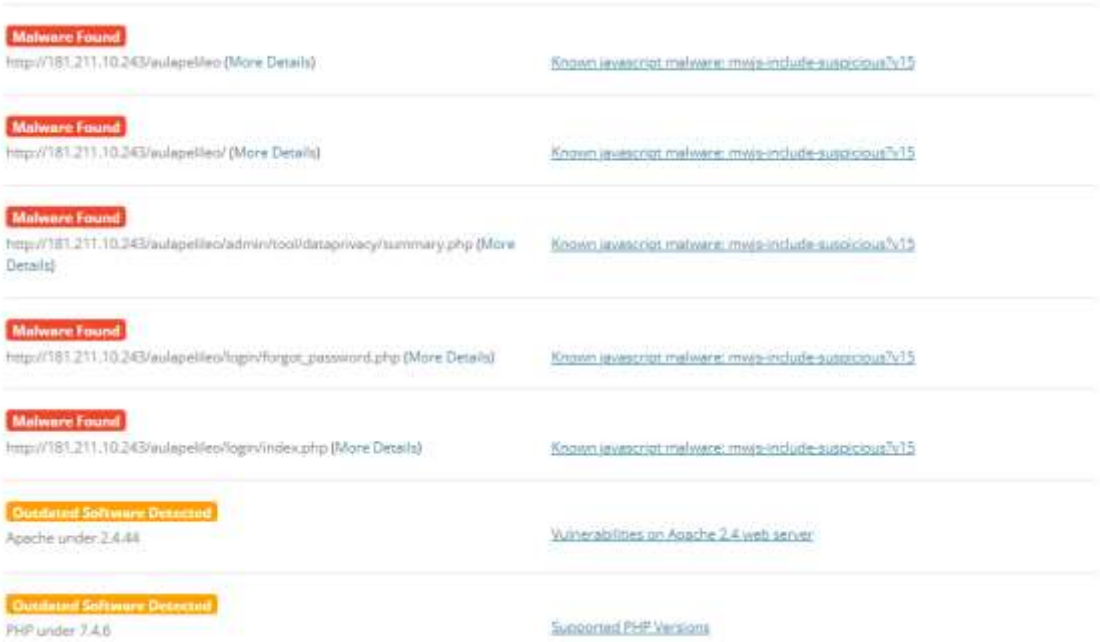
Una vez analizado todos los datos, información y vulnerabilidades, a continuación, se resumen los hallazgos:

Figura 46. Información Aula Virtual Moodle

Fuente: elaboración propia

En esta imagen a diferencia de las anteriores, se observa que la clasificación que le ha puesto a este sitio *web* es de Riesgo de Seguridad Crítico, donde se ha encontrado *Malware*.

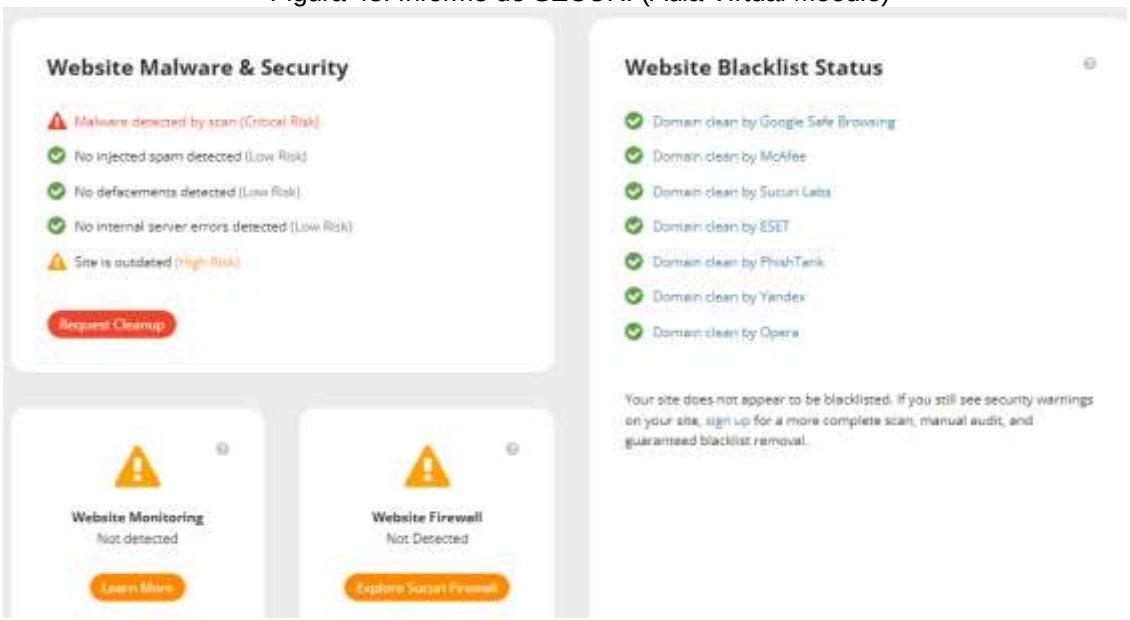
Figura 47. Recomendaciones Aula Virtual Moodle



Fuente: elaboración propia

En este apartado se observa el listado de los *malwares* encontrados los cuales fueron 5, se detalla de igual manera un apartado de más información y la dirección que este tiene, de igual manera se muestra 2 softwares obsoletos los cuales están dentro del sitio *web*.

Figura 48. Informe de SECURI (Aula Virtual Moodle)



Fuente: Elaboración propia

En el apartado de sitio *web y malware* detalla de manera más precisa lo hallado a continuación:

- *Malware* detectado por el escáner (Riesgo crítico)
- No se ha detectado spam inyectado (Riesgo bajo)
- No se han detectado desfiguraciones (Riesgo bajo)
- No se han detectado errores internos del servidor (Riesgo bajo)
- El sitio está obsoleto (Riesgo alto)

Como en los otros dos apartados, se muestra que no se ha detectado un *firewall* del sitio *web* y que este con supervisión.

En la parte de reconocer si es un sitio en lista negra, ofrece la siguiente información:

- Dominio limpio por Google Safe Browsing
- Dominio limpio por McAfee
- Dominio limpio por Sucuri Labs
- Dominio limpio por ESET
- Dominio limpio por PhishTank
- Dominio limpio de Yandex
- Dominio limpio por Opera

RESUMEN DE VULNERABILIDADES ENCONTRADAS

Una vez analizadas de 3 maneras diferentes las vulnerabilidades que existen en los tres activos de información determinados para el estudio se exponen a continuación, un cuadro con las vulnerabilidades importantes con el debido rango de riesgo que este tiene, se da un resultado alto en base a un riesgo cuya vulnerabilidad atente al sitio *web*, medio cuando no afecta tanto y bajo cuando no exista amenaza alguna. De igual manera se pone a consideración las vulnerabilidades y exposiciones comunes (CVE), que trata de un listado realizado por The MITRE Corporation sobre la información y fallas que existen, dándolas una asignación y número de identificación que estas tienen, para permitir a especialistas

en TI tomar iniciativas de mitigarlas y priorizar estas vulnerabilidades, a fin de reforzar la seguridad en los sistemas informáticos.

Debido a temas de confidencialidad y protección de la información dentro del IST Pelileo solo se mencionan las vulnerabilidades encontradas más no, especificados con sus versiones en php o algún otro dato que afectaría al instituto.

Cuadro 13. Resumen de vulnerabilidades

Vulnerabilidad	**Descripción de la Vulnerabilidad**	**Impacto**	**Riesgo**
Php	La versión del php está desactualizado. CVE (2019-11043)	Posibilidad de ejecutar código remoto.	Alto
Php	Está obsoleta la versión de php. CVE-2021-21708 416	Existe la posibilidad de que se active el uso de la memoria asignada después de liberarla, lo que resulta en un fallo, y potencialmente en la sobreescritura de otros trozos de memoria y RCE. Este problema afecta a: el código que utiliza FILTER_VALIDATE_FLOAT con límites mínimo/máximo.	Alto
Puerto 80	El puerto de comunicación que se utiliza no es seguro (HTTP)	El tráfico de red que se ejecuta dentro del sitio *web* logra ser leído, es decir el hacker observa información de forma fácil, no se encuentra encriptada entre el cliente y el servidor.	Alto
Puerto 443	Al ser un puerto que por defecto tiene que estar abierto, da una conexión HTTPS, muchas veces es bueno complementarlo con firewall para sitios *web*.	Al ser vulnerado este puerto es propenso a ataques Spectrum Power, dándole al atacante un acceso al servidor y de igual manera generar ataques de denegación de servicios.	Medio
Firewall	No se detecta ningún cortafuegos de aplicaciones de sitios *web*	Al no contar con una primera capa de seguridad, la aplicación y la red interna se encuentran vulnerables a ataques externos como DDoS.	Alto
Cabecera de Seguridad	Falta de protección de la cabecera de seguridad.	Se da un ataque de clickjaking, el cual se roba información como cuentas y contraseñas.	Media
CSP	Falta de la Política de Seguridad de contenido.	Al no tener esta política se encuentra vulnerable a ataques Cross Site Scriptiing (XSS) y ataques de inyección de datos.	Alto

Fuente: elaboración propia

Fase 5: DEFINIR CONTROLES DE CIBERSEGURIDAD

Según el Anexo A de la ISO 27001 que trata de documento normativo que sirve como guía para implementar controles de seguridad específicos. Todos estos controles están dirigidos a mejorar la Seguridad de la información dentro de una institución u organización en los que se aplique, esta normativa está compuesta por 114 controles y agrupada en 14 secciones las cuales son desde la A5 hasta la A18, en base a esto se detalla los siguientes controles que se deben aplicar dentro del IST Pelileo.

Cuadro 14. Controles de Ciberseguridad

Control	Detalle
A.5.1.1	Políticas de Seguridad de la Información: este control se refiere al proceso de escribir y examinar políticas de seguridad.
A.5.1.2	Las políticas de seguridad de la información deberán ser revisadas en diferentes fases planeadas para asegurar su adecuación y efectividad continua.
A.6.1.1	Se tiene que definir y realizar asignaciones pertinentes a la seguridad de la información.
A.6.1.2	Se deben fragmentar las responsabilidades en conflicto para reducir las posibilidades de alteración de información y los activos organizacionales.
A.6.1.4	Se tiene que mantener contacto con un grupo específico de seguridad de la información.
A.7.1.1	Se tiene que controlar los datos de los trabajadores para permitir el manejo en su debido cargo en base a la información.
A.7.1.2	Se deben fijar términos para el personal y fijar compromisos dentro de la organización referidos a la seguridad de la información,
A.7.2.1	La gerencia o el rango más alto dentro de una institución u organización, esta opta por todo el personal en una guía de buen manejo de la información para resguardarla.
A.7.2.2	Todos los trabajadores y personal de la institución deben recibir una capacitación adecuada sobre el uso de la información, de acuerdo con las funciones que desempeñen y el trabajo que este tenga en la institución.
A.7.2.3	Se opta por un proceso disciplinario con los trabajadores para la protección de la información.
A.8.1.3	Se tiene que controlar los activos y la información que se entrega.
A.8.2.1	Toda información tiene que ser clasificada de acuerdo con su contenido, ya sea crítica o sensible en términos de su divulgación e integridad.
A.9.1.1	Se tiene que documentar, analizar y revisar la política de control de acceso en base a la organización y su seguridad de la información.
A.9.1.2	Los usuarios deben tener acceso únicamente a la red y sus servicios que han sido destinados.
A.9.3.1	Se tiene que adecuar al usuario con buenas prácticas a seguir sobre el uso de la información y su autenticidad.
A.9.4.1	En este control es primordial delimitar el acceso a la información y las funciones de aplicación en base a la política de control de acceso.
A.10.1.1	Se deben desarrollar e implementar políticas para el uso y control criptográficos.
A.12.6	Gestión de las vulnerabilidades técnicas, objetivo evitar la explotación de las vulnerabilidades técnicas
A.13	Seguridad de las comunicaciones, objetivo garantizar la protección de la información en las redes y sus instalaciones de procesamiento de la información.

