UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACION FINANZAS E INFORMÁTICA

CARRERA

INGENIERIA EN SISTEMAS DE INFORMACIÓN

TEMA:

PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA EL MODULO PRE UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO BASADO EN LA NORMA ISO 27001

ALUMNO:

ANTONIO ALEXANDER PALMA VERA

CORREO:

apalmav@fafi.utb.edu.ec

TUTOR:

ING. ERICK RICAURTE ZAMBRANO

PERDIODO ACADEMICO:

2022

DISEÑAR UN PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA EL MODULO PRE UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO BASADO EN LA NORMA ISO 27001

RESUMEN

En la actualidad, el módulo pre universitario de la Universidad Técnica de Babahoyo, maneja varios procesos que permiten que la información del alumnado crezca de manera considerable, la misma que se vuelve susceptible a riesgos y vulnerabilidades. Debido a que, mediante un análisis, se encontraron falencias dentro de su sistema académico en especial en el módulo pre universitario. Para la solución de este problema, se procede a presentar un plan de gestión de seguridad informática basado en la norma ISO 27001 que permita mejorar la seguridad de la información del módulo pre universitario de la Universidad Técnica de Babahoyo. Para llevar a cabo esta investigación, se utilizó la investigación de campo para conocer y obtener la información acerca de la gestión de seguridad informática que maneja la entidad educativa, métodos de investigación deductivo – inductivo, y técnicas de investigación como la observación y encuetas.

Se recurrió a utilizar una herramienta de hacking ético llamada OWASP ZAP, para realizar un análisis de vulnerabilidades del sistema SAI, con la cual se pudieron recopilar diversas vulnerabilidades que permiten resaltar que la entidad universitaria no cuenta con procedimientos eficientes para salvaguardar la información.

PALABRAS CLAVE

- ✓ Seguridad informática
- ✓ Vulnerabilidades
- ✓ Amenazas
- ✓ Plan de gestión

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1. PLANTEAMIENTO DEL PROBLEMA

A nivel internacional, las organizaciones presentan una gran cantidad de información que las ha hecho exitosas. Todos los continentes tienen los llamados piratas informáticos que no son más que piratas hackers o crackers. Usan la sabiduría del campo técnico para cometer delitos informáticos y extraer tanta información confidencial como sea posible dentro de las corporaciones.

Un plan de gestión de seguridad informática es de importante relevancia dentro de una empresa u organización, garantizando la seguridad de la información. De esta manera surgen a nivel internacional normas estandarizadas que se pueden adaptar a la gestión de pequeñas y grandes cantidades de datos, los mismos que son fundamentales para que una organización pueda cumplir con sus actividades. En toda empresa u organización debe existir un plan de gestión de seguridad informática que garantice la integridad de sus datos. Desde este punto surgen de manera internacional diversas normas estandarizadas que se pueden aplicar y adaptar al manejo de pequeñas y grandes cantidades de datos o información, las mismas que son esenciales para llevar a cabo las actividades y procesos de una entidad. En la actualidad, la Universidad Técnica de Babahoyo cuenta con su sistema académico integral creado por el Ing. Alexander izquierdo, especialista de proyectos y soluciones tecnológicas en el año 2014, y su modulo pre universitario fue creado a partir del segundo periodo del año 2018, con el objetivo de automatizar los procesos de la entidad universitaria, este sistema maneja varios procesos que permiten que la información del alumnado crezca de manera considerable, la misma que se vuelve susceptible a riesgos y vulnerabilidades. Además, las TIC y las políticas de seguridad informática que disponen no son aprovechados en su totalidad.

El problema radica en que el módulo pre universitario carece de políticas que estén basadas al régimen de las normas estandarizadas para la seguridad de la información, debido a que mediante prácticas de ataques informáticos realizados en clases con fin educativo a los servidores de la entidad universitaria, se encontraron falencias dentro de su sistema académico en especial en el módulo pre universitario, en el cual, existen puertos abiertos, y fallas en la programación por donde la información puede ser filtrada por personas externas a la entidad, la entidad universitaria ha aplicado limitadas normas inherentes a la seguridad informática del módulo, esto determina que poco se hace por tratar de implementar políticas que permitan proteger la información y las políticas de seguridad con las que cuenta, no se basa en ningún estándar, como consecuencia, no se garantiza la confidencialidad, disponibilidad e integridad de los datos que es propiedad de la institución educativa.

De todo lo mencionado anteriormente se puede evidenciar que la entidad universitaria podría tener problemas con el módulo pre universitario en lo que tiene que ver con la seguridad de la información, la cual incide directamente con el alumnado y en el aprovechamiento adecuado de dichos recursos.

1. JUSTIFICACION

La investigación se llevó a cabo en el sistema SAI, en su módulo pre universitario de la Universidad Técnica de Babahoyo, en donde se pudo observar principalmente la carencia de normas establecidas para garantizar la seguridad de los datos, además, en el presente estudio se realizó un análisis de vulnerabilidades utilizando una herramienta de hacking ético llamado OWASP ZAP y se descubrió los problemas que tiene al no contar con un plan de contingencia ante algún tipo de amenaza o robo de información. En la entidad hay que analizar muchos aspectos en cuanto a seguridad, generalmente dentro del área de TICS ya que no cuentan con una correcta gestión en la seguridad de la información, programación y activos, obteniendo problemas en el incumplimiento de las políticas, perdida de conectividad hacia internet, puertos abiertos, fallas en la programación, entre otros. En base a los riesgos que presenta la entidad universitaria, da paso a la fundamentación de una norma que pueda integrar parámetros de seguridad, que ayudara a prevenir cualquier amenaza que ponga en peligro o riesgo los activos de información y/o evitar una inestabilidad en el ámbito laboral.

Se eligió la norma ISO 27001 debido a su marco de referencia ampliamente aceptado relacionado con la gestión de la seguridad. Una característica clave es la capacidad de adaptarse a las necesidades de una organización independientemente de su tamaño. Este reglamento es responsable de mantener la confidencialidad, integridad y disponibilidad de la información y los activos de la agencia.

2. OBJETIVOS

2.1.OBJETIVO GENERAL

Diseñar un plan de gestión de seguridad informática basado en la norma ISO 27001 que permita mejorar la seguridad de la información en el sistema SAI, en su módulo pre universitario de la Universidad Técnica de Babahoyo.

2.2.OBJETIVOS ESPECÍFICOS

- ✓ Realizar el diagnostico de vulnerabilidades del sistema SAI en su módulo pre universitario de dicha institución educativa.
- ✓ Analizar el impacto de las vulnerabilidades mediante la herramienta de hacking ético OWASP ZAP y su probabilidad de ocurrencia.
- ✓ Integrar los beneficios que ofrece la norma ISO 27001 para la protección ante cualquier amenaza que pueda poner en peligro o riesgo la información de los estudiantes y la institución.

3. LÍNEA DE INVESTIGACIÓN

La línea de investigación a utilizar es Sistemas de información y comunicación, emprendimiento e innovación. Debido a que el uso generalizado de la tecnología de la información en los negocios hace que sea aún más fácil de escalar. La comunicación con los clientes en ciudades o países diferentes a donde se encuentra la empresa, la capacidad de hacer negocios a través de Internet, y la facilidad de uso de la tecnología y la globalización de la información para todos, hacen que las organizaciones más ha ayudado a crecer más rápido, pero la proximidad y la facilidad de uso de la tecnología plantea problemas específicos para las organizaciones, haciéndolas vulnerables a las amenazas ambientales en el día a día y haciéndolas más apropiadas para las operaciones comerciales. Puede ser un riesgo real para las organizaciones que afecta su funcionamiento. Para contrarrestar estas amenazas, las organizaciones deben desarrollar planes de acción para ellas.

