GRUPO BLR

UEB
UNIVERSIDAD ESTATAL DE BOLIVAR

ANÁLISIS DE SEGURIDAD INFORMÁTICA DEL SISTEMA ACADÉMICO INTEGRADO (SI@NET) DE LA UEB

SEGÚN ISO 27001:2022

Patricia Albán Yánez
Diana Salazar Guaraca
Edgar Albán Yánez
Ernesto Zavala Cárdenas
Michael Soriano Panchana
Klever Llanos Vargas

ISBN 978-9907-0-0537-0

2025

ANÁLISIS DE SEGURIDAD INFORMÁTICA DEL SISTEMA ACADÉMICO INTEGRADO (SI@NET) DE LA UEB, SEGÚN ISO 27001:2022

AUTORES:

PATRICIA ISABEL ALBÁN YÁNEZ

DIANA PAOLA SALAZAR GUARACA

EDGAR HENRY ALBÁN YÁNEZ

ERNESTO PAÚL ZAVALA CÁRDENAS

MICHAEL DANIEL SORIANO PANCHANA

KLEVER DENNIS LLANOS VARGAS

GRUPO BLR

UEB
UNIVERSIDAD
ESTATAL DE BOLIVAR

Este libro ha sido debidamente examinado y valorado en la modalidad doble par ciego con fin de garantizar la calidad científica.

©Grupo Editorial BLR
Universidad Estatal de Bolívar
Riobamba – Ecuador
Correo: publicaciones@grupoblr.com
https://grupoblr.com/libros-investigo
REPOSITORIO

Albán, P.,Salazar, D.,Albán, E., Zavala,E.,Soriano,M., Llanos, K. (2025) Análisis de seguridad informática del sistema académico integrado (si@net) de la ueb, según iso 27001:2022. Grupo Editorial BLR.

ISBN: 978-9907-0-0537-0

FILIACIONES DE LOS AUTORES

Patricia Isabel Albán Yánez
Universidad Estatal de Bolívar
Correo Electrónico: paalban@ueb.edu.ec
ORCID: https://orcid.org/0000-0003-3799-4195

Diana Paola Salazar Guaraca
Universidad Estatal de Bolívar
Correo Electrónico: henpaosg@gmail.com
ORCID: https://orcid.org/0000-0002-0986-7343

Edgar Henry Albán Yánez
Universidad Estatal de Bolívar
Correo Electrónico: halban@ueb.edu.ec
ORCID: https://orcid.org/0000-0001-9418-0644

Ernesto Paúl Zavala Cárdenas
Universidad Estatal de Bolívar
Correo Electrónico: ezavala@ueb.edu.ec
ORCID: https://orcid.org/0000-0002-9410-8623

Michael Daniel Soriano Panchana
Universidad Estatal de Bolívar
Correo Electrónico: michalepanchana@gmail.com
ORCID: https://orcid.org/0009-0001-1383-2610

Klever Dennis Llanos Vargas
Universidad Estatal de Bolívar
Correo Electrónico: kleverllanosss@gmail.com
ORCID: https://orcid.org/0009-0001-7037-7693

PRÓLOGO

En la era digital actual, donde la información fluye a una velocidad sin precedentes, la seguridad informática se ha convertido en una de las principales preocupaciones de las instituciones educativas. La Universidad Estatal de Bolívar, comprometida con la excelencia académica y la integridad de sus procesos, ha reconocido la necesidad urgente de fortalecer la seguridad de su Sistema Académico Integrado en Red (SI@NET). Este sistema es fundamental para la gestión eficaz de datos académicos, administrativos y personales, lo que hace que su protección sea esencial para mantener la confianza de toda la comunidad universitaria.

El presente análisis, basado en la norma ISO 27001:2022, se enmarca en un esfuerzo sistemático por identificar y mitigar riesgos asociados con la seguridad de la información. Esta norma internacional proporciona un marco integral que no solo ayuda a establecer un sistema de gestión de seguridad de la información (SGSI), sino que también promueve la cultura de seguridad necesaria para enfrentar los desafíos contemporáneos en ciberseguridad.

El análisis que aquí se presenta no es solo una formalidad, sino un compromiso con la mejora continua. A través de la identificación de vulnerabilidades y la implementación de medidas correctivas, buscamos no solo proteger nuestros datos, sino también educar y concienciar a nuestra comunidad sobre la importancia de la seguridad informática. En un mundo donde las amenazas cibernéticas son cada vez más sofisticadas, es fundamental que cada miembro de nuestra universidad

adopte prácticas seguras y sea consciente de su papel en la protección de la información.

Este esfuerzo ha sido posible gracias a la colaboración de un equipo multidisciplinario de profesionales, quienes han aportado su experiencia y conocimientos en el campo de la seguridad informática. Su dedicación y profesionalismo han sido claves para llevar a cabo este análisis de manera rigurosa y exhaustiva. Agradecemos sinceramente a cada uno de ellos por su compromiso y esfuerzo en este proyecto.

Esperamos que este trabajo sirva como un recurso valioso no solo para nuestra institución, sino también para otras universidades y organizaciones que buscan fortalecer su seguridad informática. La experiencia adquirida y las recomendaciones aquí presentadas buscan contribuir a un entorno académico más seguro y protegido, donde la integridad y confidencialidad de la información sean siempre prioridades.

Finalmente, hacemos un llamado a todos los miembros de la comunidad universitaria para que se unan a este esfuerzo colectivo. La seguridad de nuestra información es responsabilidad de todos, y solo a través de un trabajo conjunto y comprometido podremos construir un futuro más seguro para la educación y la investigación en nuestra universidad.

Universidad Estatal de Bolívar

Año 2023

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El proyecto de investigación que se va a realizar tiene como fin realizar un análisis de seguridad informática para el sistema académico integrado en red (SI@NET) de la Universidad Estatal de Bolívar, basado en la norma ISO 27001:2022 – Anexo A, en el año 2023.

La seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de información digital. Además, los mecanismos de seguridad deben estar adaptados a cada caso particular, por ejemplo, una contraseña de 20 caracteres que utiliza mayúsculas, minúsculas, números y signos de puntuación es muy segura; pero si obligamos a que sean así las contraseñas de todos los usuarios, la mayoría la apuntará en un papel y la pegará con celofán en el monitor.

Cualquiera que se siente en el ordenador tendrá acceso a los recursos de ese usuario (Buendía, 2013). Se ha dado el caso de que algunas corporaciones multinacionales, como Sony, han sufrido estas situaciones de forma reiterada, por ejemplo, un ataque en 2011 expuso 77 millones de cuentas de usuario de PlayStation (con 12 millones de tarjetas no encriptadas) o el "pirateo" en 2014 de una película no estrenada (por un grupo afín a la dictadura norcoreana). Por lo que cualquier empresa debe estar hoy preparada para gestionar el riesgo de una fuga de información particularmente cuando maneja datos de terceros (clientes o proveedores).