Fuente: elaboración propia

Se toma en cuanto con los controles dados por la norma ISO 27001, se escogieron los que mejor se adaptan a la institución y como estos ayudarían a mitigar y prevenir posibles riesgos que existan o se dan con el tiempo.

GENERACIÓN DE SALVAGUARDAS

En base al resumen y criticidad de las vulnerabilidades encontradas, se recomienda implementar las siguientes salvaguardas de ciberseguridad como remediaciones de para los sitios *web* del IST Pelileo:

a) Implementar un firewall y una zona desmilitarizada (DMZ)
b) Implementar actualizaciones para las versiones obsoletas de php.
c) Realizar las configuraciones necesarias para la mitigación de las vulnerabilidades conocidas (CVE).
d) Configurar un certificado de seguridad (HTTPS).
e) Aplicar buenas prácticas en la codificación de sitios *web*.
f) Implementar las políticas necesarias de seguridad como CSP.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Los resultados de la investigación realizada mediante la aplicación de la metodología de gestión de riesgos de ciberseguridad se presentan a través de una guía de buenas prácticas enfocadas en el aseguramiento de la plataforma educativa institucional y de los activos de la información identificados que tienen relación con la gestión académica del instituto.

3.1. Guía de buenas prácticas para el aseguramiento de plataforma educativa

La ciberseguridad ocupa hoy en día una posición destacada en las organizaciones e instituciones por ser fundamental su implementación para consolidar una defensa sólida contra ataques y vulnerabilidades informáticas que perjudican a estos establecimientos.

Los ciberataques tienen como objetivo comprometer y perjudicar a los sistemas informáticos, al dañar información y robar datos sustentables. La implementación de una guía de buenas prácticas de ciberseguridad ayuda fuertemente a combatir estos problemas cibernéticos, para mejorar las organizaciones en grados de confidencialidad y protección de activos informáticos, esta responsabilidad tiene que ser asignada a un profesional en el área de TI, el cual se vea comprometido en ayudar y dar solución a cualquier vulnerabilidad de sistema mediante protocolos y normas existentes en la ciberseguridad.

Para la siguiente guía de buenas prácticas, se enfoca en dar un resumen de todo el trabajo en función de los resultados obtenidos de la metodología aplicada y por lo tanto dan sustentaciones puntuales y específicas a la realidad y contexto de la institución. Todos estos insumos están generados en el capítulo 2 y se resumen en la siguiente guía.

1. Implementar la unidad de gestión de ciberseguridad en el IST Pelileo:

Para esta implementación de una unidad de gestión de ciberseguridad, se propone dentro del organigrama del IST Pelileo, esta implementación es requerida dentro de la metodología de gestión de riesgos de ciberseguridad en la fase 1.

El propósito que tiene la UGSC dentro de la organización institucional, se mantiene a que exista un grupo específico para la seguridad de la información y estén capacitados cada integrante de esta unidad en áreas específicas de ciberseguridad.

La propuesta de implementación de la UGCS se tiene que presentar a la unidad de TI de la institución, con la que posteriormente con el rector del IST apruebe esta medida y se lleve a cabo la integración de esta unidad dentro del organigrama institucional.

Esto ayuda ampliamente en la mejora de seguridad de datos e información y los activos críticos que se ven vulnerables ante ataques cibernéticos.

2. Implementación de la Norma de Ciberseguridad en la Institución

La norma de ciberseguridad establecida para el IST Pelileo, ayuda al estudio y colaboración segura para proteger tanto a las personas como sus datos personales dentro de los sistemas informáticos. De esta manera la norma de ciberseguridad mejora el ámbito de ciberseguridad y resuelve ataques ante posibles amenazas que se da dentro de la institución y sus sitios *web*.

Se propone una implementación de esta norma dentro del IST Pelileo, conjunto a la unidad de TI del instituto en que den paso para que el rector ayude con la indicación de esta guía y su implementación la cual ayuda a tener una guía más específica sobre políticas y normas que se deben cumplir para la seguridad de datos e información institucional. Previo a la implementación o de manera continua se recomienda la evaluación a los encargados de impartir esta norma y de igual manera una vez que esta normativa entre en vigencia se tiene que realizar

campañas de concientización a cada docente, estudiante y personal administrativo dentro del instituto para que tengan conocimiento alguno de lo que conlleva la protección de la información y los posibles riesgos que están expuestos al no tener un buen manejo de datos.

3. Gestión de vulnerabilidades

Al analizar mediante varias herramientas propias de un sistema operativo como es Kali Linux y por medio de comandos en terminales y sitios *web* gratuitos que ayudaron a la auditoría de los tres sitios *web* de la institución, se logró encontrar vulnerabilidades puntuales las cuales fueron versiones de php obsoletas o con falta de actualizaciones, ante esto se detalla de igual manera los CVE que especifican la falla en la que se encuentra la vulnerabilidad y cómo es su riesgo en base a datos recopilados para mitigarlos, de igual manera algunos puertos que deben configurarse de manera que el sitio brinde seguridad, la implementación de un firewall para la *web* y políticas de seguridad que permitan a las plataformas educativas que utiliza el sitio mantenerse resguardadas.

4. Implementación de Controles y Medidas de Seguridad

Para la implementación de estos controles y medidas dadas para las vulnerabilidades encontradas en el IST Pelileo, se proponen controles basados en la NORMA INTERNACIONAL ISO/IEC 27001, Anexo 1 que muestra a los objetivos de control en análisis de la seguridad informática.
Para esto se mencionan políticas las cuales en cuanto a las vulnerabilidades y buenas prácticas que debería tener el Instituto con la información y datos que manejan entre estos se menciona:

- Políticas de seguridad de la información en apartados de gestión y gerencias para la seguridad de la información.
- Organización de la seguridad de la información y su organización interna.
- Equipos móviles y trabajo a distancia en donde se tiene que garantizar la seguridad del trabajo a distancia y del uso de los equipos móviles.

- Durante el trabajo garantizar que los trabajadores y contratistas sean conscientes y cumplan responsabilidades de la seguridad informática.
- Gestión de los activos donde se opta por proteger y dar responsabilidades sobre cada uno de estos
- La Clasificación de la Información, donde se opta por garantizar dentro del instituto que exista un nivel adecuado de protección de la información y su importancia clasificada adecuadamente.
- Control de acceso a la información por parte del instituto
- Responsabilidades del usuario que compete resguardar la autenticación de la información.
- Control de acceso a sistemas y aplicaciones para evitar el acceso no autorizado a los sistemas y aplicaciones.
- Implementación de Criptografía para controlar la información y protegerla
- Gestión de las vulnerabilidades técnicas al evitar la explotación de las vulnerabilidades técnicas existentes.
- Seguridad de las comunicaciones enfocado en gestionar redes y la protección de estas con sus debidos procedimientos seguros.

5. Implementación de Salvaguardas

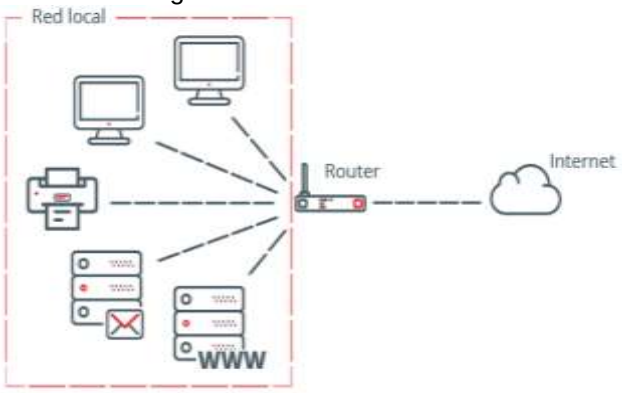
El concepto y definición de una salvaguarda corresponde a los datos que se manejan dentro de una organización o institución, la cual una vez que se haya logrado identificar las vulnerabilidades se procede a crear salvaguardas las cuales ayuden a mitigar estos riesgos existentes dentro del sistema.

En base a esto dentro del IST Pelileo se recomienda resumidamente que se implementen las siguientes salvaguardas:

a) **Implementar un firewall y una zona desmilitarizada (DMZ):** Esto trata prácticamente de un firewall específico en sitios *web* que supervisa el tráfico total de la red y permite identificar y bloquear tráfico no deseado, lo que ayuda así a prevenir ataques a usuarios. La implementación de una zona desmilitarizada (DMZ) la cual ayuda a aislar por grupos una red en donde se

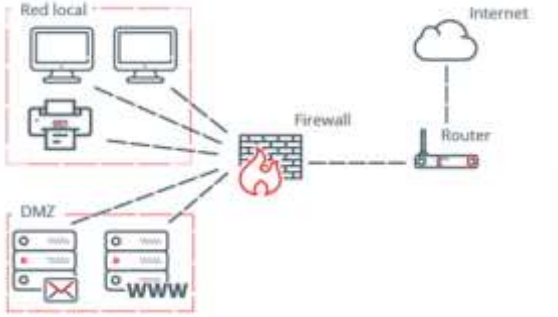
encuentran ubicados los recursos de la institución que estén accesibles al internet.

Figura 4: Zona de red normal



Fuente: Tomado de INCIBE (2019)

Figura 5: Zona desmilitarizada (DMZ)



Fuente: Tomado de INCIBE (2019)

b) Implementar actualizaciones para las versiones obsoletas de php: El tener actualizado las versiones php de la página *web* que se ocupa ayuda a protegerse de vulnerabilidades de seguridad, que muchas veces con el paso del tiempo se vuelven obsoletas y los hackers ven como puertas fáciles para ataques y robo de datos e información de la institución.

c) Realizar las configuraciones necesarias para la mitigación de las vulnerabilidades conocidas (CVE): Como se mostró anteriormente existen fallos dentro de los sitios *web*, los cuales mediante el (CVE) que trata de las Vulnerabilidades y exposiciones comunes, donde trata de una lista de información global que registra toda vulnerabilidad de seguridad que se conocen hasta el momento y cada una lleva su identificación y descripción correspondiente, en esta se presenta posibles soluciones a estos fallos.

d) **Configurar un sitio seguro (HTTPS):** La falta que se tiene en los sitios que son HTTP y no HTTPS es un gran riesgo el cual se tiene que cambiar para que la página intranet o extranet permita a los usuarios que sus datos e información estes autenticados para acceder al internet. Estas áreas deben ser privadas y tener un sitio *web* seguro para evitar robo de contraseñas y datos de cuenta que se ingresen en la página.
e) **Aplicar buenas prácticas en la codificación de sitios web:** Es fundamental que los programadores de la institución tengan buenos conocimientos de sistematización, para lograr así que al programar los sitios *web* dentro del Instituto tengan seguridad apropiada y buenas prácticas de codificación que ayude a generar un código eficiente y seguro de mantenerse.
f) **Implementar las políticas necesarias de seguridad como CSP:** La política CSP se centra en la seguridad de contenido, la cual maneja secuencia de comandos entre sitios *web* que ayude a la prevención de ataques de eyecciones de datos o Site Scripting XSS que se enfocan específicamente en robar información sustentable y desmantelar por completo los sitios o distribuciones de *malware*.