3.1.SUBLÍNEA DE INVESTIGACIÓN

La sublínea de investigación a utilizar es: Redes y tecnología inteligentes de software y hardware, debido a que la seguridad de la información es muy importante en una organización, ya sea en sus redes, hardware y software. Cuando se encuentra un problema muchas veces no se toma en cuenta o simplemente se establecen políticas de seguridad de acuerdo a la situación de la empresa y lo que está pasando, no se enfoca en implementar la seguridad de la información. Es importante analizar los activos de información que tienen mayor impacto en la organización y gestionar el riesgo. Las políticas de seguridad deben revisarse periódicamente y seguir un plan de mejora continua.

4. MARCO CONCEPTUAL

ANTECEDENTES

Para desarrollar el plan se consultaron varios proyectos de investigación enfocados en un plan de gestión de seguridad TI basado en la norma ISO 27001.

En la universidad técnica de Ambato, Mayorga, Oswaldo, Moposita, & Luis (2020) han desarrollado un proyecto de investigación titulado "Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Tecnologías de la Información de la Dirección General de Tecnologías de la Información y Comando de las Fuerzas Armadas. Armadas, utilizando la norma ISO 27001: 2013, un documento de análisis de diseño del Sistema de Gestión de Seguridad de la Información (SGSI) que establece políticas de seguridad estandarizadas internacionalmente adaptadas al sector militar de la industria y con avances tecnológicos, implementa metodologías para evaluar y mitigar riesgos, evitar fugas de información.

En la Universidad Nacional de Trujillo, Rodríguez, Ivon, Cueva, & Jhonatan (2018) desarrollaron un proyecto de investigación titulado “Implementación de un Plan de Seguridad para la Red de la Unidad Educativa Privada Femenina Cardenal Spellman”, en el cual planteó un diagnóstico para implementar un plan de seguridad en la red por buscando errores, técnicas de piratería ética y configuración de dispositivos de infraestructura de TI basados en programas gubernamentales de Seguridad de la Información (EGSI) e implementación de políticas de privacidad con Normativa ISO 27001.

En la Escuela Superior Politécnica del litoral, Orellana & Arturo (2019) realizaron un estudio titulado “El Plan de Seguridad Informática de los Sistemas de Información de la fiscalía general de la Nación”, en el cual establecieron una metodología de discusión para diseñar un plan de seguridad informática a través de la aplicación de buenas prácticas de seguridad. para mantener la confidencialidad y disponibilidad. Además, se realiza la identificación de riesgos relacionados con los sistemas de información de la dependencia y se establecen controles efectivos para mantener segura la información de la entidad.

4.1.SEGURIDAD INFORMÁTICA

La seguridad de TI garantiza la integridad, disponibilidad y acceso a la información perteneciente a una entidad, cuyo objetivo principal es mantener un riesgo mínimo para los recursos de TI para garantizar la continuidad de las operaciones de la organización, reducir costos con una plataforma de gobierno estructurada por técnicas de seguridad. permite conservar en todo momento los documentos, archivos y ficheros informáticos de la empresa manteniendo una total fiabilidad. (Figueroa, Rodriguez, Bone, & Saltos, 2017)

Las cuatro áreas clave de la seguridad de TI incluyen:

1. **Confidencialidad**: Solo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Solo los usuarios autorizados pueden modificar los datos si es necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios según sea necesario.
4. **Autenticidad**: En realidad te estás comunicando con quien crees que eres.

La seguridad informática es muy importante para evitar el robo de datos como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos, etc., lo cual es fundamental en la comunicación actual.

4.2.IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA

Según Hernández, Cantero, Giseth, Vidal, & Marcela (2019) afirman que la seguridad informática es un concepto de seguridad que nació en una época en la que no existían las redes de alta velocidad, los teléfonos móviles ni los servicios de Internet como las redes sociales o las tiendas virtuales. Es por esto que la seguridad informática muchas veces se enfoca en proteger los sistemas, es decir, las computadoras, las redes y el resto de la infraestructura de nuestra organización. La seguridad informática es un concepto fundamental de la ingeniería.

Según la norma ISO27001, Un Sistema de Gestión de la Seguridad de la Información (SGSI) es parte de un sistema de gestión común, basado en un enfoque de riesgo empresarial, que se establece para crear, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. Esto significa que se detendrá de forma intuitiva y comenzará a controlar lo que sucede en los sistemas de información y la información. Esto nos permitirá comprender mejor nuestra organización, cómo funciona y qué podemos hacer para mejorar la situación.

4.3.PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

Una organización debe entender la seguridad de la información como un proceso y no como un producto que se puede "comprar" o "instalar". Es por tanto un ciclo iterativo que incluye

actividades como evaluación de riesgos, prevención, detección y respuesta a incidentes de seguridad. Para realizar las actividades descritas en el apartado anterior, como parte del proceso de gestión de la seguridad de la información, es necesario considerar una serie de servicios o funciones de seguridad de la información:

4.4.OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

"Su objetivo principal es proteger recursos humanos o de la empresa de gran valor en hardware o software. Asimismo, se toman precauciones para asegurar que las organizaciones, personas o empresas tengan posibilidades de alcanzar los objetivos fijados. Le permite controlar y proteger sus sistemas, recursos, activos económicos, legales." (Durang, 2019). Por lo tanto, otro objetivo de seguridad es combatir los ataques de malware, virus y vulnerabilidades con los que luchan las organizaciones en la actualidad.

4.5.AMENAZAS A LA SEGURIDAD DE LA INFORMACIÓN

Amenaza hace referencia a cualquier tipo de elemento o acción que se provoque para amenazar la seguridad de la información, surgiendo igualmente al detectar la existencia de vulnerabilidades que pueden ser utilizadas en diferentes situaciones para dañar o sustraer información. "El aumento de las vulnerabilidades proviene del uso indebido de la tecnología por parte de los usuarios, también de diversas técnicas como la ingeniería social, la falta de capacitación del personal y la mayor rentabilidad de los ataques". (Muñoz & Rivas, 2017)

Para lograr un sistema de información seguro y confiable se establecen una serie de estándares, protocolos, métodos, reglas y técnicas. Sin embargo, hay amenazas a considerar:

- ✓ **Usuarios**: Se considera que es la mayor causa de problemas relacionados con la seguridad de un sistema informático, ya que sus acciones pueden acarrear graves consecuencias.
- ✓ **Malware**: Conocido como software malicioso que tiene como objetivo dañar una computadora cuando se instalan o utilizan datos ilegalmente.
- ✓ **Error de programación**: Este es un error mal desarrollado, pero también debe considerarse un riesgo, ya que evita que el sistema operativo y las aplicaciones queden obsoletos.
- ✓ **Intrusos**: cuando personas no autorizadas acceden a programas o datos a los que no deberían tener acceso.
- ✓ **Desastres**: el hardware de la computadora también se puede perder o dañar debido a un mal manejo o una intención maliciosa, como situaciones como robo, incendio o inundación.
- ✓ **Falla electrónica**: un sistema informático general puede verse afectado por una falla de energía o una falla lógica como cualquier dispositivo imperfecto.
- ✓ **Desastres naturales**: rayo, terremoto, inundación.
- ✓ **Copias de seguridad**: Para proteger los datos de forma eficaz, las copias de seguridad o copias de seguridad son imprescindibles.

4.6.CONFIDENCIALIDAD

Es la cualidad que debe tener un documento o archivo para que sólo una persona o sistema autorizado pueda entenderlo o leerlo.