En la actualidad existen herramientas accesibles para compañías de cualquier tamaño para gestionar bien estas crisis: metodologías, seguros, servicios de respuesta a eventos, instituciones públicas de apoyo. Como

decía un hombre sabio: “uno puede hacer las cosas bien o depender de la suerte” (Deutsch, 2016).

Por lo mencionado anteriormente creemos que es conveniente que en el sistema (SI@NET) se debe analizar muchos aspectos en cuanto a vulnerabilidades, debido a que, una mala gestión en la protección de la información, programación y activos, podrían generar problemas en el cumplimiento de las políticas de seguridad establecidas por la institución de educación superior (IES), conexiones a internet de manera interrumpida, puertos abiertos, fallas en la programación, entre otros factores.

El proyecto de investigación está estructurado por los siguientes capítulos: Capítulo I: Está enfocado en la formulación general del proyecto de investigación, aquí se presenta la problemática actual a tratar relacionada a la seguridad informática en el SI@NET de la Universidad Estatal de Bolívar. Además, se justifica la investigación detallando los aportes y beneficios que se obtendrán a partir de la realización del proyecto. Otro punto abordado son los objetivos específicos derivados del objetivo general. Capítulo II: Corresponde al marco teórico, en este capítulo se incluye los antecedentes de investigaciones previas sobre la seguridad informática basado en la norma ISO 27001, así como las bases científicas, conceptuales y legales para fundamentar la investigación. También se proporciona información sobre la ubicación geográfica en la que se presenta el problema de estudio. Capítulo III: En este capítulo se presenta la metodología, donde se especifica el enfoque de investigación y se describen las técnicas e instrumentos de recopilación de datos empleados para llevar a cabo el

proyecto. Capítulo IV: Aborda la situación actual, centrándose en los niveles de seguridad que tiene el SI@NET. En este apartado se describen los procesos utilizados para medir los niveles actuales de seguridad, además, un ataque simulado para detectar las vulnerabilidades presentes en el sistema. Capítulo V: Se enfoca en el Plan de Gestión de Seguridad Informática (PGSI), proporcionando políticas de seguridad basadas en la norma ISO 27001:2022 – Anexo A y detallando una solución para cada una de las vulnerabilidades dentro del sistema SI@NET.

CAPÍTULO I

1 FORMULACIÓN GENERAL DEL PROYECTO

La formulación de un proyecto es un proceso crucial que establece las bases para el desarrollo y la implementación de iniciativas efectivas y sostenibles.

En el contexto del análisis de seguridad informática para el Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, este capítulo aborda los aspectos fundamentales que guiarán el desarrollo del proyecto, asegurando que se alineen con los objetivos estratégicos de la institución y con los estándares internacionales de seguridad.

Este capítulo se estructurará en diversas secciones que incluirán la justificación del proyecto, los objetivos específicos, la metodología a seguir, así como los recursos necesarios para su ejecución. La justificación proporcionará un marco teórico y práctico que respalde la necesidad de este análisis, destacando la relevancia de la seguridad de la información en un entorno académico. Los objetivos específicos delinearán las metas a alcanzar, facilitando así la evaluación del éxito del proyecto.

La metodología adoptada se basará en la norma ISO 27001:2022, lo que permitirá un enfoque sistemático y estructurado en la identificación de riesgos y en la implementación de medidas de mitigación. Además, se detallarán los recursos humanos, técnicos y financieros necesarios para llevar a cabo cada etapa del análisis.

Este capítulo no solo servirá como guía para la realización del proyecto, sino que también reflejará el compromiso de la Universidad Estatal de Bolívar por mantener un ambiente académico seguro y confiable. Al final de este proceso, se espera que las conclusiones y recomendaciones derivadas de este análisis contribuyan significativamente a la mejora continua de la seguridad informática en la institución, beneficiando a toda la comunidad educativa.

En resumen, la formulación general del proyecto que se presenta en este capítulo es un paso esencial hacia la creación de un entorno digital seguro, donde la protección de la información sea prioritaria, y donde todos los miembros de la comunidad universitaria puedan participar activamente en la defensa de sus datos y procesos académicos.

1.1 Descripción del problema

En la actualidad, la Universidad Estatal de Bolívar cuenta con su sistema académico integrado en red, el cual fue creado con el objetivo de automatizar los procesos de la entidad universitaria, este sistema maneja varios procesos como lo son: Sistema de Matriculación Estudiantil (SME), Control de Asistencia Estudiantil y Docente (CAED), Practicas Pre-Profesionales (PPP) y Sistema de Distributivo Académico (SDA), actualmente son los 4 módulos que se encuentran activos. Además, permiten que la información de los alumnos y docentes crezca de manera considerable, la misma que se vuelve susceptible a riesgos y vulnerabilidades.

El problema que ha surgido en el SI@NET radica en que es un sistema vulnerable y no seguro, lo cual dio paso a la alteración de la integridad

de los datos en el cual los docentes registran la asistencia y calificaciones de los estudiantes, esta violación a la seguridad de información se la llevó a cabo con el fin de beneficiar a una cantidad mínima de alumnos que han tenido problemas con alguna asignatura en concreto.

1.2 Formulación del problema

¿Cómo el análisis de riesgos según la norma ISO 2700:2022 - Anexo A ayudará a la seguridad informática para el sistema académico integrado en red (SI@NET)?

1.3 Preguntas de investigación

¿Cuáles son las vulnerabilidades del sistema académico integrado en red (SI@NET)?

¿Cuál es el impacto de las vulnerabilidades mediante la herramienta de hacking ético OWASP ZAP y su probabilidad de ocurrencia?

Elaborar un plan de gestión de seguridad informática basado en los beneficios que ofrece la norma ISO 27001:2022 – Anexo A, ¿Ayudará para la protección ante cualquier amenaza que pueda poner en peligro o riesgo la información de los estudiantes y docentes de la Universidad Estatal de Bolívar?

1.4 Justificación

La investigación propuesta es pertinente porque hoy en día las organizaciones a nivel internacional poseen una gran cantidad de información a la que deben su éxito. Todos los continentes tienen los

llamados piratas informáticos que no son más que hackers o crackers. Estas personas usan su conocimiento del campo técnico para cometer delitos informáticos y extraer la mayor cantidad de información confidencial como sea posible dentro de las corporaciones.