6. Evaluación Permanente y periódica del estado de la ciberseguridad en las plataformas educativas

Una vez definidas todas las implementaciones y mostrado cada caso de vulnerabilidad sus respectivos riesgos y cómo estos se soluciona, es muy importante actualizar el análisis de vulnerabilidades y por ende la implementación de controles y salvaguardas debido a que este es un campo que va en constante cambio como el mundo tecnológico que hoy día se conoce y se ha visto en una evolución continua, por ende se opta por realizar la actualización de estos controles y salvaguardas con el fin de que las plataformas educativas estén protegidas, todo esto se realiza periódicamente previo al inicio del periodo académico, dentro del IST Pelileo, lo cual ayuda a mantenerse seguro de nuevos ataques y vulnerabilidades futuras existentes que si no se estudian y mitigan, llegaron a

afectar a las plataformas educativas y tendrían inconvenientes altos en cuanto al manejo de la información y su disponibilidad, integridad y confidencialidad de esta.

3.2. Validación de la propuesta

Para Galicia Alarcon, Balderrama, & Navarro (2017), el juicio que se tiene por parte de expertos en un tema específico se toma como método de validación útil para verificar la fiabilidad de un trabajo de investigación el cual se define como una opinión, información, evidencia, juicio y valoraciones que el designado experto dé, para esto el individuo no tiene contacto alguno con los demás expertos que validaron el instrumento y darán recomendaciones propias basadas en su investigación y análisis realizado.

Para este apartado se optó por seleccionar a 3 expertos en el área de Seguridad de la Información, estos son Ingenieros informáticos los cuales tienen una maestría ya sea en ciberseguridad como seguridad de la información, la única relación que estos comparten es el trabajo en áreas específicas de seguridad, los tres expertos están involucrados en temas de ciberseguridad desde hace más de 4 años.

Bajo este lineamiento se escogieron a los siguientes expertos:

Cuadro 15. Expertos para Validación

EXPERTOS	TITULO	CARGO
Ing. Mg. Pablo Morales	Magister en Ciberseguridad	Coordinador de carrera de desarrollo de *software* del IST Pelileo
Ing. MSc. Andrés Lagua	Magister en Ciberseguridad	Técnico de Infraestructuras y comunicaciones
Ing. MSc. David Guevara A.	Experto en Seguridad en Redes y Telecomunicaciones	Docente de la maestría de ciberseguridad en la PUCE Sede Ambato

Fuente: elaboración propia

A los cuales se les consideran expertos en el área de ciberseguridad y se les entregó un formulario con 6 preguntas mostrados en un instrumento de validación visible en el Anexo 8 las cuales se basen en el trabajo de la investigación y la guía de buenas prácticas que se realizó para el IST Pelileo de Tungurahua, de igual

manera se muestra en el anexo 9 las respuestas que los expertos dieron a la encuesta.

A continuación, se muestra el análisis de las encuestas realizadas a los 3 expertos designados, que dan como resultado una tabulación de esta información:

Tabla 3. Tabulación y análisis de datos

Indicador	Experto 1	Experto 2	Experto 3	Total	Porcentaje
1. Valore la estructura y pertinencia de la Unidad de Gestión de Ciberseguridad propuesta para el ITS	5	5	5	15	100%
2. Valore el contenido y nivel técnico de la Norma de Ciberseguridad propuesta para el ITS Pelileo	5	5	5	15	100%
3. En cuanto al análisis de vulnerabilidades realizado dentro de la investigación, valore su nivel técnico y resultados.	5	5	4	14	93.3%
4. Evalúe los controles propuestos que deben implementarse en el ITS acorde a las normativas internacionales tomadas como base.	5	5	4	14	93.3%
5. Evalúe las salvaguardas planteadas para contrarrestar las vulnerabilidades detectadas	5	4	4	13	86.6%
6. Valore la pertinencia de la guía de buenas prácticas propuesta.	5	5	5	15	100%

Fuente: elaboración propia

Como se muestra en el cuadro, la validación por parte de los expertos evidencia un porcentaje alto en varios de los criterios analizados, así, en lo que respecta a la Unidad de Gestión de Ciberseguridad, se alcanza un 100% lo que muestra que la propuesta es muy adecuada según la perspectiva de los expertos; en cuanto a la Norma de Ciberseguridad planteada, se valora con el 100% lo que indica de la misma manera que dicha norma es muy adecuada a la realidad del instituto y cubre las necesidades de seguridad para las plataformas educativas; adicional, la propuesta completa que se incorpora en la Guía de buenas prácticas también se valora con un 100% por parte de los expertos lo que indica también la pertinencia de la misma al contexto analizado; frente a estos criterios en lo que respecta al Análisis de las vulnerabilidades, la valoración es del 93,3%, que si bien es esta en el rango de Muy Adecuado, el análisis se amplía al tomar en consideración pruebas

adicionales con otras herramientas; en cuanto a los controles propuestos se tiene una valoración del 93,3% lo que se valora como Muy Adecuado, corresponde con el punto anterior, y evidencia que se encuentra acorde a las normativas tomadas como base; finalmente, en las salvaguardas se obtuvo un 86,6%, lo cual indica una valoración Muy Adecuada, que si se complementa el estudio de vulnerabilidades en una siguiente versión de la Guía, se fortalecería también las salvaguardas propuestas.

CONCLUSIONES

- La fundamentación teórica y metodológica sobre la ciberseguridad y la gestión de seguridad en plataformas educativas y organizaciones son muy escasas, por lo que la metodología seleccionada se determina como importante en el contexto de la investigación.

- La aplicación de una metodología de gestión de riesgos de ciberseguridad en una plataforma educativa, que en este caso se enfoca en el “Procedimiento de Gestión de riesgos de ciberseguridad dentro de los ITS de la Provincia de Tungurahua”, ayuda a identificar vulnerabilidades y riesgos en el área de ciberseguridad, con la cual se maneja y gestiona de mejor manera la información, específicamente en las plataformas educativas, al ser este, un procedimiento de gran magnitud para las organizaciones.

- Proponer una guía de buenas prácticas para el aseguramiento y control de una plataforma educativa, la cual se estructure en función de las características de la institución educativa, de los activos de información críticos, de los resultados del análisis de vulnerabilidades y toma como sustento aspectos claves de distintas normativas internacionales que regulan y establecen criterios para mejorar la ciberseguridad en el instituto.

- La propuesta incluye algunos elementos fundamentales que deben definirse previo a la implementación de la Guía de buenas prácticas, así, la estructuración de una Unidad de Gestión de Ciberseguridad, que está establecida acorde a la estructura organizacional del instituto y se corresponde con el Plan Operativo Anual vigente, por otra parte se definió una Norma de Ciberseguridad que establece políticas, estándares, procesos y actividades enfocados en los usuarios responsables del manejo de la información y que acoge criterios validados por la ISO 27001.

- La evaluación de la utilidad y pertinencia de la guía propuesta mediante el método de validación de expertos es un método importante para verificar la

utilidad y pertinencia de la propuesta, además de que la enriquece con criterios basados en la experiencia y conocimientos de los expertos participantes.

RECOMENDACIONES

- Se recomienda a futuro ampliar el presente estudio, en lo que respecta al análisis de vulnerabilidades y riesgos, para lo que se recomienda tomar como base a OWASP Top 10, el cual define algunos criterios adicionales a los sugeridos por la metodología usada.

- Para enriquecer la presente investigación, sería una alternativa crear un vínculo entre todos los institutos de la zona, para la cooperación y mejoramiento de la seguridad informática en la comunidad educativa.

- Se sugiere a futuro analizar y aplicar una metodología de continuidad del negocio para fortalecer las medidas preventivas y correctivas frente a los problemas de ciberseguridad.

- Es importante que todo el personal del instituto tenga una capacitación sobre la ciberseguridad y la implementación de la Norma de Ciberseguridad junto con la Guía de buenas prácticas propuesta, para que se minimicen los riesgos y se cree una cultura de seguridad en la institución.

- Para complementar la propuesta técnica, se debería establecer un plan de recuperación ante desastres naturales, para resguardar no solo de manera digital la información sino también de manera física.

BIBLIOGRAFÍA

Aguilar Antonio, J. M. (2020).. *RESI*, 15. Obtenido de *La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas.*

Aon. (04 de 03 de 2020). *NOA*. Obtenido de *Nuevo informe de tendencias en ciberseguridad para 2020:* https:// noa. aon. es/ riesgos- y- tendencias- de-ciberseguridad-para-2020/

Avast. (29 de 10 de 2021). *¿Qué es el adware y cómo puede prevenirlo?* Obtenido de AVAST: https://www.avast.com/es-es/c-adware

Barrera Rea, V., & Guapi Mullo, A. (2018). *La importancia del uso de las plataformas virtuales en la educación superior*. Atlante Cuadernos de Educación y Desarrollo.

Bautista Rosell, J. (10 de 2019). Universidad Carlos III Madrid. *Obtenido de Ataques DDoS con IoT, Análisis y Prevención de Riesgos*: https:// e- archivo. uc3m. es/handle/10016/29630

Becerra, J. A., Sánchez Acevedo, M. E., Castañeda, C., Bohórquez, A., Páez Méndez, R. V., Baldomero Contreras, A., & León, I. P. (2019). *La Seguridad en el Ciberespacio Un desafío para Colombia*. Bogotá: ESDEG-SIIA.

Becerro, S. (2009). *Plataformas Educativas, un entorno para profesores y alumnos.* Revista digital para profesionales de la enseñanza, 7.

Beteta Lazarte, J. E., & Narva De la Cruz, M. (2019). *Análisis de la preparación de las organizaciones Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el medio empresarial y que podrían impactar en sus operaciones de negocio.* Publisher: Universidad Peruana de Ciencias Aplicadas (UPC).

Bogantes, A. (2020). *El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados*. iiisci, 6.

Bonifaz, L. (2016). *Plataformas Virtuales Que Utilizan En El Siglo Xxi Las Instituciones De Educación Superior En El Ecuador Durante El Proceso De Enseñanza-Aprendizaje Caso De Estudio*: Moodle, Schoology Y Sidweb. 10.

Carrillo Morales, J. J., Zambrano Avellán, N., Zambrano Lectong, T. J., & Bravo Zambrano, M. (2020). *Proceso de Ciberseguridad: Guía Metodológica para su implementación* - ProQuest. ProQuest, 41-50.

Carrillo, M. V. (2021). *Plataformas Educativas y herramientas digitales para el aprendizaje*. Vida Científica Boletín Científico de la Escuela Preparatoria No. 4, 12.

Castillo, D., & Álvarez, C. (2021). *Estrategia metodológica para la aplicación de plataformas educativas en Educación General Básica*. Revista Arbitrada Interdisciplinaria Koinonía, 597-615.

Chicoma Palacios, D. A. (2019). *Efectividad del sistema integrado de gestión administrativa (SIGA) en la gestión logística de la UGEL San Ignacio 2018*. Repositorio Institucional - UCV.

Chulde Obando, L. E. (2021). *Diseño de un modelo de ciberseguridad basado en la Norma ISO/IEC 27002:2017 para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac*. Repositorio de la Universidad InternaciSEK,SEK , 182.

CISCO. (19 de mayo de 2020). *Cisco*. Obtenido de https:// www. cisco. com/ c/ es_ mx/products/security/what-is-cybersecurity.html

Contreras, J., & Oliveros, D. (2018). *Plataformas E-Learning, sus riesgos y amenazas E-Learning Platforms Their Risks and Threats*. Universidad

Santiago de Cali, Facultad de Ingeniería, Programa de Tecnología en Sistemas de Información , 10.

Cortés, M., & Iglesias León, M. (2005). *Generalidades sobre metodología de la investigación.* Ciudad del Carmen, Camp.: Universidad Autónoma del Carmen.