"Por lo tanto, un documento (o archivo o mensaje) se considera confidencial si y solo si puede ser entendido por la persona u organización con la que está dirigido o autorizado. En el caso de un mensaje, esto evita que sea interceptado y leído por una persona no autorizada." (Bogantes, 2020, pág. 3)

4.7.VULNERABILIDADES

Las vulnerabilidades son claramente las debilidades de los sistemas informáticos y donde operan; la presencia exclusiva de una o más vulnerabilidades que no sean autodestructivas debe existir una amenaza a explotar y causar problemas en la organización empresarial, de esta manera se puede suponer que si la vulnerabilidad no tiene amenaza no será necesario aplicar un cheque.

Las áreas donde se pueden identificar vulnerabilidades de seguridad son:

- **Organización**: se ve afectada por ser el lugar físico donde trabaja un grupo de personas tanto dentro como fuera.
- **Procesos y Procedimientos**: Los procesos y procedimientos se verán afectados por su participación en el procesamiento de la información.
- **Recursos humanos**: son las personas que son los principales responsables de las vulnerabilidades que afectan a la organización porque son ellos quienes trabajan y manipulan la información, ya sea física o lógica.

- **Medio ambiente**: El medio ambiente se verá afectado si no se siguen las pautas para mantener un espacio estable y libre de amenazas.
- **Configuración del sistema de información**: debido a la falta de una correcta configuración del sistema de información, la brecha queda abierta a vulnerabilidades que pueden ser aprovechadas por los malos.
- **Hardware y software**: La selección del tipo de tecnología a utilizar para las tareas de la empresa debe tener en cuenta la seguridad que ofrece y las ventajas que se obtienen con su uso.
- **Equipos de comunicación**: Es fundamental considerar la seguridad de los medios que usamos para comunicarnos, ya que dentro de una organización siempre habrá interacciones con diferentes usuarios internos y externos.

4.8.ADMINISTRACIÓN DE RIESGOS

Según Gonzalez, Lorenzo, Andino, & Silva (2018) deducen que el proceso interactivo e iterativo de evaluación y gestión de riesgos basada en el conocimiento con sus respectivos impactos, orientado a mejorar la toma de decisiones dentro de la organización. La gestión de riesgos se puede aplicar en cualquier situación que presente una oportunidad de mejora para la empresa, los factores clave que se deben tener en cuenta en TI son: seguridad, control (prevención, detección y remediación), lineamientos de uso y políticas a implementar. Se deben evitar tareas a nivel de toda la organización de la empresa en sus niveles comercial, financiero, administrativo y de sistemas.

La aplicación de la norma ISO 27001 sobre seguridad, la gestión de riesgos es una de las tareas más importantes cuando queremos definir un proyecto y las iniciativas que tomaremos

para mejorar la seguridad de la información en su organización. El objetivo tras el análisis de riesgos es poder reducir el riesgo en el que incurre la empresa a un nivel aceptable sobre la base del análisis de situación inicial.

4.9.PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA

"Un plan de gestión de seguridad de la información es un conjunto de medios administrativos, técnicos y de personal que, de manera interdependiente, aseguran niveles de seguridad de la información acordes con la importancia de los activos a proteger y los riesgos estimados". (Ramírez, 2017). El Plan de Gestión de la Seguridad TI es el documento básico que establece los principios organizativos y funcionales de las operaciones de seguridad TI para la organización y reúne todas las políticas y responsabilidades de seguridad de los participantes en los procesos TI, así como las medidas y procedimientos prevenir, detectar y responder a las amenazas a similar.

4.10. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Según Basurco & Alberto (2020), un SGSI adopta un enfoque sistemático, utilizado para gestionar la información confidencial de una organización empresarial con el fin de mantener su integridad y confidencialidad. Este modelo de gestión de riesgos incluye a todo el personal, procesos internos, procesos externos y sistemas gestionados por el departamento de TI. Al implementar ISMS, ayuda a las pequeñas, medianas y grandes empresas a proteger los activos de información, lo que permitirá a la empresa lograr confiabilidad frente a los competidores.

4.11. LA ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO)

La Organización Internacional para la Estandarización conocida como ISO es una organización internacional independiente, no gubernamental, con muchos miembros, el trabajo de esta organización a través de sus miembros es recopilar conocimientos y desarrollar estándares basados en el consenso alineados con el mercado que ayuden a impulsar soluciones e innovación para empresas que enfrentan desafíos globales. (Gómez & Fernanda, 2019)

4.12. NORMA ISO 27001

La norma ISO 27001 establecida por la Organización Internacional de Normalización para certificar los sistemas de gestión de seguridad de la información pertenecientes a organizaciones comerciales, al lograr la certificación. “las empresas pueden demostrar la integridad de sus datos a los clientes, accionistas y empleados de la entidad; Al mismo tiempo, mejora la seguridad de la información y reduce los peligros actuales, como el fraude, la pérdida o la fuga de datos importantes de una empresa.” (Quispe & Samuel, 2020)

Al verificar que una empresa cumple con los requisitos para certificarse con la Norma ISO 27001, será emitido por un organismo de certificación independiente y autorizada la certificación con la cual quedara demostrado que la organización empresarial ha establecido políticas de precaución para proteger la información.

4.12.1. ANEXOS DE LA NORMA ISO 27001

Dentro de las normas ISO 27001, el Anexo A es más conocido por ser prescriptivo, lo que indica que su uso es esencial. También es parte integral de la norma ISO 27001 en lo que respecta a los controles de seguridad, ya que proporciona una lista de controles básicos para mejorar la protección de la información dentro de una organización. A continuación, se muestran los 14 anexos o dominios que componen la norma ISO 27001.

- **Anexo 5**: Políticas de seguridad de la información: se enfoca en los controles sobre como revisar y escribir las políticas de seguridad.
- **Anexo 6:** Aspectos organizativos de la Seguridad de la Información: se enfoca en establecer responsabilidades, en los dispositivos móviles y el teletrabajo.
- **Anexo 7:** Seguridad ligada a los Recursos Humanos: se enfoca en las situaciones referentes a la contratación de un nuevo personal.
- **Anexo 8:** Gestión de recursos: Hace referencia a los nuevos inventarios, clasificando los medios de almacenamiento y la información.
- **Anexo 9**: Control de Accesos: Hace referencia al modo de acceso a la información, medios de almacenamiento o cualquier otro dispositivo que contenga información.
- **Anexo 10:** Cifrado: Hace énfasis a los controles para la gestión de encriptación de los datos e información.
- **Anexo 11**: Seguridad física y ambiental: Factores externos que pueden afectar la seguridad, la seguridad del dispositivo y los controles para garantizar los medios.
- **Anexo 12:** Seguridad en la Operativa: Controles relacionados con la gestión de malware o protección contra vulnerabilidades.

- **Anexo 13:** Seguridad de las Telecomunicaciones: Controlar la seguridad de la red, la transferencia de información y la mensajería.
- **Anexo 14:** Adquisición, desarrollo y mantenimiento de los Sistemas de Información: Controles que establecen los requisitos de seguridad para el desarrollo y soporte.
- **Anexo 15:** Relaciones con Suministradores: Contiene lo necesario para la celebración de contratos y seguimiento de proveedores.
- **Anexo 16:** Gestión de Incidentes en Seguridad de la Información: Se utilizan para reportar eventos, vulnerabilidades y procedimientos de respuesta.
- **Anexo 17:** Aspectos de Seguridad de la Información en la gestión de continuidad del negocio: Está relacionado con la planificación de la continuidad del negocio.
- **Anexo 18:** Cumplimiento: Control sobre la identificación e implementación de las normas de seguridad de la información.

4.13. HACKING ÉTICO

El hacking ético se define por la actividad de profesionales dedicados. H. Los hackers éticos que no recurran a estas prácticas con los fines delictivos tradicionalmente asociados a ellas. Estas personas son contratadas para piratear sistemas, identificar y corregir vulnerabilidades potenciales y prevenir de manera efectiva la explotación por parte de piratas informáticos malintencionados. Evalúan, fortalecen y mejoran la seguridad. es un experto que se especializa en pruebas de penetración de sistemas informáticos y software para Son responsables de implementar hacks éticos para probar la seguridad de sus sistemas.