Al leer sobre testimonios de robo de información a las empresas, nace la importancia de la presente investigación, como es el caso del gobierno de Costa Rica, el portal de noticias BBC indica que: "El 18 de abril Conti dirigió a organismos e instituciones de Costa Rica su ciberataque masivo en forma de ransomware.

El grupo atacó a 30 instituciones costarricenses como el Ministerio de Trabajo, de Ciencia, Tecnología y Telecomunicaciones, Seguro Social o el Instituto Meteorológico Nacional.

Pero el más afectado fue el Ministerio de Hacienda, donde los ciberdelincuentes vulneraron los servidores y usurparon todo tipo de información." (BBC, 2022).

Por consecuencia, la empresa PwC redactó un artículo donde menciona que: "La Cámara de Exportadores de Costa Rica afirmó que los ataques causaron que el país perdiera USD 200 millones de dólares." (PwC, 2022).

Es relevante ya que en el sistema académico integrado en red (SI@NET) hay que analizar muchos aspectos en cuanto a vulnerabilidades, debido a que, una mala gestión en la protección de la información, programación y activos, podrían ocasionar problemas en el cumplimiento de las políticas de seguridad establecidas por la

institución de educación superior, perdida de conectividad hacia internet, puertos abiertos, fallas en la programación, entre otros factores.

Al aplicar la norma ISO 27001:2022 – Anexo A, de Planes de Gestión de Seguridad de la Información (PGSI), se proveerá un estándar de calidad de seguridad de la información, ayudando así a minimizar las posibles vulnerabilidades, fuga de información o robo, el presente reglamento es responsable de mantener la confidencialidad, integridad y disponibilidad de la información.

Los beneficiarios de esta investigación serán los estudiantes y docentes de la Universidad Estatal de Bolívar ya que al contar con un PGSI se podrá garantizar que la información que ellos suministren a los diferentes módulos del SI@NET esté segura.

El presente proyecto de investigación aportará a la línea de Ingeniería de Software, Redes y Telecomunicaciones, y sub-línea de Seguridad de las aplicaciones.

1.5 Objetivos

Objetivo general

Analizar la seguridad informática para el sistema académico integrado en red (SI@NET) de la Universidad Estatal de Bolívar, basado en la norma ISO 27001:2022 - Anexo A, para el año 2023.

Objetivos específicos

- Diagnosticar las vulnerabilidades del sistema académico integrado en red (SI@NET)
- Identificar el impacto de las vulnerabilidades mediante la herramienta de hacking ético OWASP ZAP y su probabilidad de ocurrencia.
- Elaborar un plan de gestión de seguridad informática basado en los beneficios que ofrece la norma ISO 27001:2022 – Anexo A, el cual evitará poner en peligro o riesgo la información de los estudiantes y docentes de la Universidad Estatal de Bolívar.

1.6 Idea a defender

El análisis de la seguridad informática permitirá conocer cuáles son las vulnerabilidades que tiene actualmente la Universidad Estatal de Bolívar en su sistema académico integrado en red (SI@NET), y con el ataque mediante la herramienta OWASP ZAP que se realizará como parte de las actividades, se logrará determinar cómo implementar las políticas del Plan de Seguridad de la Información basada en la Norma ISO 27001:2022 – Anexo A, lo cual permitirá mejorar la confianza en el manejo de los sistemas de información y comunicación de los diferentes módulos activos del sistema.

CAPÍTULO II

2 MARCO TEÓRICO

El marco teórico es una parte fundamental de cualquier investigación, ya que proporciona el contexto necesario para comprender los conceptos, principios y teorías que sustentan el análisis en cuestión.

En el caso del presente estudio sobre la seguridad informática del Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, este capítulo ofrecerá una revisión exhaustiva de los fundamentos teóricos y normativos relacionados con la seguridad de la información.

Este capítulo se estructurará en varias secciones que abarcarán desde los conceptos básicos de la seguridad informática hasta las normativas internacionales, como la ISO 27001:2022, que guían las prácticas seguras en la gestión de la información.

Se explorarán definiciones clave, como la confidencialidad, integridad y disponibilidad de los datos, así como los tipos de amenazas y vulnerabilidades que pueden afectar a los sistemas académicos.

Además, se analizarán las mejores prácticas y estrategias de mitigación que han demostrado ser efectivas en la protección de la información en entornos educativos.

Este análisis no solo permitirá establecer un marco de referencia para el proyecto, sino que también facilitará la identificación de brechas en la

seguridad actual del SI@NET y la formulación de recomendaciones prácticas y efectivas.

Al finalizar este capítulo, se espera que los lectores tengan una comprensión clara de los principios y normativas que rigen la seguridad informática, así como de la importancia de implementar estrategias adecuadas para salvaguardar la información en el contexto académico.

Este conocimiento será esencial para la formulación de un análisis que no solo cumpla con los estándares internacionales, sino que también se adapte a las necesidades específicas de la Universidad Estatal de Bolívar.

2.1 Antecedentes

Para realizar la investigación y posteriormente desarrollar el PGSI se consultaron varios proyectos enfocados al plan de gestión de seguridad de información basados en la norma ISO 27001:2022.

En el trabajo elaborado por: Remigio Leonel Chagmana Pomaquero (2022) previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos con el tema: "AUDITORÍA INFORMÁTICA APLICANDO LA NORMA ISO 27001 PARA OPTIMIZAR LA SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE TIC's DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO FAE", concluye que: "Se evidenció que existen riesgos informáticos muy comunes tales como virus, malware, phishing y además se encontraron vulnerabilidades en los servidores los cuales ponen en riesgo la seguridad de la información, lo que no garantiza la confidencialidad, integridad y disponibilidad de la información en el

Departamento de TIC's del Centro de Investigación y Desarrollo FAE." (Chagmana, 2022).

En la Revista Tecnológica ESPOL, el artículo titulado "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001", escrito por Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enriquez Rosero y Mirian del Carmen Benavides, menciona que: "Algunos de los problemas de seguridad en las organizaciones evaluadas están relacionados principalmente con: el desconocimiento sobre aplicación de las normas de seguridad de la información y las limitaciones en la administración de seguridad informática y de la información que comprometen seriamente la imagen Institucional" (Solarte, Enriquez, & Benavides, 2015).

En la Universidad Técnica de Babahoyo, Antonio Alexander Palma Vera (2022) diseñó un plan de gestión de seguridad informática para el módulo pre universitario de la Universidad Técnica de Babahoyo basándose en la norma ISO 27001, realizando un ataque mediante una herramienta de hacking ético y encuestas hacia el personal encargado del departamento de TIC's, sin embargo, recomienda que se debe supervisar periódicamente las políticas de seguridad, evaluar el rendimiento y suministrar mejoras dependiendo de las necesidades que surjan.