Díaz, M. B. (2020). *Plataformas Educativas online con seguridad*. Obtenido de https:// www. iescerrodelviento. com/ index. php/ centro/ 76- transformacion-digital- educativa/ 77- seguridad- en- la- red/ 255- plataformas- educativas-online-son-seguridad

EHACK. (27 de 04 de 2022). EHACK. Obtenido de *Las Fases del Hacking Ético* : https://ehack.info/las-fases-del-hacking-etico/

Escobar, A. (2019). *Plataformas Virtuales de Aprendizaje en la Educación Superior. Interconectando Saberes*, 83-100.

Fernández Bermejo, D., & Martínez Atienza, G. (2018). *Ciberseguridad, Ciberespacio y Ciberdelincuencia.* Madrid: Thomson Reuters Aranzadi.

Folgueiras Bertomeu, P. (2016). *La entrevista.* diposit.ub.edu.

Galicia Alarcon, L., Balderrama, J., & Navarro, R. (2017). SCIELO. Obtenido de *Validez de contenido por juicio de expertos: propuesta de una herramienta virtual:* http:// www. scielo. org. mx/ scielo. php? script= sci_ arttext& pid= S1665-61802017000300042

Garay Quisbert, L. M., & Sanchez Seña, A. W. (2021). *Propuesta de mejora de la gestión de seguridad de la información en la empresa mobiliaria PEVISO Ingenieros SAC*. Lima – Perú, 2020. repositorio.epneumann.edu.pe, 14.

García, H., Cen, I., & Us, L. (2016). *Evolución De Una Plataforma Educativa Como Herramienta De Evaluación Y Formación De Ingenieros*. ANFEI Digital.

Group, I. D. (08 de 02 de 2021). *En 2020 crecieron los ataques realizados a usuarios de plataformas educativas | Seguridad*. Obtenido de IT Reseller: https://www.itreseller.es/seguridad/2021/02/en-2020-crecieron-los-ataques-realizados-a-usuarios-de-plataformas-educativas

INCIBE. (19 de 09 de 2019). INCIBE. Obtenido de *Qué es una DMZ y cómo te puede ayudar a proteger tu empresa*: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

ISOTools, E. (21 de 05 de 2015). PMG SSI - ISO 27001. Obtenido de *PMG SSI - ISO 27001*: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Jácome Chávez, V. (2019). *Plan de seguridad para la gestión de riesgos en el datacenter de la Facultad de Ingeniera en Ciencias Aplicadas con la metodología Magerit V3.0.* UNIVERSIDAD TÉCNICA DEL NORTE, 246.

Kaspersky. (13 de 01 de 2021). *¿Qué es el riskware?* Obtenido de latam.kaspersky.com: https:// latam. kaspersky. com/ resource-center/ threats/ riskware

León, M., Ramos, A., Mapp, U., & Reyes, S. (2021*). Evaluación de plataformas de aprendizaje virtual usadas en universidades de Panamá*. IPC , 61.

Leyva Haza, J., & Guerra Véliz, Y. (2020). Objeto de *investigación y campo de acción: componentes del diseño de una investigación científica*. EDUMECENTRO, 241-260.

Luna, C., & Rosa, C. (2009). *Análisis formal del estándar NIST para modelos RBAC*. Colibri Udelar, 17.

Luna, S. (2007). *Manual Práctico Para El Diseño De La Escala Likert*. Vihmai.

Martinez, P., & Roca, D. (2014). *El control del clima de los invernaderos de plástico.* Un enfoque actualizado*.* Bogotá: Universidad Nacional de Colombia.

Martínez-Ardila, H., Becerra-Ardila, L.-E., & Cárdenas-Solano, L.-J. (2016). *Gestión de seguridad de la información*: revisión bibliográfica. Ediciones Profesionales de la Información SL, 931-948.

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). *Formación y concienciación en ciberseguridad bascompetencias: una revisión sistemática de literatura.* Attribution-NonCommercial-NoDerivatives 4.0 International, 36.

Morales Paredes, P. I., & Chicaiza, R. (2021). *Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador.* Dialnet, 49-75.

Naveiro Cabanas, F. X. (2021). *Plan de adecuación al Esquema Nacional de Seguridad (ENS), para una administración pública local*. Universitat Oberta de Catalunya (UOC).

OEA. (2020). *Educación en Ciberseguridad*. Whipe Paper Series, 34.

Olaya Oliveros, A. (2021). *Ataques cibernéticos*. repository.unimilitar.edu.co, 35.

Orizont. (13 de junio de 2017). Obtenido de Orizont VI Edición: https://n9.cl/x09bg

Padilla, G. I., Torres, M., & Padilla, E. J. (2020). *Aprendizaje autónomo y plataformas digitales: el uso de tutoriales de YouTube de jóvenes en Ecuador*. SciELO, 285-297.

Peña, J., & Segura, L. (2014). *La importancia del componente educativo en toda estrategia de Ciberseguridad.* Escuela Superiro de Guerra - Estudios en Seguridad y Defensa, 5-13.

Rivera, F. I., & Ibarra, A. (2019). *Ciberseguridad: algunas consideraciones en operaciones de M&A.* 2019 Práctica Mercantil para abogados: los casos más relevantes en 2018 de los grandes despachos (págs. 557-576). Wolters Kluwer.

Rodríguez Jiménez, A., & Pérez Jacinto, A. (2017). *Métodos científicos de indagación y de construcción del conocimiento*. Revista Escuela de Administración de Negocios, 175-195.

Rodríguez, I. (04 de septiembre de 2020). *¿Qué es la auditoría SOC 2?* Obtenido de ¿Qué es la auditoría SOC 2?: https://www.auditool.org/blog/auditoria-externa/7338-que-es-la-auditoria-soc-2

Rueda, R. (2018). *Uso del ciclo de Deming para asegurar la calidad en el proceso educativo sobre las Matemáticas.* Revista Ciencia UNEMI, 8-19.

Salazar, C. S. (17 de 01 de 2019*). La triada de Seguridad de la Información. Panamá*.

Sanz, E. D. (2021). *La Ley privacidad.* La Ley privacidad, 10.

Serrano, M. (2006). *El uso de una plataforma virtual como recurso didáctico en la asignatura de filosofía*. 363.

Steduto, P., Hsiao, T., Fereres, E., & Raes, D. (2012). *Respuesta del rendimiento de los cultivos al agua.* Roma: FAO.

Suite, G. (3 de septiembre de 2021). *Estándares y normas ISO para mejorar la ciberseguridad*.Obtenido de Global Suite Solutions: http s:// ww w.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/

Torres Arízaga, A. M. (2018). *Propuesta de modelo de gestión de calidad de servicio de Tecnologías de Información en el sector PYME basado en COBIT, COSO, ITIL y las prácticas de la industria*. Universidad del Azuay, 150.

Valencia, G. I. (2014). *Ciberseguridad Para La Educación Online*. Obtenido De Ciberseguridad Para La Educación Online: https:// revista. seguridad. unam. mx/numero22/ciber-seguridad-para-la-educacion-online

Velásquez, R. (2020). *La Educación Virtual en tiempos de Covid-19.* revista-cientifica-internacional.org, 7.

Viñas, M. (2017). *La importancia del uso de plataformas educativas.* SEDECI, 13.

Yuly, P. P. (2017). *Importancia de la ciberseguridad en Colombia.* Universidad Piloto de Colombia, 9.

Zabalo Arteche, E. (2019). *La ciberseguridad como norma. Estudio del estado del arte en estándares y certificación en materia de seguridad cibernética aplicada a industria 4.0 e IoT*. addi, 42.

ANEXOS

Anexo 1. Encuesta a Estudiantes del Instituto Superior Tecnológico Pelileo

Pontificia Universidad Católica del Ecuador | Sede Ambato

Este instrumento de evaluación es parte del trabajo de tesis: “CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL”. Y busca determinar características como el uso y medidas de precauciones sobre la ciberseguridad en sus plataformas educativas. Sus respuestas serán tratadas de forma impersonal.

Gracias por su colaboración, responda a las siguientes preguntas:

N.	INTERROGANTES	Totalmente de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
a) CONFIDENCIALIDAD						
1	¿Cree que su información dentro de su Plataforma Educativa debe permanecer privada?					
2	¿Cree que es riesgoso transmitir datos personales de usuario en entornos no seguros?					
3	¿Piensa que su contraseña debe estar bien estructurada para tener una buena seguridad al acceso de sus cuentas?					
TOTAL		**%** **--**				
b) INTEGRIDAD						
1	¿Cree que si le roban información personal presentara riesgos cibernéticos?					
2	¿Sabe usted que, si su información ha sido cambiada o alterada, es específicamente por ataques o por descuidos personales?					
3	¿Piensa que su información deberá estar siempre protegida en su Plataforma Educativa?					
TOTAL		**%** **--**				
c) DISPONIBILIDAD						

1	¿Al momento de utilizar su Plataforma Educativa ha percibido errores de carga?					
2	¿Conoce que los ataques cibernéticos son los causantes de perjudicar la presentación de la información dentro de una Plataforma Educativa?					
3	¿Piensa que se debe implementar medidas de seguridad para proteger la información dentro de su Plataforma Educativa?					
TOTAL		**%** **--**				

Anexo 2. Encuesta a Docentes del Instituto Superior Tecnológico Pelileo

Pontificia Universidad Católica del Ecuador | Sede Ambato

Este instrumento de evaluación es parte del trabajo de tesis: “CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL”. Y busca determinar características como el uso y medidas de precauciones sobre la ciberseguridad en sus plataformas educativas. Sus respuestas serán tratadas de forma impersonal.

Gracias por su colaboración, responda a las siguientes preguntas:

N.	INTERROGANTES	Totalmente de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
a) CONFIDENCIALIDAD						
1	¿Cree que la información o material que sube en su Plataforma Educativa está completamente seguro?					
2	¿Considera importante implementar seguridad en el material y links que utiliza en actividades educativas?					
3	¿Considera que su contraseña debe estar bien estructurada para tener una buena seguridad al acceso de sus cuentas?					
TOTAL				**% --**		
b) INTEGRIDAD						
1	¿Cree que toda su información dentro de la plataforma Educativa institucional está totalmente correcta y segura?					
2	¿Sabe usted que cuando su información ha sido cambiada o alterada, es específicamente por ataques o por descuidos personales?					

3	¿Considera que su información y material de trabajo deberá estar siempre protegido en la Plataforma Educativa?					
TOTAL		**%** **--**				
c) DISPONIBILIDAD						
1	¿Al momento de utilizar su Plataforma Educativa ha percibido errores de carga o caída del sistema?					
2	¿Cree que los ataques cibernéticos son los causantes de perjudicar la presentación de la información dentro de la Plataforma Educativa?					
3	¿Piensa que se debe implementar medidas de seguridad para proteger la información dentro de su Plataforma Educativa?					
TOTAL		**%** **--**				

Anexo 3.

Modelo de entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

<table>
<tr><td colspan="2"> 
</td></tr>
<tr><td colspan="2">Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional</td></tr>
<tr><td>Objetivo</td><td>Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional para un mejoramiento de esta.</td></tr>
<tr><td>Investigador</td><td>Nombre:
Ingeniero del Instituto Superior Tecnológico Pelileo</td></tr>
<tr><td colspan="2">Consideraciones Generales
1. Se le solicita responder de forma abierta pero objetiva
2. La información aquí recolectada tiene fines investigativos</td></tr>
<tr><td colspan="2">Desarrollo
1. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?
_____
_____
_____
2. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?</td></tr>
</table>

_____

_____

_____

3. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?

_____

_____

_____

4. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?

_____

_____

_____

5. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?

_____

_____

_____

6. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?