4.14. HACKING ÉTICO EXTERNO

Este tipo de pirateo se realiza a través de redes públicas de Internet. Esto indica que se está realizando un ataque contra el equipo de una institución que brinda servicios a Internet. B. Servidores web, servidores de correo, servidores de nombres, etc.

4.15. HACKING ÉTICO INTERNO

Este truco se hace internamente en una computadora en la red corporativa. Según varios autores, muchas vulnerabilidades suelen descubrirse durante este tipo de pruebas. técnicas del Hacking

4.16. KALI LINUX

Esta poderosa herramienta es un sistema operativo basado en Debian con funciones y aplicaciones que son muy útiles para las pruebas de penetración y la auditoría de redes. Kali Linux es un sistema operativo gratuito utilizado para pruebas de seguridad informática. Con más de 300 herramientas de prueba de penetración incluidas, los administradores pueden auto verificar la efectividad de sus estrategias de seguridad, riesgos y mitigación. “Hace que las pruebas de penetración sean más fáciles y accesibles para administradores y especialistas en seguridad. También se adhiere a los estándares de Debian, lo que facilita mucho las cosas gracias a su interfaz gráfica. Los usuarios pueden cambiar el sistema operativo según sus necesidades y preferencias.” (Sánchez, 2017)

4.17. NMAP

Según el criterio de Tandazo & Rueda (2017), NMAP es una herramienta de auditoría de seguridad de red que realiza un análisis de cada paquete IP. Los administradores de red suelen mantener el mismo inventario porque NMAP procesa la información de DNS que tiene en cuenta los tipos de puertos, los protocolos, los estados de los puertos y las direcciones MAC vinculadas a esos puertos.

4.18. OWASP ZAP

OWASP ZAP es un programa de escaneo de vulnerabilidades para varios sistemas operativos. Consiste en ejecutar el análisis en el sistema de destino, y ZAP, un cliente (consola o basado en gráficos) que muestra e informa sobre el progreso del análisis. Desde la consola, puede programar OWASP ZAP para realizar análisis programados mediante cron.

"En funcionamiento normal, OWASP ZAP primero escanea el puerto con nmap o su propio escáner de puerto para encontrar el puerto abierto, luego intenta varios exploits para vulnerarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de complementos, están escritas en NASL (Nessus Attack Scripting Language)" (Lopez, 2017, pág. 4)

5. MARCO METODOLÓGICO

5.1.TIPOS DE INVESTIGACIÓN

Investigación de campo

La investigación de campo permitió obtener información necesaria para llevar a cabo la investigación en el mismo lugar de los hechos, donde circunscribe el objeto de investigación que es en la Universidad Técnica de Babahoyo, para conocer y obtener la información acerca de la gestión de seguridad informática que maneja la entidad educativa.

5.2.METODOS DE INVESTIGACIÓN

Método Inductivo/Deductivo

El método Inductivo/Deductivo se aplicó porque a través de la base de conceptos y definiciones del marco teórico, permitió conocer más a profundidad el impacto positivo que podría tener al pasar de la parte teórica a la práctica en la gestión de la seguridad de la Información y los Activos de la Universidad técnica de Babahoyo.

5.3. ANALISIS DE VULNERABILIDADES

Se realizo un análisis de vulnerabilidades usando el sistema operativo Kali Linux en su última versión (2022), luego de ello se procedió a instalar el programa de hacking ético llamado OWASP ZAP, en el cual se colocará el enlace correspondiente del sistema académico integran en su modulo pre universitario.

5.4.TÉCNICAS DE INVESTIGACIÓN

La Entrevista

Para el presente trabajo de investigación, es necesario e imprescindible realizar la entrevista como técnica fundamental para la obtención de información de primera mano, la cual será aplicada al director del Departamento de las TIC´s y al Oficial encargado de Seguridad Informática de la Universidad técnica de Babahoyo.

Observación

Esta técnica permitió verificar directamente en el sitio, la forma en la que se desarrolla el trabajo en relación a la Gestión de Seguridad Informática.

5.5.INSTRUMENTOS DE INVESTIGACIÓN

Los instrumentos utilizados en la investigación son:

- ✓ Guía de entrevista.
- ✓ Guía de observación

5.6.ANÁLISIS DE VULNERABILIDADES Y RIESGOS

En esta sección, se recurrió a utilizar una herramienta de hacking ético llamada OWASP ZAP, para realizar un análisis de vulnerabilidades del sistema SAI, los cuales amenazan con poner en riesgo la información estudiantil e institucional de la Universidad Técnica de Babahoyo.

A continuación, se muestra el resultado después de haber realizado un profundo análisis, determinando las amenazas y vulnerabilidades encontradas:

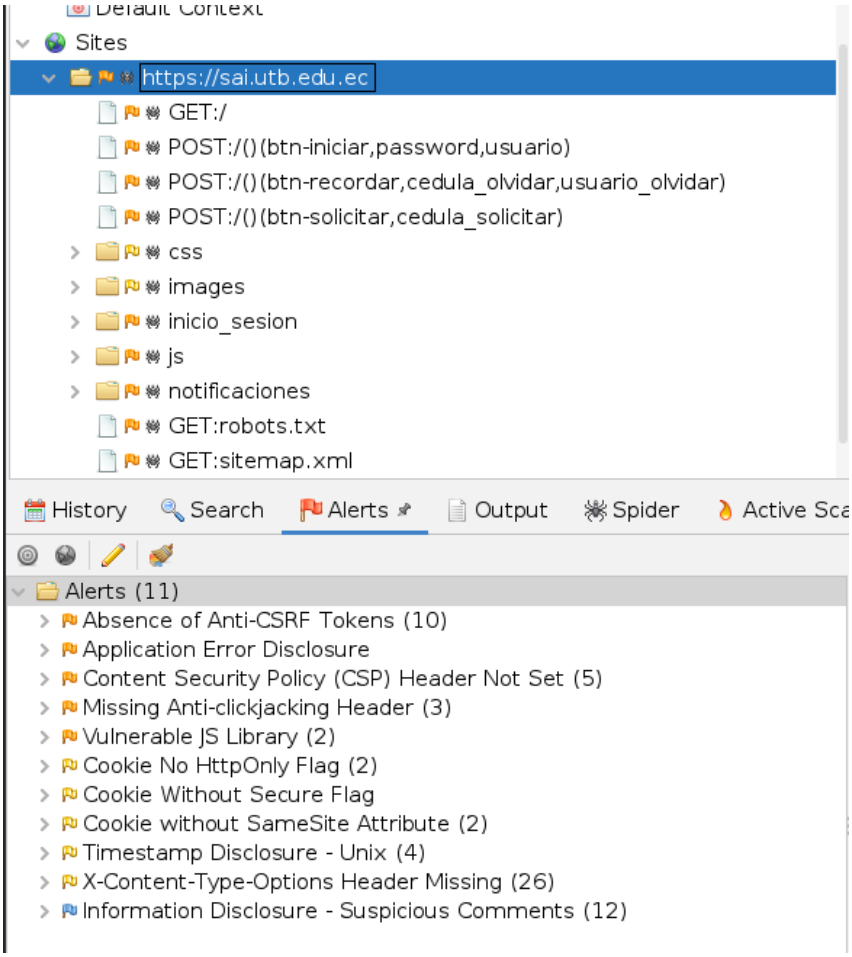
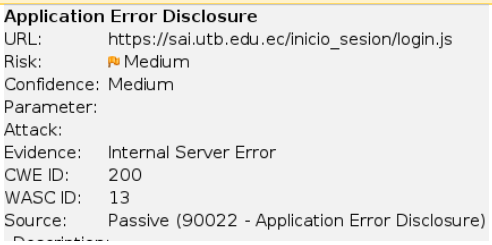
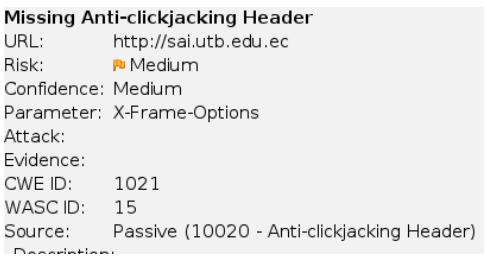