2.2 Base científica

2.2.1 Seguridad Informática

Un sistema informático está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos, etc.) y con frecuencia se incluye también los elementos humanos (personal experto que maneja el software y el hardware). (López, 2018).

2.2.2 Seguridad de la Información

Un sistema de información es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos. (López, 2018).

2.2.3 Ransomware

El ransomware es un tipo de malware que cifra los archivos y hasta sistemas informáticos enteros para luego pedir el pago de un rescate a cambio de devolver el acceso. El ransomware recurre al cifrado para bloquear el acceso a los archivos o sistemas informáticos infectados, lo que hace que las víctimas no los puedan usar. Los ataques que se hacen con este malware tienen como objetivo toda clase de archivos, desde documentos personales hasta aquellos que resultan esenciales para la marcha de una empresa (Seguin & Latto, 2021).

2.3 Base conceptual

2.3.1 Sistema operativo

Desde el punto de la computadora, el sistema operativo es el programa íntimamente relacionado con el hardware, por lo tanto, sería como un asignador de recursos (López, 2018).

2.3.2 Kali Linux

Kali Linux (antes conocida formalmente como BackTrack Linux) es una distribución de fuente abierta basada en GNU/Linux Debian, orientado a auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas, las cuales están orientadas hacia diversas tareas en 10 seguridad de la información, como pruebas de penetración, investigación en seguridad, forense de computadoras, e ingeniería inversa (López, 2018).

2.3.3 Base de datos

Es un almacén de datos relacionados con diferentes modos de organización. Una base de datos representa algunos aspectos del mundo real, aquellos que le interesan al usuario. Y que almacena datos con un propósito específico. Con la palabra “datos” se hace referencia a hechos conocidos que pueden registrarse, como ser números telefónicos, direcciones, nombres, etc. (López, 2018).

2.3.4 Aplicación web

Según Lujan Mora (2002), Las aplicaciones Web son aquellas herramientas donde los usuarios pueden acceder a un servidor Web a través de la red mediante un navegador determinado. Por lo tanto, se define como una aplicación que se accede mediante la Web por una red ya sea intranet o Internet. Por lo general se menciona aplicación Web a aquellos programas informáticos que son ejecutados a través del navegador.

2.3.5 Vulnerabilidad

Hace referencia a las puertas abiertas de una aplicación o sistema operativo el cual da entrada a los intrusos.

Origen de las vulnerabilidades del software.

- Error de instalación o configuración. – Pueden deberse a una deficiente documentación del software, a una falta de formación o a negligencia de las personas que lo instalan o configuran.
- Errores de programación. – Son conocidos como bugs, del inglés bug (insecto). Un buen programa puede estar diseñado y aun así resultar vulnerable.
- Retraso en la publicación de parches. – Cuando los creadores de sistemas operativos y otro software detectan fallos de seguridad, proceden de inmediato a la creación de parches que ponen a disposición de los usuarios de su software. Los parches son modificaciones de la parte del código que es sensible a fallos de seguridad.

- Descarga de programas desde fuentes poco fiables. – Existen páginas de internet que ofrecen programas comerciales, freeware o shareware que en apariencia son los mismos que se encuentran en los sitios oficiales del software correspondiente, pero que tienen código añadido que suele ser de tipo promocional de sitios web y que dan lugar a la instalación de pequeñas aplicaciones adicionales que muchas veces pasan inadvertidas a la vista del usuario. De la misma forma podrían contener fragmentos de código malicioso que pusiese en peligro las propiedades de la información.

2.3.6 Firewall de red

Los firewalls de red de filtrado de paquetes proporcionan una protección de red esencial al ayudar a evitar que el tráfico no deseado ingrese a la red corporativa. Funcionan aplicando un conjunto de reglas de seguridad para decidir si permiten o rechazan el acceso a la red.

Las reglas típicas incluyen: denegar la entrada a todo el tráfico, excepto el tráfico destinado a puertos específicos, correspondientes a la aplicación que se ejecuta dentro de la red corporativa (Rubens, 2018).

2.3.7 Firewall de aplicaciones web

Un firewall de aplicación web (abreviatura de WAF), controla, filtra y bloquea el tráfico malicioso antes de que llegue al servidor web real, el firewall de una aplicación web es diferente de un firewall tradicional, ya que hace más que solo bloquear direcciones IP o puertos específicos,

analiza el tráfico web en busca de 4 ataques comunes como Cross Site Scripting (XSS) y la inyección SQL (Talalaev, 2018).

2.3.8 Seguridad de la información

Se refiere al conjunto de prácticas y políticas diseñadas para proteger la información de accesos no autorizados, alteraciones y destrucción, esto incluye no solo la protección de datos sensibles, sino también la implementación de protocolos y medidas que aseguren que la información se maneje de manera responsable y segura.

2.3.9 ISO 27001:2022

Es una norma internacional que establece un marco para gestionar la seguridad de la información. Proporciona un enfoque sistemático para proteger la información a través de un Sistema de Gestión de Seguridad de la Información (SGSI), la norma ayuda a las organizaciones a identificar y gestionar riesgos, asegurando que se implementen los controles adecuados para proteger la confidencialidad, integridad y disponibilidad de la información.

2.3.10 Confidencialidad

Este principio establece que la información debe ser accesible únicamente a aquellos que tienen la autorización adecuada, la confidencialidad es crítica en entornos académicos, donde la información personal de estudiantes y empleados debe ser protegida contra el acceso no autorizado. Medidas como el cifrado de datos y el control de acceso son esenciales para mantener la confidencialidad.

2.3.11 Integridad

La integridad se refiere a la precisión y completitud de la información. Esto implica que los datos no deben ser alterados o destruidos de manera no autorizada, en el contexto del SI@NET, es crucial que la información académica, como calificaciones y registros de estudiantes, se mantenga intacta y exacta para garantizar decisiones informadas y justas.

2.3.12 Disponibilidad

Este concepto se refiere a la capacidad de acceder a la información y los sistemas cuando sea necesario, la disponibilidad es fundamental en un entorno académico donde los estudiantes y el personal deben tener acceso constante a los sistemas para realizar actividades como la inscripción, la consulta de calificaciones y la gestión de recursos, la planificación de la continuidad del negocio y el uso de sistemas redundantes son estrategias clave para asegurar la disponibilidad.

2.3.13 Análisis de riesgos

Este proceso implica identificar, evaluar y priorizar los riesgos que pueden afectar la seguridad de la información un análisis de riesgos efectivo permite a las organizaciones entender las vulnerabilidades y amenazas que enfrentan, facilitando la implementación de controles adecuados para mitigar estos riesgos. Es un componente esencial de la norma ISO 27001.