_____

_____

_____

7. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

_____

_____

_____

Anexo 4. Encuestas

Encuesta 1

Entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

Pontificia Universidad Católica del Ecuador | Sede Ambato	
Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional	
Objetivo	Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional para un mejoramiento de esta.
Investigador	Freddy Gustavo Morales Tobón Ingeniero en Sistemas, Magister en Tecnologías de la Información del Instituto Superior Tecnológico Pelileo
Consideraciones Generales 3. Se le solicita responder de forma abierta pero objetiva 4. La información aquí recolectada tiene fines investigativos	
Desarrollo 8. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional? Mitigar el riesgo en cuanto a la fuga de información 9. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?	

Los datos personales de los estudiantes, información académica

10. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?

    Muy importante ya que, si esta información es vulnerada , personas externas pudieran hacer mal uso de esta.

11. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?

    Corta fuegos, (Firewall) con el que permita proteger el paso de información a través de credenciales.

12. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?

    Resguardando la integridad de la información tanto personal como institucional.

    Los usuarios se sentirían cómodos, ya que la información no está siendo vulnerada con ataques de acceso indebidos.

13. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?

    Integridad de la información y un control adecuado para así mitigar el acceso indebido de la parte externa.

14. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

    La integridad de la información siempre y cuando esta sea gestionada de una manera segura.

    La información cuando es filtrada causa inconvenientes. Combatiendo a esto con buenas prácticas de gestión de la información.

Encuesta 2

Entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional

Objetivo	Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional para un mejoramiento de esta.
Investigador	Luis Hernán Urquizo Tintín Ingeniero en Sistemas, Especialista en Diseño y Administración Web del Instituto Superior Tecnológico Pelileo

Consideraciones Generales

5. Se le solicita responder de forma abierta pero objetiva
6. La información aquí recolectada tiene fines investigativos

Desarrollo

15. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?
    La seguridad de la información en sí.
16. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?
    Resguardar los datos para que no exista personas externas que vulneren la información dentro de este sistema
17. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?
    La importancia es mucha ya que con estas seguridades podríamos tener bien resguardada la información o los datos de los estudiantes y sus notas que son ingresadas en el sistema.

18. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?

    Tener resguardada todo lo referente a la parte académica de los estudiantes, como sus notas y asignaturas. De mayor consideración de los estudiantes.

19. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?

    Que la información estaría mejor resguardada y ayudaría a la Institución en si a que no sea vulnerada por otras personas externas.

20. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?

    Estos beneficios serian positivos ya que mediante este tipo de tecnología apoya a la no vulneración de información de estos sistemas.

21. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

    Con este sistema el instituto tendría la suficiente seguridad que la información y los datos que se ingresen en el sistema, den seguridad. Logrando así tener datos verídicos sin ningún cambio.

Encuesta 3

Entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

<table>
<tr><th colspan="2">Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional</th></tr>
<tr><td>Objetivo</td><td>Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional para un mejoramiento de esta.</td></tr>
<tr><td>Investigador</td><td>Alex Bladimir Morales Taquiri
Tecnólogo en Informática y Análisis de Sistemas del Instituto Superior Tecnológico Pelileo</td></tr>
<tr><td colspan="2">Consideraciones Generales
7. Se le solicita responder de forma abierta pero objetiva
8. La información aquí recolectada tiene fines investigativos</td></tr>
<tr><td colspan="2">Desarrollo
22. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?
La protección de la documentación que se trabaja dentro de la plataforma e información personal de estudiantes y docentes.
23. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?
Las notas de los estudiantes y la información personal de estudiantes y docentes.
24. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?
Muy importante, porque la información personal una vez obtenida se puede usar para muchas cosas, desde hackeo de cuentas institucionales y personales.
25. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?</td></tr>
</table>

Resguardar todos los datos y tener un Firewall para evitar el hackeo y el ingreso mal intencionado de personas internas o externas de la institución, ya sean estudiantes que deseen cambiar sus notas.

26. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?

    La información estará resguardada y 100% segura y libre de ataques cibernéticos

27. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?

    El resguardo de los datos, tener la información personal segura.

28. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

    Tanto estudiantes como docentes están más tranquilos con la información que se maneja dentro de las plataformas a través de la plataforma que se maneja y evitar su pérdida de información.

Encuesta 4

Entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional	
Objetivo	Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su

	plataforma educativa institucional para un mejoramiento de esta.
Investigador	Diego Sebastián Sánchez Villegas Ingeniero en Sistemas e Informática, Magister en Informática Educativa del Instituto Superior Tecnológico Pelileo

Consideraciones Generales

9. Se le solicita responder de forma abierta pero objetiva
10. La información aquí recolectada tiene fines investigativos

Desarrollo

29. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?

    La seguridad de los datos, respaldo de la información

30. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?

    La información de matrículas, notas, asistencias. Resguardar toda esta información con las debidas seguridades que existen actualmente.

31. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?

    Es muy importante la información que se tiene, ya que básicamente está el historial informativo ya sea de un estudiante como docente. Se debe asegurar esta información para que no sea alterada.

32. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?

    Herramientas en seguridad, utilizar medidas de seguridad, protocolos de seguridad y normas.

33. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?

    La seguridad de la base de datos o la información.

    Que la página sea segura y la información se sienta segura al estar resguardada, hablando en entorno de seguridad web.

34. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?

La información seria respaldada tanto de los docentes como estudiantes ya que se contaría con mejor seguridad.

35. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

    Tener una página web con seguridades, los usuarios estarían resguardados y toda su información de igual manera dentro de las páginas.

Encuesta 5

Entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional

Objetivo	Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional para un mejoramiento de esta.
Investigador	Fernando Patricio Beltrán Fuentes Ingeniero en Sistemas del Instituto Superior Tecnológico Pelileo

Consideraciones Generales

11. Se le solicita responder de forma abierta pero objetiva
12. La información aquí recolectada tiene fines investigativos

Desarrollo

36. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?
    La protección de datos
37. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?
    Realizar Backups
38. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?
    Muy importante, por los datos en sí que se guardan dentro de la plataforma
39. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?
    Firewall, actualización de los equipos.
40. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?
    Evitar los robos de información
41. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?
    Se tendría una persona que se haga responsable en lo que es la seguridad de la información dentro de la Institución
42. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?
    Los usuarios en general se sentirían seguros y protegidos dentro de estos sistemas y plataformas educativos.

Encuesta 6

Modelo de entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional

Objetivo	Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional para un mejoramiento de esta.
Investigador	Pablo Morales P. Ingeniero Magister del Instituto Superior Tecnológico Pelileo

Consideraciones Generales

13. Se le solicita responder de forma abierta pero objetiva
14. La información aquí recolectada tiene fines investigativos

Desarrollo

43. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?

    El beneficio principal de implementar un control de ciberseguridad sería garantizar la disponibilidad, integridad y confidencialidad de la información institucional.

44. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?

La información principal para resguardar sería el historial académico de los estudiantes del Instituto Pelileo además de los registros de las evaluaciones en la plataforma Moodle.

45. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?

    Considero, que muy importante, ya que son datos sensibles y muy importantes que definen el historial académico del estudiante

46. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?

    Para implementar un control de seguridad lo importante sería capacitar al personal docente, administrativo y estudiantes en aspectos básicos de seguridad, lo cuál sería un complemento perfecto para aplicar buenas prácticas de ciberseguridad.

47. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?

    Seguridad en acceso a la información

    Integridad de los datos almacenados en el sistema

    Prevención de posibles ciberataques

48. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?

    Mejor control del personal académico y/o administrativo encargado

    Buenas prácticas de control en materia de ciberseguridad

    Identificación de vulnerabilidades

49. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

    Contribuye en el acceso y control de los sistemas institucionales lo cual brinda seguridad al entorno educativo institucional

Encuesta 7

Modelo de entrevista aplicada al personal de la unidad de TIC en el Instituto Superior Tecnológico Pelileo, con el fin de obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional.

<table>
<tr><td colspan="2">  </td></tr>
<tr><td colspan="2">Modelo de entrevista para obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional</td></tr>
<tr><td>Objetivo</td><td>Obtener información sobre criterios específicos de la implementación de un control de seguridad dentro de su plataforma educativa institucional para un mejoramiento de esta.</td></tr>
<tr><td>Investigador</td><td>Fernando Pico
Ingeniero
del Instituto Superior Tecnológico Pelileo</td></tr>
<tr><td colspan="2">Consideraciones Generales
15. Se le solicita responder de forma abierta pero objetiva
16. La información aquí recolectada tiene fines investigativos</td></tr>
<tr><td colspan="2">Desarrollo
50. ¿Cuáles cree que serían los beneficios de implementar un control de seguridad dentro de la plataforma educativa institucional?
● Alta disponibilidad
● Integridad de la información
● Control de acceso
● Operatividad
● Detección de intrusiones</td></tr>
</table>

51. ¿Qué aspectos considera importantes resguardar dentro de la Plataforma Educativa institucional?
    - Cuentas de usuario
    - Información
    - Backups
52. ¿Qué tan importante considera la protección de datos personales dentro de la Plataforma Educativa?

    Altamente importantes

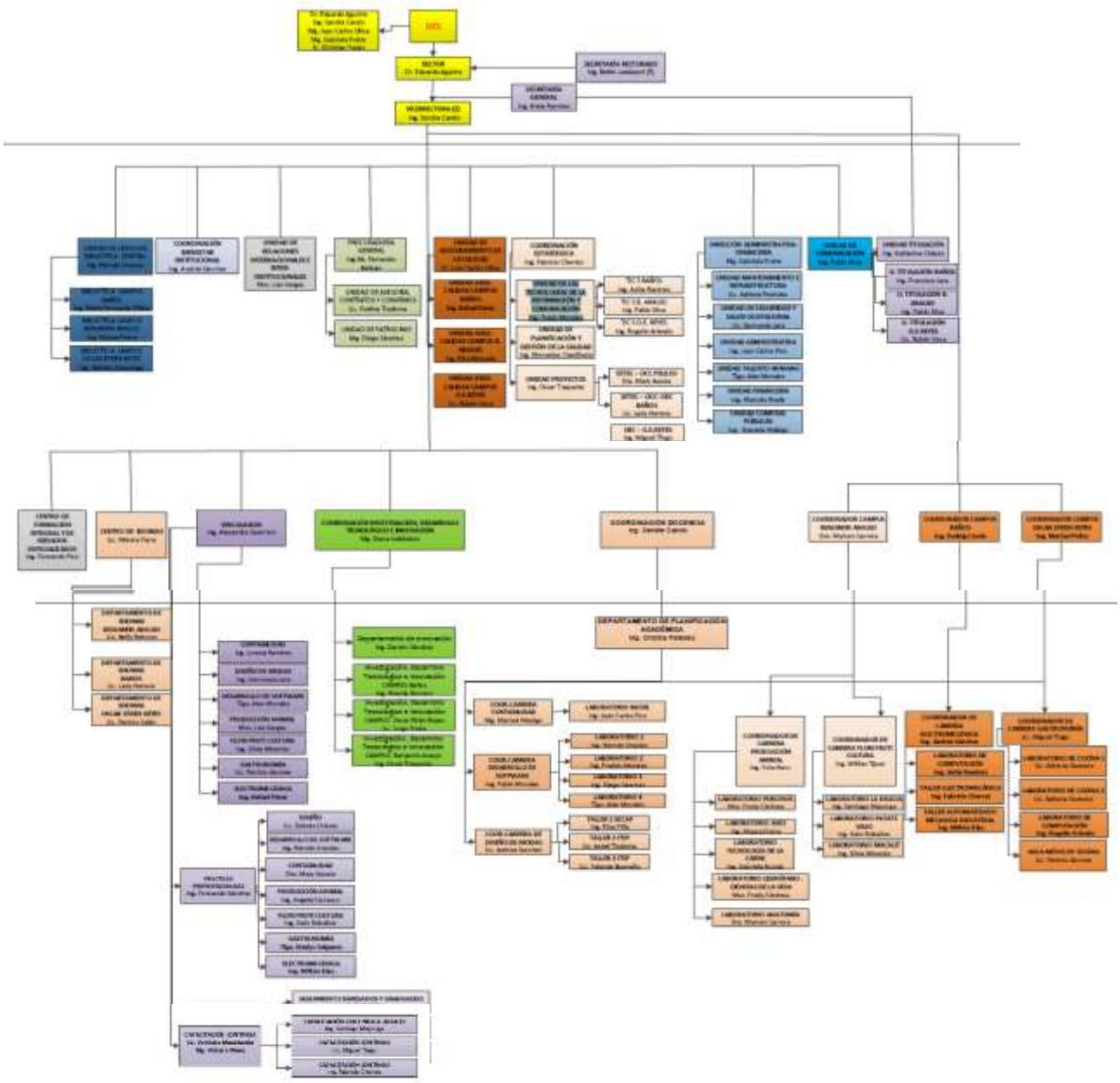
53. ¿Qué aspectos consideraría como primordiales para la implementación de un control de seguridad en la Plataforma Educativa?
    - Robustez
    - Disponibilidad
    - Accesibilidad
    - Flexibilidad
    - Adopción de nuevos eventos
    - Escalabilidad
    - Tolerancia a fallos