Ilustración 1Analisis de vulnerabilidades. Fuente: Palma (2022)

En la siguiente tabla, se detallan las vulnerabilidades encontradas con su respectivo nivel de riesgo:

VULNERABILIDAD		POSIBLE AMENAZA	RIESGO	ALERTAS
Ausencia de tokens anti-CSRF		Este ataque obliga al navegador web de la víctima, verificado por un servicio (como el correo electrónico o la banca en casa), a enviar solicitudes a una aplicación web vulnerable.	MEDIO	10
Divulgación de error de aplicación		Un atacante autenticado puede aprovechar esta vulnerabilidad y podría obtener información para comprometer el sistema del usuario.	MEDIO	1
Encabezado de política de seguridad de contenido (CSP) no establecido		El principal objetivo del CSP es mitigar y reportar ataques XSS. Los ataques XSS se aprovechan de la confianza del navegador en el contenido que recibe del servidor. El navegador de la víctima ejecutará los scripts maliciosos porque confía en la fuente del contenido, aun cuando dicho contenido no provenga de donde se supone.	MEDIO	5
Falta el encabezado antisecuestro de clics		En lugar de que un elemento visible maneje los clics, los clics son secuestrados y recibidos por un elemento dentro de un iframe no visual en el sitio web. El secuestro de clics puede provocar intentos de intrusión, correos electrónicos no	MEDIO	3

		deseados, intercambios de credenciales u otras consecuencias maliciosas específicas del sitio.		
Biblioteca JS vulnerable	**Vulnerable JS Library** URL: https://sai.utb.edu.ec/js/bootstrap.min.js Risk: Medium Confidence: Medium Parameter: Attack: Evidence: * Bootstrap v3.3.2 CWE ID: 829 WASC ID: Source: Passive (10003 - Vulnerable JS Library)	Las bibliotecas de JavaScript de terceros pueden generar una variedad de vulnerabilidades basadas en DOM, incluido DOM-XSS, que pueden explotarse para apoderarse de las cuentas de los usuarios.	MEDIO	2
Bandera de Cookie No HttpOnly	**Cookie No HttpOnly Flag** URL: http://sai.utb.edu.ec Risk: Low Confidence: Medium Parameter: PHPSESSID Attack: Evidence: Set-Cookie: PHPSESSID CWE ID: 1004 WASC ID: 13 Source: Passive (10010 - Cookie No HttpOnly Flag)	la cookie (típicamente su cookie de sesión) se vuelve vulnerable al robo de modificación mediante script malicioso.	BAJO	2
Divulgación de información - Comentarios sospechosos	**Information Disclosure - Suspicious Comments** URL: http://sai.utb.edu.ec Risk: Informational Confidence: Medium Parameter: Attack: Evidence: user CWE ID: 200 WASC ID: 13 Source: Passive (10027 - Information Disclosure - Suspicious	Un atacante que aprovechara esta vulnerabilidad podría descifrar el tráfico cifrado de TLS/SSL.	BAJO	12

Tabla 1Vulnerabilidades encontradas. Fuente: Palma (2022)

6. RESULTADOS

Este proyecto está orientado al desarrollo de un plan de gestión de seguridad informática que permita mantener la integridad, confidencialidad y alta disponibilidad de los datos del módulo pre universitario de la Universidad Técnica de Babahoyo, basándose en la norma ISO 27001.

6.1.Alcance del plan de seguridad informática

Para definir el alcance, se consideraron aspectos importantes como los activos, la estructura organizacional y los recursos que forman parte de los procesos diarios en el sistema SAI en su Módulo Preuniversitario.

Para ello se hará énfasis en los activos, que por su valor en relación a la disponibilidad de la información del sistema SAI en su módulo pre universitario, pueda ser susceptible a sufrir riesgos de seguridad:

- **Recursos de información** (gestión informática): Bases de datos, información almacenada en medios digitales o impresos.
- **Activos de software** (departamento de TI): Sistema académico integral en su módulo pre universitario.
- **Activos de hardware** (gestión informática): Base de datos o copia de seguridad.

6.2.Impacto de vulnerabilidades

Después de utilizar la herramienta OWASP ZAP para el análisis de vulnerabilidades y riesgos del sistema SAI, en su módulo pre universitario. Se procede a detallar los impactos que estas vulnerabilidades tienen y a quien afecta.

IMPACTO/CONSECUENCIAS	SISTEMA ACADÉMICO INTEGRAL	SERVIDOR / HARDWARE	BASE DE DATOS	SOFTWARE EN EL SERVIDOR	PORCENTAJE DE INCIDENCIA
Ausencia de tokens anti-CSRF	1	0	0	0	25%
Divulgación de error de aplicación	1	1	1	0	75%
Encabezado de política de seguridad de contenido (CSP) no establecido	1	0	1	1	75%
Falta el encabezado antisecuestro de clics	1	0	0	0	25%
Biblioteca JS vulnerable	1	0	1	1	75%
Bandera de Cookie No HttpOnly	1	0	0	0	25%
Divulgación de información - Comentarios sospechosos	1	0	0	1	50%

Tabla 2Impacto de vulnerabilidades. Fuente: Palma (2022)

En la siguiente tabla se presentan los niveles de impacto que tiene cada vulnerabilidad encontrada

NIVEL DE IMPACTO	
1% - 25%	BAJO
25% - 50%	MEDIO
50% - 100%	ALTO

Tabla 3 Niveles de impacto de vulnerabilidades. Fuente: Palma (2022)

Se procede a realizar un plan de gestión de seguridad informática a partir del orden prioritario de las actividades a mitigar dependiendo de su nivel de impacto representado en el siguiente cuadro:

ACTIVIDAD	VULNERABILIDAD	NIVEL
ACT 1	Divulgación de error de aplicación	ALTO
ACT 2	Encabezado de política de seguridad de contenido (CSP) no establecido	ALTO
ACT 3	Biblioteca JS vulnerable	ALTO
ACT 4	Divulgación de información - Comentarios sospechosos	MEDIO
ACT 5	Falta el encabezado antisecuestro de clics	BAJO
ACT 6	Bandera de Cookie No HttpOnly	BAJO
ACT 7	Bandera de Cookie No HttpOnly	BAJO

Tabla 4 Plan de gestión por actividad. Fuente: Palma (2022)

Después de haber calculado los niveles de impacto de cada vulnerabilidad, se procede a detallar el nivel de probabilidad de ocurrencia de que cada vulnerabilidad encontrada sea violentada por atacantes externos, dichas probabilidades se muestran en la siguiente tabla desde la que muestra mayor impacto hasta la de menor impacto:

PROBABILIDAD				
ALTO	50% - 100%	Divulgación de error de aplicación	Encabezado de política de seguridad de contenido (CSP) no establecido	Biblioteca JS vulnerable
MEDIO	25% - 50%	Divulgación de información - Comentarios sospechosos		
BAJO	1% - 25%	Falta el encabezado antisecuestro de clics	Bandera de Cookie No HttpOnly	Ausencia de tokens anti-CSRF

Tabla 5 Niveles de probabilidades de amenazas. Fuente: Palma (2022)

7. DISCUSIÓN DE RESULTADOS

Mediante la investigación ya realizada, se proponen soluciones para las vulnerabilidades encontradas mediante el análisis con la herramienta de hacking ético llamada OWASP ZAP, la cual nos arroja resultados en un rango bajo de probabilidad de impacto del 1% al 14% se encontró la *falta de encabezado antisecuestro de click*, y *Bandera de Cookie No HttpOnly*, la solución recomendada para resolver estas vulnerabilidades es enmarcar las páginas en un sitio de Visualforce con páginas en dominios externos que se hayan agregado a una lista de dominios de confianza, además, se deben crear tokens CSRF para cada usuario que ingresa al sistema y almacenarlos, estos tokens deben ser únicos. Para ello se recomienda aplicar el *anexo 17* de la norma ISO 27001, el cual trata sobre la gestión de incidentes en la seguridad de la información, el mismo trata sobre detectar, evaluar e informar los incidentes que tanga la seguridad de la información.