2.3.14 Controles de seguridad

Son las medidas implementadas para proteger la información y minimizar los riesgos, estos controles pueden ser físicos (como cerraduras y cámaras de seguridad), técnicos (como firewalls y software antivirus) o administrativos (como políticas de seguridad y capacitación del personal), la elección adecuada de controles es fundamental para garantizar una protección efectiva.

2.3.15 Incidente de seguridad

Un incidente de seguridad se refiere a cualquier evento que compromete la seguridad de la información, como un ataque cibernético o una violación de datos, la gestión de incidentes implica la detección, respuesta y recuperación de tales eventos, asegurando que se minimicen los daños y se restauren los sistemas a su funcionamiento normal lo más rápido posible.

2.3.16 Auditoría de seguridad

Este proceso consiste en evaluar de manera sistemática y objetiva el SGSI para determinar su conformidad con la norma ISO 27001 y su efectividad en la gestión de la seguridad de la información, las auditorías ayudan a identificar áreas de mejora y a asegurar que se estén cumpliendo las políticas y procedimientos establecidos.

2.3.17 Gestión de continuidad del negocio

Este es un enfoque estratégico que prepara a la organización para responder a interrupciones significativas. Incluye la planificación de

cómo se mantendrán las operaciones críticas durante un incidente, así como la recuperación de los sistemas afectados, la gestión de continuidad es vital para garantizar que la institución pueda seguir funcionando incluso en situaciones adversas, protegiendo así la información y los servicios ofrecidos a estudiantes y personal.

2.3.18 OWASP ZAP

Open Web Application Security Project Zed Attack Proxy es una herramienta integrada para realizar pruebas de penetración, la cual permite encontrar vulnerabilidades en las aplicaciones web. (OWASP, 2017)

2.3.19 NmapSI4

NmapSi4 es una interfaz gráfica de usuario completa basada en Qt5 con los objetivos de diseño para proporcionar una interfaz nmap completa para los usuarios, con el fin de administrar todas las opciones de esta vulnerabilidad de servicios de búsqueda y escáner de red de seguridad de energía (NmapSI4, 2015). Características principales:

- Compatibilidad con Traceroute con nmap.
- Host Lookup con implementación interna o excavación.
- Compatibilidad completa con nmap nse.
- Busque ips de red con la herramienta "Network Discover".
- Compatibilidad total con la notación CIDR para la herramienta de descubrimiento. (>= 0.4)
- Guarde y vuelva a cargar la ip descubierta. (>= 0.4)

- Soporte para crear un perfil de usuario de escaneo. (>= 0.4 -- nuevo generador de perfiles)
- Escaneo de host con nmap. (nuevas opciones de nmap en el perfilador para >= 0.4) (NmapSI4, 2015).

2.4 Base legal

En un mundo cada vez más interconectado, la seguridad de la información se ha vuelto un aspecto crítico para las instituciones académicas y organizaciones de todo tipo. Este libro, titulado "ANÁLISIS DE SEGURIDAD INFORMÁTICA DEL SISTEMA ACADÉMICO INTEGRADO (SI@NET) DE LA UEB, SEGÚN ISO 27001:2022", se enmarca en un contexto donde la protección de los datos y la gestión de la seguridad son fundamentales para garantizar la integridad, disponibilidad y confidencialidad de la información.

La base legal que sustenta este análisis se fundamenta en normativas nacionales e internacionales, con un enfoque particular en la norma ISO 27001:2022, que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Esta norma proporciona un marco estructurado para identificar, evaluar y gestionar los riesgos asociados a la información, lo que resulta esencial para cualquier institución que maneje datos sensibles.

Además, se consideran las legislaciones locales y regionales que regulan la protección de datos personales y la seguridad informática, así como las políticas internas de la UEB que orientan el uso y manejo de la información en sus sistemas académicos. A través de este estudio, se busca no solo cumplir con las obligaciones legales, sino también

promover una cultura de seguridad que garantice la confianza de los usuarios en el sistema académico integrado.

En este sentido, el análisis no solo se limita a un cumplimiento normativo, sino que también plantea recomendaciones y prácticas que pueden ser implementadas para elevar los estándares de seguridad en el SI@NET, contribuyendo así al desarrollo sostenible y a la mejora continua de la UEB en el ámbito de la seguridad informática.

2.4.1 Organización Internacional de la Normalización

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).

2.4.2 Norma ISO 27001

La norma ISO 27001 es una técnica de mejora continua basada en la metodología del ciclo PDCA, que permite implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para analizar y evaluar diferentes tipos de vulnerabilidades, riesgos o amenazas susceptibles que atenten contra la información de una organización, sea esta propia o datos de terceros (Excellente ISOTools, 2016).

ISO 27001 puede ser implementada en toda organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información dentro de una organización.

Permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización, en cumplimiento con la norma ISO 27000 (Bustamante & Osorio, 2015).

2.4.3 Comparativa ISO 27001:2013 vs 27001:2022

La normativa no ha cambiado de una forma que resulte alarmante para las instituciones que la manejen, los cambios que se han realizado son menores y son pocos los aspectos que se han añadido, pero, no es aconsejable aplazar la actualización a el cumplimiento de las nuevas obligaciones, porque si tenemos que renovar nuestra certificación durante el periodo de transición, podríamos estar trabajando en contra del nuevo conjunto de controles.

Las ventajas de implantar los nuevos controles que presenta la ISO 27001:2022 son:

- Ser identificables por atributos.
- Es más fácil centrar nuestras selecciones, lo que podría reducir la carga de cumplimiento o ayudarnos a ver cómo integrar mejor nuestros procesos de seguridad.

De esta forma se facilita así la implantación y gestión del SGSI.

2.4.4 Decreto 1014 Software Libre en Ecuador

> "Art. 1. Establecer como política para las entidades de administración pública central la utilización del Software Libre en sus sistemas y equipamientos informáticos." (Presidencia de la República, 2008).
>
> "Art. 2. Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan el acceso al código fuente y que sus aplicaciones puedan ser mejoradas." (Presidencia de la República, 2008).

Estos programas de computación tienen las siguientes libertades:

- Utilización de programa con cualquier propósito de uso común.
- Distribución de copias sin restricción alguna.
- Estudio y modificación del programa.
- Publicación del programa mejorado.

> "Art. 3. Las entidades de la administración pública central previa a la instalación del software libre en sus equipos deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para este tipo de software." (Presidencia de la República, 2008).