54. ¿Cuáles serían las ventajas de la implementación de un control de seguridad en la Plataforma Educativa?
    - Alta disponibilidad
    - Integridad de la información
    - Control de acceso
    - Operatividad
    - Detección de intrusiones
55. ¿Qué beneficios considera tendría la gestión de seguridad en la Plataforma Educativa?
    - Control centralizado
    - Alto nivel de rendimiento operativo

56. ¿De qué manera la implantación de un control de seguridad en la Plataforma Educativa contribuye a mejorar un ambiente educativo más resguardado?

    Genera mayor seguridad en las transacciones de los usuarios y confianza en los reportes que se despliegue.

Anexo 5. Organigrama Estructural Instituto Superior Tecnológico “PELILEO”



Anexo 6. Normativa

Pontificia Universidad Católica del Ecuador | Sede Ambato

NORMA DE CIBERSEGURIDAD

INSTITUTO SUPERIOR TECNOLÓGICO “PELILEO”

ELABORADO POR:

Carlos Alonso Santamaría Calucho

REVISADO POR:

Mg. Teresa Freire Aillón

Mg. Pablo Morales

Propuesta desarrollada en el Marco del Trabajo de Titulación previo a la obtención del Título de Ingeniero en Sistemas

Ambato – Mayo 2022

INDICE

Misión institucional alineada a la política de Ciberseguridad

Formar profesionales competentes y emprendedores en la solución de problemas socio-económicos locales, regionales y nacionales, sustentados en la cultura organizacional, el mejoramiento continuo, asegurando la confidencialidad, integridad y disponibilidad de la información, con una planta docente permanentemente calificada.

1. Antecedentes

Dentro del campo educativo el manejo de datos e información es sumamente importante y es considerada como un instrumento que, junto a otros activos, es valioso proteger para el Instituto Tecnológico Superior Pelileo, por lo que deberá siempre estar resguardado ante posibles ataques, lo que ayude a tener disponibilidad, integridad y confidencialidad de la información dentro del sistema institucional, para contribuir así a la gestión eficaz de la ciberseguridad en el IST.

Los ataques cibernéticos y vulnerabilidades de la información han ido en crecimiento, con lo que existe mayores amenazas que son aprovechadas por ciber atacantes para obtener datos o alterarlos, de igual manera otras amenazas como el espionaje, sabotaje o piratería. El ataque más común es el de (DDoS), este deniega servicios y pone en riesgo la disponibilidad de la información que afecte a usuarios de la institución y sus servicios que otorgue. Por lo anterior, dentro del IST Pelileo se propone una política de gestión de seguridad de la información que es manejada por los integrantes del IST ya sean docentes, estudiantes y personal administrativo.

2. Objetivos

2.1 Objetivo General

Proteger la información y datos del IST Pelileo y la tecnología utilizada dentro del instituto, para ello se planifica una norma la cual ayude a la protección interna y externa de datos, con el fin de garantizar un proceso correcto de confidencialidad, integridad y accesibilidad de información.

2.2 Objetivos Específicos

a) Desarrollar políticas y procedimientos que salvaguarden y conserven los datos del IST Pelileo.
b) Gestionar la prevención de amenazas cibernéticas y reducir los riesgos de seguridad de la información, para garantizar éxito y seguridad en el instituto.
c) Describir planes de ciberseguridad, que cree concientización sobre los peligros del internet y capacitaciones para informar sobre la importancia que tiene los datos Institucionales y como se deberían proteger.

3. Importancia

Esta guía de normas y políticas de Seguridad de la información, tiene como fin principal brindar las información y estrategias apropiadas para dar cumplimiento a los principios de la Triada CID; confidencialidad, integridad y disponibilidad, por medio de políticas y normas de seguridad de la información, en las que se mencionan los compromisos de los usuarios, docentes, estudiantes y personal administrativo del IST Pelileo, al igual que la unidad de TIC, enfocándose en la protección de *software* y hardware que permitan reducir el impacto en ataques cibernéticos o fallos de las plataformas educativas. Por lo tanto, es importante que todas estas implementaciones sean acordes a la protección de datos institucionales.

4. Contexto Normativo

En base a la Norma ISO 27001 y 27032, centradas en la Seguridad de la Información, se implementa en el IST Pelileo, la planificación para estructurar un Sistema de Gestión de Seguridad de la Información señala que es necesario: “Establecer políticas, estándares, procesos y objetivos para gestionar los riesgos de los ataques cibernéticos para lograr resultados consistentes con las políticas y objetivos generales de la organización, para reducir así la mayoría de las fallas que pueden ocurrir”.

5. Seguridad de la Información

El Instituto Tecnológico Superior Pelileo, para asegurar que la información conserve su integridad, disponibilidad y confidencialidad deberá optar por la implementación de buenas prácticas que buscan centralizarse en la protección de los datos al ocupar una plataforma educativa o servicio dentro del sistema de procesamiento de información los cuales permitan una buena operatividad dentro de la institución. Esta se logra mediante el cumplimiento y compromiso de la unidad de TIC designado a la protección de la información y con la participación de todos los usuarios e integrantes del instituto: docentes, estudiantes y personal administrativo, esto permitirá un mejor cumplimiento de las pautas y requisitos de seguridad, así como el desarrollo de estrategias de mejora continua dentro del sistema

institucional, de igual manera una mayor conciencia por parte de los usuarios para la seguridad de datos, se tiene una respuesta rápida a los incidentes de seguridad.

6. Responsabilidades

Todos los Integrantes del IST Pelileo, Docentes, estudiantes, personal administrativo y terceros que tengan acceso a la información o manejen datos del sistema dentro del desarrollo de sus actividades cotidianas, deberán cumplir con las políticas establecidas en el presente manual.

Existirá un personal responsable de la Seguridad Integral de la Información el cual es designado como oficial de seguridad para la protección y control de la información. En concordancia con lo señalado, la implementación de políticas internas y externas relacionadas a la ciberseguridad deberá ser manejado por este personal, adicionalmente se muestra a continuación las responsabilidades de quienes intervienen en este proceso los cuales son:

6.1 Docentes

a) Guiar a los estudiantes a un mejoramiento de uso de datos e información dentro de las plataformas educativas y el sistema institucional.
b) Asegurar contenido seguro en la plataforma educativa
c) Controlar y verificar enlaces a recursos opcionales de clases.
d) Mantener una navegación segura en clase.

6.2 Estudiantes

a) Proteger sus datos personales de terceros.
b) No ingresar datos en páginas que roben información.
c) Cuidar la navegación en el internet y paginas maliciosas
d) Controlar archivos que se suban a la plataforma y no altere ninguna política de seguridad de la información.

6.3 Personal Administrativo

a) Asegurar que las políticas de seguridad de la información se cumplan
b) Analizar posibles vulnerabilidades en el sistema e informar a la unidad de TIC y los encargados de esta gestión de seguridad.
c) Mantener la confidencialidad de datos en general de la institución.
d) Apoyar a la gestión de seguridad de la información para que se cumplan las normas y políticas establecidas.

POLÍTICAS Y NORMAS DE LA SEGURIDAD DE LA INFORMACIÓN

1. Política de control de Acceso a la Información

1.1 Alcance

Controlar el acceso a la información y permitir que solo las personas autorizadas accedan a ella de acuerdo con las regulaciones para mantener la confidencialidad e integridad del sistema institucional.

Proceso Control de Cuentas de Usuarios

a) Los usuarios de la plataforma educativa dentro del sistema informático institucional deberán tener un control previo a la autorización de la unidad de TIC o responsable de la plataforma educativa, el cual evitara crear usuarios genéricos.
b) El acceso lógico de aplicación y el correo electrónico institucional deberá ser manejado por la directiva de servicio de TICS, el cual en el caso de un usuario ya acabar su contrato o tiempo de trabajo, este será suspendido o si en casos diferentes se necesita modificaciones, ser ellos mismo los que gestionen este proceso.
c) Las contraseñas de los sistemas informáticos dentro del IST Pelileo deberán tener al menos 12 caracteres alfanuméricos mixtos, estos incluirán al menos un número y una letra mayúscula y si es opcional, al menos un carácter especial. El usuario y contraseña identificador de cada usuario dentro del instituto es sumamente personal y confidencial lo cual no podrá ser divulgado o intercambiada en ningún caso con otros usuarios, ya sean internos o externos por ningún motivo.
d) Dentro de los sistemas informáticos del IST se mantendrá un sistema de inicio de sesión único (SSO), el cual permite un logueo seguro y el uso de un nombre de usuario y contraseña central.

2. Política de uso de equipos institucionales y dispositivos móviles

2.1 Alcance

Establecer las directrices para el uso de equipos de cómputo y dispositivos móviles.

Respecto al Uso General y Propiedad:

Proceso Control de Permisos en Dispositivos

a) Tanto docentes, estudiantes y el personal administrativo deberá usar equipos de cómputo y dispositivos móviles que proporcione el instituto, salvo que realicen funciones externas o tengan el permiso autorizado de ingreso y uso de sus propios equipos.
b) No se permite acceder a la información privada y aplicaciones de uso personales de docentes o personal administrativo de la institución en sí, a través de computadoras públicas, con el fin de modificar o cambiar información.
c) Se deberá bloquear los permisos de navegación dentro de la institución para una navegación segura.

Autenticación y Acceso:

Proceso Control de Contraseñas

a) El usuario al tener un equipo deberá implementar un método de bloqueo ya sea: contraseña, PIN de seguridad u otras opciones que permita la protección de datos y el acceso a estos ordenadores y dispositivos móviles de forma segura para tener en cuenta que si se vulnera será su responsabilidad.
b) Las contraseñas de acceso al sistema no se deberán almacenar en los sitios web que recurren y mucho menos en aplicaciones de escritorio. Si se requiere ingreso de datos personales, el usuario deberá autenticar esa información de inicio de sesión. De igual manera no se debe mostrar o tener a la vista de terceros las contraseñas.

Proceso Control de Dispositivos Externos

c) En departamentos que manejen la información del IST, no se permite el uso de dispositivos extraíbles ni medios de almacenamiento externos que funcionan a través de puertos USB. Los usuarios administradores que

requieran el uso de estos dispositivos deberán contar con permiso y solicitar que se realice esta petición, con el fin de evitar la depreciación de información y para restringir el borrado de datos.