Otra vulnerabilidad dentro de este rango de bajo impacto es *la ausencia de tokens anti-CSRF*, para solucionar este tipo de vulnerabilidad se debe bloquear la ejecución de secuencias de comandos para evitar que los formularios enviados mediante el método POST se envíen sin consentimiento de nadie. Se recomienda aplicar el *anexo 9* de la norma ISO 27001, el cual trata sobre los controles de accesos de usuarios, el mismo describe sobre asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios de información.

Dentro del rango medio de probabilidad de impacto del 14% - 29% se encontró la *Divulgación de información - Comentarios sospechosos,* para solucionar este tipo de vulnerabilidad se debe actualizar las claves de registro disponibles para las diferentes

versiones de .NET Framework y de esta manera lograr que no se pueda divulgar información del sistema académico integral. Se recomienda aplicar el *anexo 16* de la norma ISO 27001, el cual trata sobre la gestión de los incidentes que ocurren con la seguridad de la información, el mismo define sobre garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de vulnerabilidades y eventos de seguridad.

Dentro del rango alto de probabilidad del 29% - 50%, se encontró la *divulgación de error de aplicación* y el *encabezado de política de seguridad de contenido (CSP) no establecido,* para solucionar la divulgación de error de aplicación hay que utilizar canales de comunicación seguros al transferir datos entre el sistema académico integral y la base de datos, aparte de esto, verificar que partes del código de programación está causando este tipo de problemas, sin embargo, para solucionar el encabezado de política de seguridad de contenido (CSP) no establecido, se debe especificar que todo el contenido del sistema académico integral, en especial su módulo pre universitario, debe cargarse utilizando HTTPS, para de esta manera asegurar de que el navegador solo se conecte a través de canales grabados. Se recomienda aplicar el *anexo 16* de la norma ISO 27001, el cual trata sobre la gestión de los incidentes que ocurren con la seguridad de la información, el mismo define sobre garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de vulnerabilidades y eventos de seguridad.

Otra vulnerabilidad que está dentro del rango alto es sobre la *Biblioteca JS vulnerable,* y para darle solución a este problema se debe actualizar las bibliotecas de JavaScript y establecer HttpOnly dentro del código de programación para evitar que terceras

personas obtengan información de cookies a través de JS. Se recomienda aplicar el *anexo 12* de la norma ISO 27001, el cual trata sobre la protección contra códigos maliciosos, es decir, asegurarse de que el procesamiento de información esté protegido contra malware o contra personas que quieran atacar el sistema académico integral.

8. CONCLUSIONES

Mediante un plan de gestión de seguridad informática para sistema SAI en su módulo pre universitario de la universidad técnica de Babahoyo, basándose en las normas ISO 27001, sirvió de gran ayuda para identificar las vulnerabilidades y posibles amenazas que puede sufrir el sistema a futuro, aplicando controles adecuados para conservar la integridad y seguridad de la información.

Con la elaboración de un análisis de riesgos mediante una herramienta de hacking ético, se pudo identificar siete vulnerabilidades, de las cuales, 3 fueron de impacto bajo, 1 fue de impacto medio, y 3 de impacto alto, las cuales, si no se tratan y no se mitiga su nivel de riesgo, es posible que en un futuro el sistema académico integral en su modulo pre universitario sufra una violación por parte de terceros. La Universidad Técnica de Babahoyo debe poner énfasis en para garantizar su seguridad informática.

Los objetivos de este caso de estudio fueron cumplidos mediante el diagnostico de vulnerabilidades, el análisis de su impacto, probabilidad de ocurrencia de ataques y mitigar las mismas mediante un plan de gestión de seguridad informática basado en la norma ISO 27001.

Con la ayuda de una entrevista y una investigación de campo se logró evidenciar la falta de políticas y normas certificables en el sistema académico integral en su modulo pre universitario.

9. RECOMENDACIONES

La seguridad y confidencialidad de la información es esencial en todo tipo de entidades en la actualidad, es importante que la Universidad Técnica de Babahoyo despierte el compromiso y el interés por parte de los altos mandos, con el objetivo de brindar apoyo al área de sistemas y desarrollar un comité de seguridad informática, con el fin de gestionar la seguridad de la información del sistema académico integral en especial en su modulo pre universitario, dando un seguimiento en el cumplimiento de normas y políticas estandarizadas, para un manejo controlado de los activos de la información. Reducir el riesgo de vulnerabilidades de los activos de información de acuerdo con las políticas de seguridad propuestas en este caso de estudio basándose en los controles estandarizados ISO 27001.

Llevar a cabo capacitaciones de concientización para todos los docentes y alumnos de la entidad universitaria sobre el impacto de la seguridad de la información, También reconocer la importancia de proteger la información mediante el cumplimiento de políticas de seguridad y la prevención de incidentes que amenacen la continuidad de la entidad universitaria. Supervisar periódicamente las políticas de seguridad, evaluar su rendimiento y sugerir mejoras en función de las necesidades de la Universidad Técnica de Babahoyo.

Se toma conciencia sobre la importancia de la seguridad de la información actualmente, dando a conocer lo fundamental que es contar con plan de gestión de seguridad informática basándose en la norma ISO 27001, para así tener un procedimiento continuo en la gestión de la seguridad informática en el sistema SAI en su modulo pre universitario, y de esta manera tener la posibilidad de eliminar o mitigar los riesgos de la información.

10. REFERENCIAS

Basurco, R., & Alberto, G. (2020). *Implementación del Sistema de Gestión de Calidad (SGC) bajo el enfoque de la norma ISO 9001:2015, en una empresa que brinda servicios de seguridad informática y de la información.* Perú. Obtenido de https://repositorio.utp.edu.pe/handle/20.500.12867/3221

Bogantes, A. (2020). El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados. *Sistemas, cibernética e informática, 17,* 6. Obtenido de http://www.iiisci.org/journal/PDV/risci/pdfs/CB294NT20.pdf

Durang, A. (2019). *EVALUACIÓN DE TÉCNICAS DE ETHICAL HACKING PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD INFORMATICA EN UNA EMPRESA PRESTADORA DE SERVICIOS.* Pimentel, Perú. Obtenido de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/7359/Durand%20More%2c%20Andr%c3%a9s%20David.pdf?sequence=1&isAllowed=y

Figueroa, J., Rodriguez, R., Bone, C., & Saltos, J. (2017). *La seguridad informática y la seguridad de la información.* Manta, Ecuador. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/420

Gómez, C., & Fernanda, L. (2019). *Diseño de un sistema de gestión de seguridad informática para la e Empresa Flores Jayvana S.A.S.* Bogotá, Colombia. Obtenido de https://repository.unad.edu.co/handle/10596/28404