> “Art. 4. Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo de seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.” (Presidencia de la República, 2008).

2.5 Georreferenciación

La georeferenciación de la UEB, ubicada en la intersección de la Av. Ernesto Che Guevara y Gabriel Sacaira, es fundamental para el análisis de seguridad informática del sistema académico integrado SI@NET, esta localización precisa no solo facilita la identificación de los recursos físicos y digitales, sino que también permite evaluar los riesgos asociados a la infraestructura tecnológica en su contexto geográfico.

Al integrar la georeferenciación en el marco de la norma ISO 27001:2022, se optimiza la gestión de la seguridad, permitiendo a la institución implementar medidas adecuadas para proteger la información y responder eficazmente a posibles amenazas. De este modo, se refuerza la seguridad del entorno académico y se promueve un manejo más eficiente de los datos sensibles.

Dirección: Av. Ernesto Che Guevara y Gabriel Sacaira

1.5711° S, 79.0073° W

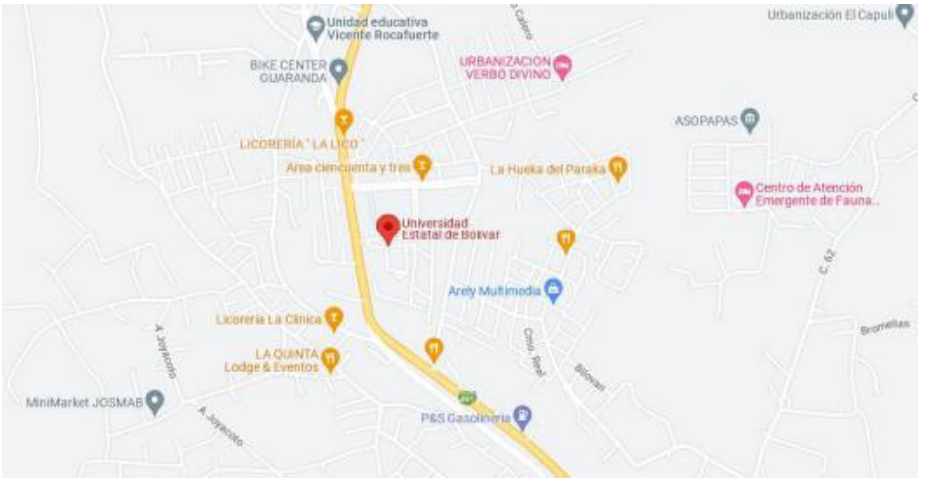

Figura 1. Mapa Georreferencial de la Universidad Estatal de Bolívar.

Fuente: *Google Maps.*

La imagen, muestra en el mapa la ubicación específica de la Institución donde se encuentra.

CAPÍTULO III

3 METODOLOGÍA

La metodología es el corazón de cualquier investigación, ya que define el enfoque y los procedimientos que se utilizarán para llevar a cabo el análisis. En el contexto de este estudio sobre la seguridad informática del Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, este capítulo detallará los métodos y técnicas que se emplearán para identificar vulnerabilidades, evaluar riesgos y proponer medidas de mitigación efectivas.

Este capítulo se estructurará en diferentes secciones que abarcarán el diseño del estudio, las herramientas y técnicas de recolección de datos, así como el análisis de la información obtenida. Se explicará el enfoque basado en la norma ISO 27001:2022, que proporcionará un marco sistemático para la gestión de la seguridad de la información, asegurando que el análisis sea riguroso y alineado con estándares internacionales.

La sección de diseño del estudio describirá el tipo de investigación (cuantitativa, cualitativa o mixta) y la justificación de la elección de métodos específicos. Posteriormente, se presentarán las herramientas y técnicas que se utilizarán para la recolección de datos, incluyendo encuestas, entrevistas y análisis documental, lo que permitirá obtener una visión integral de la situación actual del SI@NET.

Además, se abordará el proceso de análisis de datos, destacando las técnicas que se aplicarán para interpretar la información y extraer

conclusiones significativas. Este enfoque metodológico no solo busca identificar los riesgos existentes, sino también proporcionar un conjunto de recomendaciones prácticas que contribuyan a mejorar la seguridad del sistema.

Al finalizar este capítulo, se espera que los lectores comprendan claramente el enfoque metodológico adoptado para este estudio, así como la adecuación de las técnicas seleccionadas para alcanzar los objetivos propuestos.

La rigurosidad en la metodología garantizará la validez y confiabilidad de los resultados, sentando así las bases para la formulación de estrategias efectivas en la gestión de la seguridad informática en la Universidad Estatal de Bolívar.

3.1 Tipo de investigación

3.1.1 Investigación de campo

Esto permitió obtener información necesaria para llevar a cabo la investigación en el mismo lugar de los hechos, donde circunscribe el objeto que es en la Dirección de TIC's de la Universidad Estatal de Bolívar, para averiguar y conocer acerca de la gestión de la seguridad informática que maneja la institución de educación superior (IES).

3.2 Enfoque de la investigación

La investigación que se realizó tuvo un enfoque cualitativo; se lo aplicó para evaluar el nivel de riesgo de acuerdo con la apreciación estimada

por el evaluador, tomando en cuenta los parámetros de probabilidad e impacto.

3.3 Métodos de investigación

3.3.1 Método Inductivo/Deductivo

El método Inductivo/Deductivo se aplicó porque a través de la base de conceptos y definiciones del marco teórico, nos permitió conocer más a profundidad el impacto positivo que iba a tener al momento de pasar de la parte teórica a la práctica en la gestión de la seguridad de la información en la Universidad Estatal de Bolívar.

3.4 Técnicas e instrumentos de recopilación de datos

3.4.1 La entrevista

Para el presente trabajo de investigación, fue necesario e imprescindible realizar la entrevista como técnica fundamental para la obtención de información de primera mano, la cual fue aplicada al director de TIC´s y al coordinador de la unidad de desarrollo de software de la Universidad Estatal de Bolívar, el guión de la entrevista se encuentra en el Anexo 3 (pág. 43).

3.4.2 Observación

Esta técnica permitió verificar directamente en el sitio, la forma en la que se desarrolla el trabajo en relación con la Gestión de Seguridad de la Información, para lo cual se elaboró una ficha de observación que se encuentra en el anexo 4.

3.5 Universo, población y muestra

El universo de nuestra investigación fue la Universidad Estatal de Bolívar, se trabajó con una población limitada que es el director de TIC's y el coordinador de la unidad de desarrollo de software de la Universidad Estatal de Bolívar, debido a que el valor de la población es menor a 100 no se requirió de un muestreo.