Acceso a Redes:

Proceso Control de Conexiones

a) Tener mucho cuidado y no confiar en redes WiFi que sean públicas o gratuitas, es mejor utilizar una red de datos móviles personal y no una red inalámbrica no identificada como segura.
b) Dentro de conexiones automáticas deberá estar deshabilitada en los dispositivos móviles y ordenadores para que no dé paso a la conexión de redes no autorizadas.
c) El *software* utilizado en el IST debe respetar los derechos de propiedad intelectual, además, el responsable de informática TIC debe asegurar una navegación segura y óptima para los usuarios.

3. Política de Activos de Información

3.1 Alcance

Definir métodos para los activos de información dentro del IST, que les permita proteger la información contra cualquier divulgación, uso, modificación o destrucción no autorizado.

Proceso Control de Información

a) El encargado de la gestión de Seguridad de la Información, en colaboración con la unidad de TIC, serán los responsables de identificar y clasificar los activos de información pertenecientes al IST, a lo largo de todas las operaciones.
b) Se debe crear y utilizar información limitada por parte de los usuarios dentro de la institución educativa, para evitar pérdidas que puede suponer un riesgo para el IST.
c) Los encargados de gestionar y manejar los activos de información tienen la responsabilidad de tomar las medidas oportunas y controlar los permisos de acceso según la clasificación de la información. Esta información es restringida y deberá basarse en procesos los cuales permitirán que se eliminen datos de acuerdo con los procedimientos aplicables.

4. Política de Firewall y Acceso a Redes

4.1 Alcance

Se debe supervisar las políticas de privacidad y establecer derechos de acceso para el uso de servicios de red y firewall.

Proceso Control de Firewall

a) Se debe realizar las siguientes revisiones por parte del Auditor Informático interno del IST al menos anualmente, de los siguientes aspectos:
   - Programar un conjunto de reglas para el firewall y control de Switchs dentro de la institución.
   - Que como regla concluyente del proxy y del firewall deberá tener la denegación de todo tráfico en la red.
   - Permisos exclusivos a usuarios administrativos, para la conexión remota al firewall y sistemas de control de tráfico de redes.
   - Tener implementada y habilitada el IPS (Sistema de Prevención de Intrusos).

b) En este apartado se puede permitir la implementación de un *software* de soporte y control remoto para uso interno del IST, este *software* será evaluado por la unidad de TIC. Si se necesita realizar un soporte y control previo, los usuarios serán los que autoricen la solicitud, en caso contrario si no hay disponibilidad se notificará vía correo electrónico al encargado de seguridad de la información.

c) En sitios externos de conexión se debe tener un acceso seguro, se implementará servicios como VPN entre otros. En caso de que terceros proveedores que no brindan soporte remoto, se permitirá el uso de aplicaciones o programas aprobadas por la unidad de TIC y la institución en sí.

5. Política de uso y Acceso a Internet

5.1 Alcance

Dentro de lo que es el Internet como herramienta de trabajo y sus facetas de contenido amplio que tiene, es en donde se permite navegar en muchos sitios del mundo. Relevante o no las actividades del instituto y los recursos de navegación deben ser controlados, verificados y monitoreados para tener una buena seguridad tanto para el usuario como el IST.

Proceso Control de Navegación en Internet

a) Se debe restringir y no permitir lo siguiente:

1. El ingreso a sitios que estén relacionados con: sexo explícito, pandillas o vallas publicitarias, habilidades delictivas, drogas, juegos de azar y sitios que promuevan la violencia, entre otras cosas que afecten a los principios y valores del IST.
2. Restringir el acceso y uso de redes sociales o servicios de mensajerías tales como: Facebook, Messenger, WhatsApp, entre otros similares, cuyo objetivo es la interacción de grupos de personas no identificadas, los cuales intercambiar información delicada del IST, que puede poner en riesgo la integridad de datos.
3. La descarga de archivos no permitidos dentro del IST, ya sean como videos, imágenes o programas sin licencia que se descarguen de sitios públicos en Internet debe ser autorizado y vigilado por responsables de cada proceso de seguridad de la información, con esto establecer procedimientos y controles necesarios para monitorear y asegurar el uso adecuado de los recursos.

6. Política de manejo de Hardware y Software

6.1 Alcance

Se debe velar por el correcto funcionamiento de la infraestructura tecnológica de hardware y *software* que posee la institución educativa.

Proceso Control de Hardware y Software

a) No se deberán realizar copias no autorizadas de programas o archivos confidenciales del IST, excepto para copias que realicen permisos de seguridad.
b) La utilización de programas y *software* libre deberán ser licenciados después de un análisis de vulnerabilidades y estándares para la facilitación por parte del sector de seguridad de la información.
c) No se permite el uso inadecuado de los recursos informáticos del IST con fines comerciales o externos que perjudiquen al sistema.
d) Los integrantes y miembros ya sean directivos, personas administrativas o estudiantes que tengan conocimiento del uso indebido de hardware y *software* dentro del IST deben notificar el asunto para realizar debidos procesos de mitigación y control de información.
e) Queda terminantemente prohibida y restringida la modificación o cambios sin permisos posteriores en cuanto a la configuración del hardware y software. En el caso de existir estas anomalías o deficiencias dentro del sistema se debe comunicar a la unidad de TIC, quien procederá a solucionar este problema.
f) La Unidad de TIC será el responsable de realizar inspecciones al sistema para garantizar la seguridad tanto de equipos como el de componentes tecnológicos, esto ayudará a identificar vulnerabilidades dentro del IST las cuales deberán ser mitigadas con procesos específicos a estos.
g) El Área de TI deberá revisar el lugar de trabajo en busca de actualizaciones en los equipos del IST, la instalación y licenciamiento de softwares antivirus especificaciones y observar que cuente con parches de seguridad adecuados.

7. GLOSARIO DE TÉRMINOS Y DEFINICIONES

Con el objeto de definir el alcance de los conceptos clave utilizados en este documento:

Activo de Información: Trata de elementos ya sean de *software* o hardware que tienen una importancia dentro del IST. En ellos esta información y datos que tiene un tipo de valor significativo para el instituto.

Accesos y Permisos: Trata de verificar y validar los permisos necesarios para los usuarios a las áreas restringidas que solo personal administrativo puede ingresar.

Clave o PIN: Trata de una sentencia la cual ayuda a autorizar los procesos de identificación en cuentas de usuario que se cree en el instituto, y de igual manera un pin tiene el mismo propósito de ser un dato único que sirva para validación de datos que requiere tener un usuario.

Confidencialidad: Trata de tener plenamente la garantía de que la información dentro del instituto se mantendrá protegida y privada.

Disponibilidad: Conlleva a que el instituto tenga la garantía total de que la información estará siempre presente y disponible para los usuarios y no presentara fallos en la hora de mostrarla.

Dispositivo móvil: Trata de un dispositivo de tecnología que tiene *software* implementado estos son como celulares, *tablets*, entre otros.

Equipos de Cómputo: Son ordenadores como Laptops o equipos de mesa que tienen sus propios sistemas.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, estos datos constituyen un mensaje que se puede enviar ya sea desde un remitente hasta un destinatario.

Información Crítica: Trata de la importancia que esa información tiene y lo relevante que puede ser para el instituto. Esta deberá ser protegida y resguardada.

Integridad: Trata en mantener la información y datos privados sin que se identifique modificaciones externas o cambios inesperados que puedan perjudicar al usuario.

Seguridad de la Información: Son mecanismos que se optan dentro de la institución para mantener la información protegida.

Sistema de Información: Un conjunto de recursos de información los cuales tratan en manejar toda la gestión de procesos y mantenimientos que ayuden a almacenar difundir y procesar información según determinados procedimientos.

Tecnología de la Información: Trata de un proceso de hardware y *software* que operan de la mano para la transmisión de métodos, creación y almacenamiento de datos informáticos.

Anexo 7. Resultados

Resultado 1

Reporte de vulnerabilidades con Uniscan para el dominio https://www.itspelileo.edu.ec/

SCAN TIME

Scan Started: 19/5/2022 23:25:59

TARGET

Domain https://www.itspelileo.edu.ec/

Server Banner: Apache

Target IP: 46.4.253.178

CRAWLING

Directory check:
CODE: 200 URL: https://www.itspelileo.edu.ec/administrator/
CODE: 200 URL: https://www.itspelileo.edu.ec/bin/

File check:
Skipped because https://www.itspelileo.edu.ec/uniscan208/ did not return the code 404

Check robots.txt:

Check sitemap.xml:

Crawling finished, found: 1 URL's

FCKeditor File Upload:

Timthumb:

File Upload Forms:

Source Code Disclosure:

Web Backdoors:

PHPinfo() Disclosure:

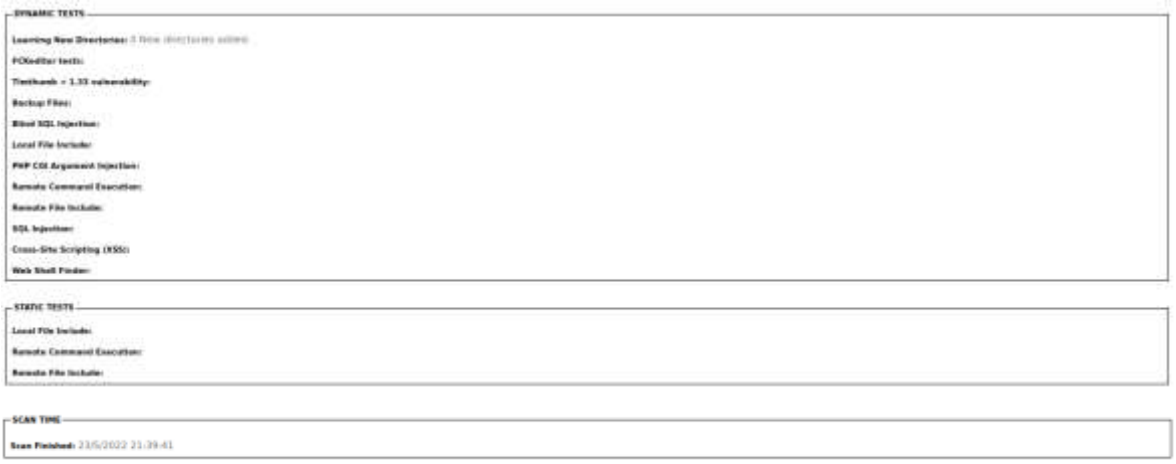
External hosts:

E-mails:

Ignored Files:

Resultado 2

Reporte de vulnerabilidades con Uniscan para el dominio http://siga.istx.edu.ec:8080/siga-web/



Resultado 3

Reporte de vulnerabilidades con Uniscan para el dominio http:// 181.211.10.243/aulapelileo/login

CRAWLING

Directory check:

File check:
CODE: 200 URL: http://181.211.10.243/aulapelileo/login/tests/

File check:
Skipped because http://181.211.10.243/aulapelileo/login/uniscan991/ did not return the code 404

Check robots.txt:

Check sitemap.xml:

Crawling finished, found: 87 URL's

FCKeditor File Upload:

Timthumb:

File Upload Forms:

Source Code Disclosure:
Source Code Found: http://181.211.10.243/dashboard/docs/auto-start-xampp.html

Web Backdoors:

PHPinfo() Disclosure:
phpinfo() page: http://181.211.10.243/dashboard/phpinfo.php
System: Linux localhost.localdomain 3.10.0-1127.10.1.el7.x86_64 #1 SMP Wed Jun 3 14:28:03 UTC 2020 x86_64
PHP version: 7.1.33
Apache Version: Apache/2.4.41 (Unix) OpenSSL/1.1.1d PHP/7.1.33 mod_perl/2.0.8-dev Perl/v5.16.3
Server Administrator: you@example.com
User/Group: daemon(2)/2
Server Root: /opt/lampp
DOCUMENT_ROOT: /opt/lampp/htdocs

http://php.net
http://xdebug.org
https://community.apachefriends.org
http://eaccelerator.net
http://framework.zend.com
http://bitnami.com
https://twitter.com
https://translate.apachefriends.org
https://bitnami.com
https://www.facebook.com
http://git-scm.com
http://www.slimframework.com
https://make.wordpress.org
http://kcachegrind.sourceforge.net
http://sqlite.org
https://support.google.com
http://www.proftpd.org

E-mails:
E-mail Found: your-gmail-username@gmail.com
E-mail Found: social-icons@2x.png
E-mail Found: mike@hyperreal.org
E-mail Found: humbedooh@apache.org
E-mail Found: fastly-logo@2x.png
E-mail Found: you@example.com
E-mail Found: license@php.net
E-mail Found: your@email-address.com
E-mail Found: stack-icons@2x.png
E-mail Found: kevinh@kevcom.com
E-mail Found: social-icons-large@2x.png
E-mail Found: sourceforge-logo@2x.png
E-mail Found: recipients@example.com
E-mail Found: recipients@email-address.com
E-mail Found: xampp-cloud@2x.png

Ignored Files:

DYNAMIC TESTS

Learning New Directories: 1 New directories added.