Gonzalez, S., Lorenzo, V., Andino, O., & Silva, N. (2018). La gestión de riesgo: el ausente recurrente de la administración de empresas. *Revista Ciencia UNEMI,* 13. Obtenido de https://www.redalyc.org/journal/5826/582661257005/582661257005.pdf

Hernández, M., Cantero, Z., Giseth, L., Vidal, R., & Marcela, D. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista venezolana de gerencia*, 11. Obtenido de https://www.redalyc.org/journal/290/29063446029/29063446029.pdf

Lopez, M. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. *Revista Publicando*, 21. Obtenido de https://core.ac.uk/download/pdf/236645046.pdf

Mayorga, M., Oswaldo, F., Moposita, T., & Luis, J. (2020). *Plan de gestión de seguridad informática basado en la Norma ISO 27001 para el Departamento de Tecnología de la Información en la Empresa Plasticaucho Industrial S.A.* Ambato, Ecuador. Obtenido de https://repositorio.uta.edu.ec/handle/123456789/30696

Muñoz, M., & Rivas, L. (2017). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI*, 15. Obtenido de https://pdfs.semanticscholar.org/2cfa/3c743f39189d6052b1816dd558c21c6a4355.pdf

Orellana, P., & Arturo, H. (2019). *Desarrollo de un plan de mitigación de seguridad informática a una red inalámbrica de comunicación de datos para una institución privada, a través de la aplicación de hacking ético para la identificación de amenazas, riesgos y vulnerabilidades.* Guayaquil, Ecuador. Obtenido de https://www.lareferencia.info/vufind/Record/EC_bdd37af53f57c674918b68d8e8a3fede

Quispe, A., & Samuel, E. (2020). *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao.* Lima, Perú. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/47276

Ramírez, M. L. (2017). Análisis de riesgos en un sistema de gestión de seguridad de la información (SGSI) con metodologías complementarias. *Universidad Piloto de Colombia*, 18. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2913/00004422.pdf?sequence=1&isAllowed=y

Rodríguez, C., Ivon, A., Cueva, S., & Jhonatan, W. (2018). *Plan de seguridad informática basado en la norma Iso 27002 para mejorar la gestión tecnológica del colegio carmelitas – Trujillo.* Trujillo, Perú. Obtenido de https://dspace.unitru.edu.pe/handle/UNITRU/11066

Sánchez, J. (2017). *Análisis de vulnerabilidades y diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato.* Ambato, Ecuador. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/25531/1/Tesis_t1232si.pdf

Tandazo, K., & Rueda, M. (2017). *PREVENCIÓN, DETECCIÓN Y REDUCCIÓN DE RIESGOS DE ATAQUES POR ESCANEO DE PUERTOS USANDO TECNOLOGÍAS DE VIRTUALIZACIÓN.* Sangolquí, Ecuador. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/6906/1/T-ESPE-047328.pdf

11. ANEXOS

Entrevista al Ing. Alberto Alcívar, director del departamento de tecnologías, y al Ing. Alexander Izquierdo, especialista de proyecto y soluciones tecnológicas, como se muestra en la siguiente tabla:

PREGUNTA	OBSERVACIÓN
1. ¿Qué problemas de seguridad informática ha tenido el sistema SAI en su módulo pre universitario?	• Exploits • Borrado de información • Piezas de Malware
2. ¿Qué problema fue más perjudicial para el sistema y que aún no se pueda controlar en su totalidad?	• La pérdida y manipulación de información • Inyecciones SQL
3. ¿Qué mecanismos, técnicas o herramientas de seguridad se utilizan en el sistema académico integral de la Universidad Técnica de Babahoyo?	Ninguno, no se ha considerado hasta el momento.
4. ¿Se aplican actualmente políticas o normas de seguridad para proteger la información la información en el sistema SAI en su modulo pre universitario?	No existen políticas certificables o estandarizadas.
5. ¿Qué conocimientos tiene sobre las políticas o normas que gestionan la Seguridad de la información?	Con respecto a las políticas y normas de seguridad de la información el conocimiento con el que se cuentas es parcialmente suficiente.
6. ¿Tiene conocimiento sobre las Normas ISO 27001?	El conocimiento con sobre las normas ISO 27001 es suficiente.
7. ¿Cree que es necesario un plan de gestión de seguridad informática para el sistema SAI en su modulo pre universitario basado en la norma ISO 27001 para mantener la confidencialidad de la información?	Si es necesario debido a la inexistencia de políticas y normas de seguridad para gestionar la información.

Tabla 6 Anexo de encuesta realizada. Fuente: Palma (2022)

Recuento de alertas por riesgo y confianza

		Confianza				
		Usuario confirmado	Alto	Medio	Bajo	Total
Riesgo	Alto	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Medio	0 (0,0%)	1 (9,1%)	3 (27,3%)	1 (9,1%)	5 (45,5%)
	Bajo	0 (0,0%)	0 (0,0%)	4 (36,4%)	1 (9,1%)	5 (45,5%)
	Informativo	0 (0,0%)	0 (0,0%)	0 (0,0%)	1 (9,1%)	1 (9,1%)
	Total	0 (0,0%)	1 (9,1%)	7 (63,6%)	3 (27,3%)	11 (100%)

Ilustración 2 Recuento de alertas por riesgo y confianza. Fuente: Palma (2022)

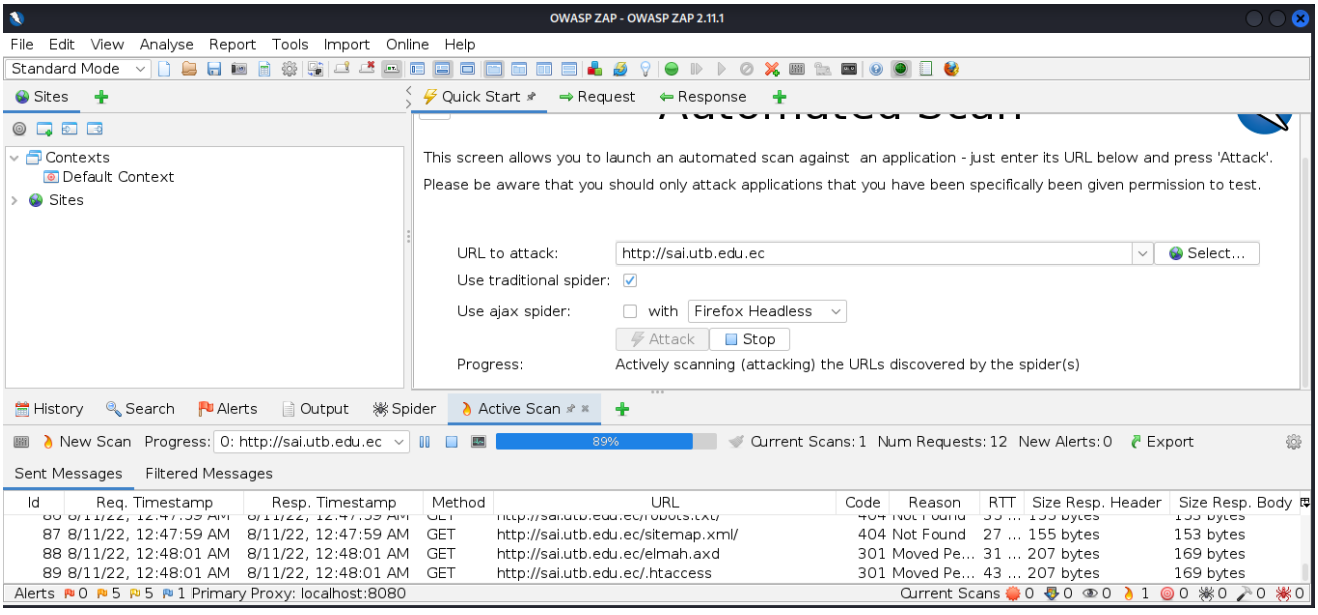


Ilustración 3 Programa de hacking ético OWASP ZAP. Fuente: Palma (2022)