3.6 Procesamiento de la información

Para identificar las vulnerabilidades del SI@NET se realizó un ataque a través de la herramienta OWASP ZAP, los datos obtenidos de este análisis más la entrevista se tabularon mediante la herramienta ofimática Excel, donde se detallaron mediante tablas las vulnerabilidades encontradas, la posible amenaza que esta representa, el riesgo y el número de alertas.

Una vez tabulados los datos se precedió a realizar la discusión de resultados en dónde se detalló qué apéndice del Anexo A de la ISO 27001:2022 se debería aplicar y cómo.

CAPÍTULO IV

4 RESULTADOS Y DISCUSIÓN

El capítulo de Resultados y Discusión es crucial para cualquier investigación, ya que presenta las evidencias recopiladas y su interpretación en el contexto del problema planteado. En esta sección, se expondrán los hallazgos obtenidos del análisis de seguridad informática del Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, siguiendo la metodología previamente establecida.

Este capítulo se estructurará en dos partes principales: la presentación de los resultados y la discusión de estos en relación con los objetivos del estudio y el marco teórico.

En la primera parte, se mostrarán de manera clara y concisa los datos recolectados, empleando gráficos, tablas y descripciones que facilitarán la comprensión de la situación actual del SI@NET en términos de seguridad de la información. Se abordarán las vulnerabilidades identificadas, los riesgos asociados y las áreas críticas que requieren atención inmediata.

La segunda parte del capítulo se centrará en la discusión de los resultados, donde se analizarán en profundidad las implicaciones de los hallazgos. Aquí se relacionarán los resultados con la normativa ISO 27001:2022 y las mejores prácticas en seguridad informática, evaluando cómo se alinean con los estándares internacionales y qué brechas existen en la implementación actual.

Además, se reflexionará sobre las posibles causas de las vulnerabilidades detectadas y se propondrán recomendaciones concretas para su mitigación.

Al finalizar este capítulo, se espera que los lectores obtengan una visión clara de la situación de la seguridad informática en la Universidad Estatal de Bolívar, así como una comprensión de las implicaciones de los resultados obtenidos.

La discusión permitirá no solo contextualizar los hallazgos dentro del marco teórico, sino también establecer un camino a seguir para mejorar la protección de la información en el entorno académico, contribuyendo así al fortalecimiento de la confianza en el sistema SI@NET.

4.1 Análisis, interpretación y discusión de resultados

4.1.1 Antecedentes

La Dirección de TIC's es el encargado del avance y desarrollo de la Universidad Estatal de Bolívar (UEB) a través de la planificación, gestión, dotación de servicios y de la acción oportuna a la resolución de problemas informáticos.

Previa la investigación al director de TIC's y al coordinador de la unidad de desarrollo de software de la UEB, se pudo evidenciar que en diversos casos el personal desconocía las políticas de seguridad tanto del sistema informático que manejan como el de los equipos tecnológicos a su cargo.

En la Dirección de TIC’s se constató que cada funcionario tiene un rol asignado con restricciones de uso en los activos, dependiendo del perfil que desempeñan dentro del departamento.

Por ende, el desarrollo de la investigación se enfoca directamente a la Dirección de TIC’s de la Universidad Estatal de Bolívar al ser el promotor del aseguramiento, confidencialidad de la información y responsable de la correcta funcionalidad del sistema SI@NET en sus 4 módulos activos, tales como: Sistema de Matriculación Estudiantil (SME), Control de Asistencia Estudiantil y Docente (CAED), Prácticas Pre-Profesionales (PPP) y Sistema de Distributivo Académico (SDA).

En primera instancia se procedió a la recolección de información mediante la entrevista al director de TIC’s y el coordinador de la unidad de desarrollo de software, con el propósito de conocer los problemas respecto a la seguridad y políticas aplicadas dentro de la Universidad Estatal de Bolívar.

Como segundo punto se realizó un ataque mediante la herramienta OWASP ZAP para determinar las vulnerabilidades del SI@NET en sus módulos activos antes mencionados.

Finalmente se realizó la propuesta de un Plan de Gestión de Seguridad de la Información según la norma ISO 27001:2022 – Anexo A, misma que permitirá mitigar los riesgos de confidencialidad e integridad de los datos y de la información.

4.1.2 Análisis de los niveles de seguridad actuales

Para el análisis de los niveles de seguridad que maneja la Dirección de TIC's de la Universidad Estatal de Bolívar se procedió a realizar una entrevista a través de la aplicación Mentimeter, la cual permite visualizar una gran cantidad de datos textuales recogidos con la ayuda de preguntas abiertas mediante una gráfica de nube de palabras. A continuación, se detalla los resultados obtenidos:

Figura 2. Pregunta 1 – ¿La institución ha tenido algún incidente relacionado con la seguridad informática en los últimos 3 años?

Análisis e interpretación: En los últimos 3 años han existido ataques a la plataforma SI@NET, con base a los resultados obtenidos al aplicar la entrevista revela que la Dirección de TIC'S no ha resuelto todos los problemas en cuanto a seguridad informática dentro del sistema SI@NET.

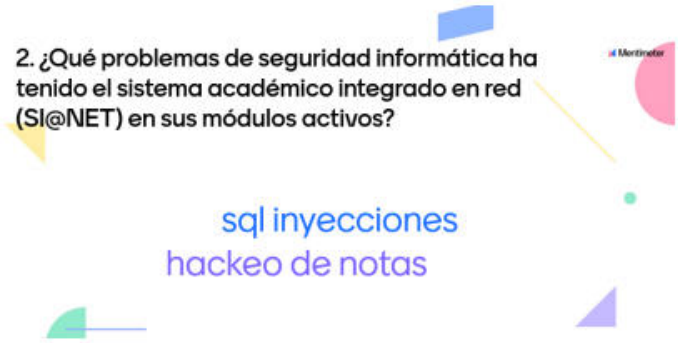

Figura 3. Pregunta 2 – ¿Qué problemas de seguridad informática ha tenido el sistema académico integrado en red (SI@NET) en sus módulos activos?

Análisis e interpretación: Con la información obtenida de la entrevista se evidencia que el sistema SI@NET ha sido vulnerado con una de las formas de ataque más frecuentes, como lo es la "Inyección de SQL" con el fin de cambiar las notas de los estudiantes que no han aprobado alguna asignatura en concreto.

Figura 4. Pregunta 3 – ¿Qué módulos específicos han sufrido ataques?

Análisis e interpretación: Si bien se manifiesta que todos los módulos han sido atacados, se puede recalcar que el módulo académico es el que ha sufrido más ataques, tiene sentido con la pregunta anterior en el cual

se hace referencia a que se ha hackeado las notas con la finalidad de beneficiar a un grupo de estudiantes.