FCKeditor tests:

Timthumb < 1.33 vulnerability:

Check robots.txt:

Check sitemap.xml:

Backup Files:

Crawling finished, found: 12 URL's

FCKeditor File Upload:

Timthumb:

File Upload Forms:

Source Code Disclosure:

Web Backdoors:

PHPinfo() Disclosure:

External hosts:
https://community.jboss.org
http://wild□y.org
https://issues.jboss.org

E-mails:

Ignored Files:

DYNAMIC TESTS

Learning New Directories: 1 New directories added.

FCKeditor tests:

Timthumb < 1.33 vulnerability:

Backup Files:

Blind SQL Injection:

Blind SQL Injection:

Local File Include:

PHP CGI Argument Injection:

Local File Include:

Remote Command Execution:

Remote File Include:

SQL Injection:

Cross-Site Scripting (XSS):

Web Shell Finder:

PHP CGI Argument Injection:

Remote Command Execution:

Remote File Include:

SQL Injection:

Cross-Site Scripting (XSS):

Web Shell Finder:

STATIC TESTS

Local File Include:

STATIC TESTS

Local File Include:

Remote Command Execution:

Remote File Include:

Remote Command Execution:

Remote File Include:

SCAN TIME

Scan Finished: 20/5/2022 0:40:37

Anexo 8. Encuesta a Expertos en el área de Ciberseguridad y Seguridad de la Información

Este instrumento de evaluación es parte del trabajo de tesis: “ CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL”. Y busca determinar la validación del trabajo en base a opiniones de expertos y sus conocimientos que tiene sobre este tema, ayudando a tener una valoración sobre lo realizado. Sus respuestas serán tratadas de forma impersonal.

PROPUESTA A VALIDAR	Guía de Buenas prácticas de Ciberseguridad para el aseguramiento de una plataforma educativa
Objetivo de la validación	Determinar si la propuesta planteada cumple criterios técnicos y es aplicable a la realidad de la institución objeto de estudio
Experto	
Función de los Expertos	● Revisar y Analizar la propuesta ● Llenar el cuestionario de validación
Instrumento de validación	Cuestionario de 6 preguntas
Escala de validación	5 Muy Adecuada 4 Adecuada 3 Poco Adecuada 2 Inadecuada 1 Muy inadecuada

Gracias por su colaboración, responda a las siguientes preguntas:

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de encuesta para obtener información sobre criterios específicos de expertos en base al trabajo de Tesis

Indicador	**5 Muy Adecuada**	**4 Adecuada**	**3 Poco Adecuada**	**2 Inadecuada**	**1 Muy inadecuada**	**Total**
1. Valore la estructura y pertinencia de la Unidad de Gestión de Ciberseguridad propuesta para el ITS						
2. Valore el contenido y nivel técnico de la Norma de Ciberseguridad propuesta para el ITS Pelileo						
3. En cuanto al análisis de vulnerabilidades realizado dentro de la investigación, valore su nivel técnico y resultados.						
4. Evalúe los controles propuestos que deben implementarse en el ITS acorde a las normativas internacionales tomadas como base.						
5. Evalúe las salvaguardas planteadas para contrarrestar las vulnerabilidades detectadas						
6. Valore la pertinencia de la guía de buenas prácticas propuesta.						

Qué elementos técnicos sugeriría implementar a futuro para complementar la propuesta

Anexo 9. Resultados de las encuestas de validación

Encuesta 1. Expertos en el área de Ciberseguridad y Seguridad de la Información

Este instrumento de evaluación es parte del trabajo de tesis: " CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL". Y busca determinar la validación del trabajo en base a opiniones de expertos y sus conocimientos que tiene sobre este tema, ayudando a tener una valoración sobre lo realizado. Sus respuestas serán tratadas de forma impersonal.

Pontificia Universidad Católica del Ecuador | Sede Ambato	
PROPUESTA A VALIDAR	Guía de Buenas prácticas de Ciberseguridad para el aseguramiento de una plataforma educativa
Objetivo de la validación	Determinar si la propuesta planteada cumple criterios técnicos y es aplicable a la realidad de la institución objeto de estudio
Experto	Pablo Israel Morales Paredes – Ingeniero de Sistemas y Computación - Magister en Ciberseguridad
Función de los Expertos	● Revisar y Analizar la propuesta ● Llenar el cuestionario de validación
Instrumento de validación	Cuestionario de 6 preguntas
Escala de validación	5 Muy Adecuada 4 Adecuada 3 Poco Adecuada

	2 Inadecuada 1 Muy inadecuada

Gracias por su colaboración, responda a las siguientes preguntas:

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de encuesta para obtener información sobre criterios específicos de expertos en base al trabajo de Tesis

Indicador	**5 Muy Adecuada**	**4 Adecuada**	**3 Poco Adecuada**	**2 Inadecuada**	**1 Muy inadecuada**	**Total**
7. Valore la estructura y pertinencia de la Unidad de Gestión de Ciberseguridad propuesta para el ITS	X					
8. Valore el contenido y nivel técnico de la Norma de Ciberseguridad propuesta para el ITS Pelileo	X					
9. En cuanto al análisis de vulnerabilidades realizado dentro de la investigación, valore su nivel técnico y resultados.	X					
10. Evalúe los controles propuestos que deben implementarse en el ITS acorde a las normativas internacionales tomadas como base.	X					
11. Evalúe las salvaguardas planteadas para contrarrestar las vulnerabilidades detectadas	X					

12. Valore la pertinencia de la guía de buenas prácticas propuesta.	x					

Qué elementos técnicos sugeriría implementar a futuro para complementar la propuesta

Potenciar los controles de Ciberseguridad en el Instituto mediante la capacitación constante del personal a cargo para hacer frente a los ataques que pueden venir en el fututo (Security Awareness).

Crear un vínculo entre todos los institutos para la cooperación y mejoramiento de la seguridad informática en la comunidad educativa.

Establecer un plan de recuperación ante desastres naturales, para resguardar no solo de manera digital la información sino también de manera física.

Encuesta 2. Expertos en el área de Ciberseguridad y Seguridad de la Información

Pontificia Universidad Católica del Ecuador | Sede Ambato

Este instrumento de evaluación es parte del trabajo de tesis: " CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL". Y busca determinar la
validación del trabajo en base a opiniones de expertos y sus conocimientos que tiene sobre este tema, ayudando a tener una valoración sobre lo realizado. Sus respuestas serán tratadas de forma impersonal.

Pontificia Universidad Católica del Ecuador | Sede Ambato

PROPUESTA A VALIDAR	Guía de Buenas prácticas de Ciberseguridad para el aseguramiento de

	una plataforma educativa
Objetivo de la validación	Determinar si la propuesta planteada cumple criterios técnicos y es aplicable a la realidad de la institución objeto de estudio
Experto	Ing. Andrés Sebastián Lagua Gavilanes MSc.
Función de los Expertos	● Revisar y Analizar la propuesta ● Llenar el cuestionario de validación
Instrumento de validación	Cuestionario de 6 preguntas
Escala de validación	5 Muy Adecuada 4 Adecuada 3 Poco Adecuada 2 Inadecuada 1 Muy inadecuada

Gracias por su colaboración, responda a las siguientes preguntas:

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de encuesta para obtener información sobre criterios específicos de expertos
en base al trabajo de Tesis

Indicador	**5 Muy Adecuada**	**4 Adecuada**	**3 Poco Adecuada**	**2 Inadecuada**	**1 Muy inadecuada**	**Total**
1. Valore la estructura y pertinencia de la Unidad de Gestión de Ciberseguridad propuesta para el ITS	X					

2. Valore el contenido y nivel técnico de la Norma de Ciberseguridad propuesta para el ITS Pelileo	X					
3. En cuanto al análisis de vulnerabilidades realizado dentro de la investigación, valore su nivel técnico y resultados.	X					
4. Evalúe los controles propuestos que deben implementarse en el ITS acorde a las normativas internacionales tomadas como base.	X					
5. Evalúe las salvaguardas planteadas para contrarrestar las vulnerabilidades detectadas		X				
6. Valore la pertinencia de la guía de buenas prácticas propuestas.	X					

Qué elementos técnicos sugeriría implementar a futuro para complementar la propuesta

Se recomienda la implementación de un Sistema de Gestión de Seguridad de la Información, en la cual se establezca responsabilidades a todo el personal del Instituto.

Encuesta 3. Expertos en el área de Ciberseguridad y Seguridad de la Información

Este instrumento de evaluación es parte del trabajo de tesis: “ CONTROL DE SEGURIDAD EN UNA PLATAFORMA EDUCATIVA INSTITUCIONAL”. Y busca determinar la validación del trabajo en base a opiniones de expertos y sus conocimientos que tiene sobre este tema, ayudando a tener una valoración sobre lo realizado. Sus respuestas serán tratadas de forma impersonal.

PROPUESTA A VALIDAR	Guía de Buenas prácticas de Ciberseguridad para el aseguramiento de una plataforma educativa
Objetivo de la validación	Determinar si la propuesta planteada cumple criterios técnicos y es aplicable a la realidad de la institución objeto de estudio
Experto	Ing. David Guevara A, Mg
Función de los Expertos	● Revisar y Analizar la propuesta ● Llenar el cuestionario de validación
Instrumento de validación	Cuestionario de 6 preguntas
Escala de validación	5 Muy Adecuada 4 Adecuada 3 Poco Adecuada 2 Inadecuada 1 Muy inadecuada

Gracias por su colaboración, responda a las siguientes preguntas:

Modelo de encuesta para obtener información sobre criterios específicos de expertos en base al trabajo de Tesis

Indicador	5 Muy Adecuada	4 Adecuada	3 Poco Adecuada	2 Inadecuada	1 Muy inadecuada	Total
1. Valore la estructura y pertinencia de la Unidad de Gestión de Ciberseguridad propuesta para el ITS	X					
2. Valore el contenido y nivel técnico de la Norma de Ciberseguridad propuesta para el ITS Pelileo	X					
3. En cuanto al análisis de vulnerabilidades realizado dentro de la investigación, valore su nivel técnico y resultados.		X				
4. Evalúe los controles propuestos que deben implementarse en el ITS acorde a las normativas internacionales tomadas como base.		X				
5. Evalúe las salvaguardas planteadas para contrarrestar las vulnerabilidades detectadas		X				
6. Valore la pertinencia de la guía de buenas prácticas propuesta.	X					

Qué elementos técnicos sugeriría implementar a futuro para complementar la propuesta

El tema propuesto es adecuado, y está correctamente desarrollado, yo sugiero a futuro proponer el uso de metodologías de continuidad de negocio en caso de existir problemas de seguridad.