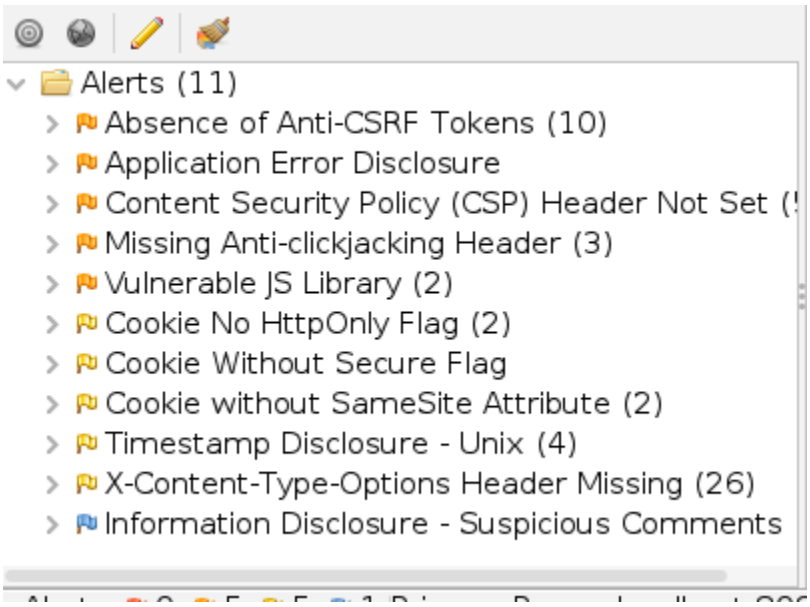


Ilustración 4 Vulnerabilidades encontradas con sus alertas. Fuente: Palma (2022)

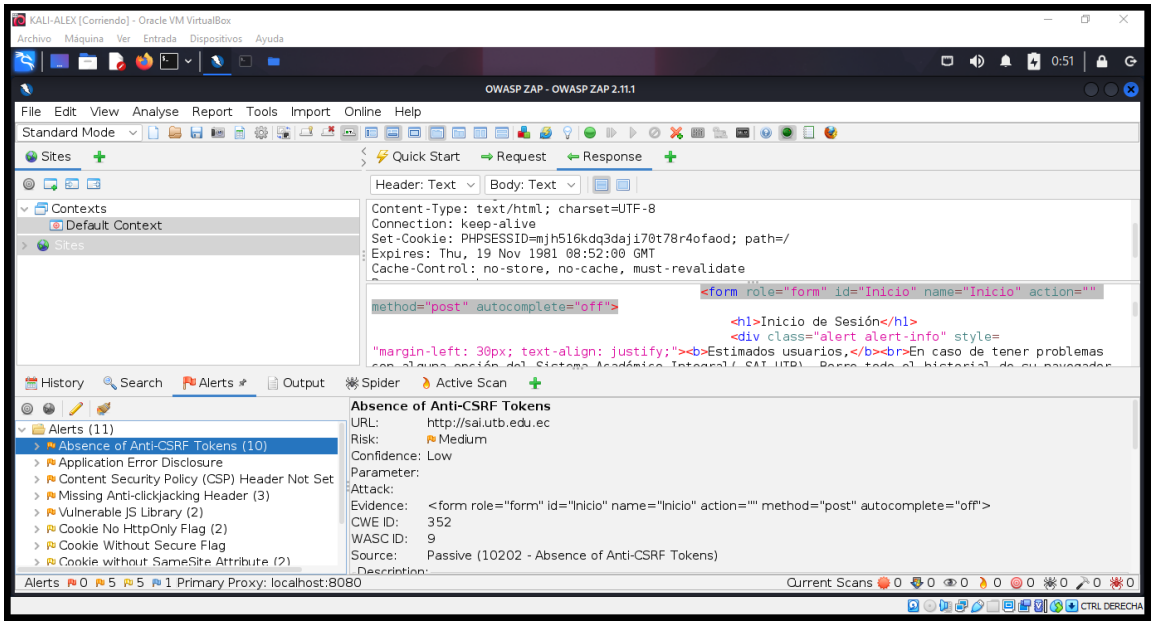


Ilustración 5 Amenazas encontradas con su reporte individual. Fuente: Palma (2022)

1% - 25%	Falta de encabezado antisecuestro de click	Engañar a los usuarios en algún falso botón o vinculo.	ANEXO 17	Gestión de incidentes en la seguridad de la información, Detectar amenazas y recuperar información.
	Bandera de Cookie No HttpOnly			
	Ausencia de tokens anti-CSRF	Permite obligar a un usuario a realizar acciones en contra de su voluntad.	ANEXO 9	Controles de accesos de usuarios, Estricto control de autenticación de usuarios.
25% - 50%	Divulgación de información - Comentarios sospechosos	Un usuario no autenticado podría acceder a una cuenta y realizar actos indebidos.	ANEXO 16	Gestión de los incidentes que ocurren con la seguridad de la información, gestionar la seguridad de la información y comunicar algún tipo de amenaza.
50% - 100%	Divulgación de error de aplicación	Un atacante envía scripts maliciosos a un servidor y este los ejecuta.		
	Encabezado de política de seguridad de contenido (CSP) no establecido			
	Biblioteca JS vulnerable	Falta parche de seguridad por lo que el sitio es fácil de abusar, envían falsas solicitudes a un servidor	ANEXO 12	Protección contra códigos maliciosos, Proteger el sistema de cualquier ataque de malware o algún ataque de ingeniería social.

Tabla 7Aplicación de anexos normas ISO

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

Babahoyo, 11 de agosto de 2022

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

En mi calidad de Tutor del Trabajo de la Investigación del Sr.: **Palma Vera Antonio Alexander**, cuyo tema es: PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA EL MODULO PRE UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO BASADO EN LA NORMA ISO 27001, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio, obteniendo como porcentaje de similitud de **[6%]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

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

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

ERICK MAGNO RICAURTE ZAMBRANO

Ing. Erick Ricaurte Zambrano, MSIG,MBA
DOCENTE DE LA FAFI.

Ilustración 6 Certificado de porcentaje de similitud con otras fuentes en el sistema de anti plagio. Palma (2022)

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

Babahoyo, 07 de julio de 2022
D-FAFI-UTB-0221-2022

Decano FAFI
Se Aprueba Proyecto Factible
20/07/2022.

Ingeniero
Marcos Oviedo Rodríguez, Ph.D.
RECTOR
UNIVERSIDAD TÉCNICA DE BABAHOYO.
En su Despacho. –

De mis consideraciones:

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

El Señor **PALMA VERA ANTONIO ALEXANDER,** con cédula de identidad No. 094081397-5, Estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo Abril 2022 – Septiembre 2022, trabajo de titulación modalidad Caso de Estudio, previo a la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS DE INFORMACIÓN,** solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar el Caso de Estudio en la institución de su digna Rectoría, el cual titula: **PLAN DE GESTIÓN DE RIESGOS DE LA SEGURIDAD INFORMÁTICA PARA EL MÓDULO PRE UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, BASADO EN LA NORMA ISO 27001.**

Del señor Rector,

Atentamente.

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA
DECANATO

RECIBIDO
UNIVERSIDAD TECNICA DE BABAHOYO
SECRETARIA FAFI
20/07/2022 FECHA: 16h37 HORA:

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO

C/c: Archivo

UNIVERSIDAD TECNICA DE BABAHOYO
SECRETARIA
FECHA 20/07/2022 HORA 10:51

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Mercedes Soto Valencia	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

19

Ilustración 7 Carta de autorización. Palma (2022)