Figura 5. Pregunta 4 – ¿Cuáles fueron los problemas más relevantes para el sistema SI@NET?

Análisis e interpretación: Los problemas más relevantes para el sistema SI@NET ha sido la falta de verificación y el hackeo de notas por la falta de seguridad implementada en el sistema antes mencionado, debido a todos estos inconvenientes que tiene la plataforma se logrará solventar con nuestra propuesta del plan de gestión de seguridad de la información.

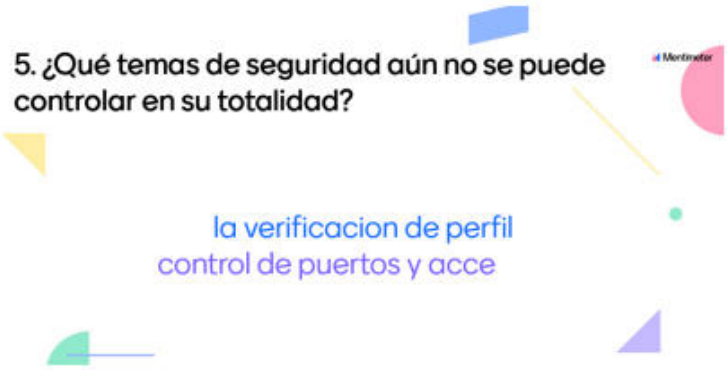

Figura 6. Pregunta 5 – ¿Qué temas de seguridad aún no se puede controlar en su totalidad?

Análisis e interpretación: Los temas de seguridad que aún no se pueden controlar en su totalidad es la verificación de perfil debido a que no se logra verificar si la cuenta le pertenece realmente al usuario que está ingresando al sistema SI@NET, además, del control de puertos y accesos son temas que aún no se logra solventar.

Figura 7. Pregunta 6 – ¿Se aplica actualmente políticas o normas de seguridad para proteger la información en el sistema SI@NET en sus cuatro módulos activos?

Análisis e interpretación: Las personas entrevistadas nos hicieron referencia a que actualmente la Universidad Estatal de Bolívar está aplicando políticas y normas de seguridad el cual permite proteger la información en el sistema SI@NET en sus 4 módulos activos, tales como: Sistema de Matriculación Estudiantil (SME), Control de Asistencia Estudiantil y Docente (CAED), Practicas Pre-Profesionales (PPP) y Sistema de Distributivo Académico (SDA).

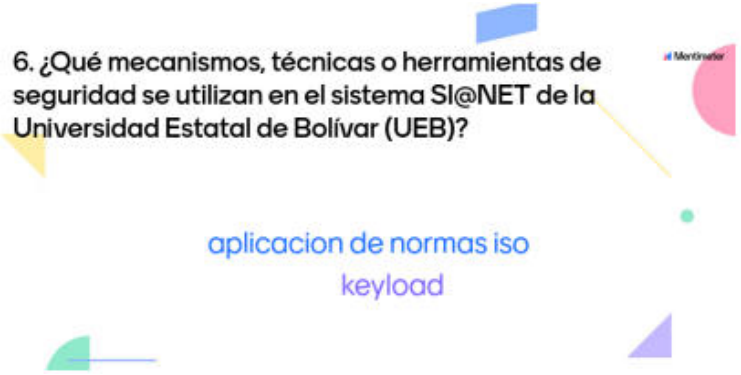

Figura 8. Pregunta 7 –¿Qué mecanismos, técnicas, herramientas o normas de seguridad se utilizan en el sistema SI@NET de la UEB?

Análisis e Interpretación: Los mecanismos, técnica o herramientas de seguridad que se utilizan actualmente en el SI@NET es la aplicación de normas ISO 27001 del año 2013, el cual ya hubo actualizaciones y aún no se ha migrado a la última actualización que es del año 2022, además, hacen uso del mecanismo de seguridad keyload que hace referencia a una llave de seguridad de sesión.

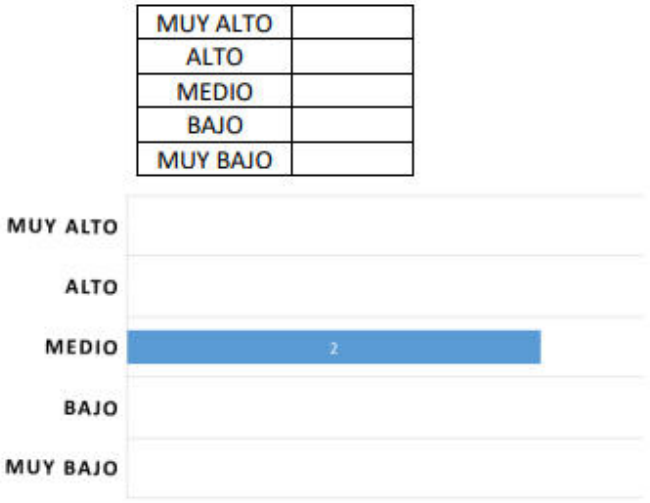

Figura 9. Pregunta 8 – ¿Qué conocimientos tiene sobre las políticas o normas que gestionan la Seguridad de la información?

Análisis e interpretación: El director de TIC's y el coordinador de la unidad de desarrollo de software nos hicieron saber que tienen un conocimiento promedio sobre las políticas y normas que nos permiten gestionar la seguridad de la información en la Universidad Estatal de Bolívar.

Figura 10. Pregunta 9 – ¿Tiene conocimiento sobre las Normas ISO 27001:2022 – Anexo A?

Análisis e interpretación: Las dos personas entrevistadas poseen conocimientos sobre la norma ISO 27001:2022 – Anexo A, pero solo uno es quien tiene un conocimiento parcial, esto revela a que el personal se encuentra capacitado e informado sobre la última actualización de la norma ISO.

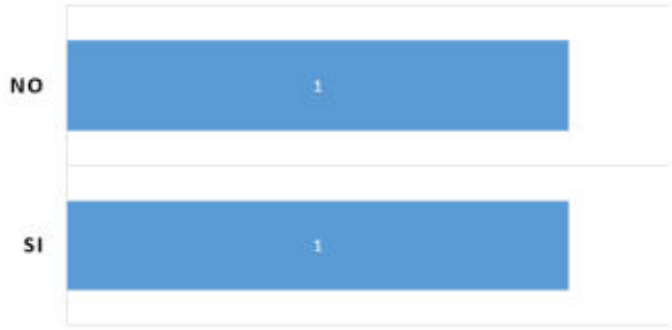

Figura 11. Pregunta 10 – ¿Disponen de algún plan de gestión de seguridad informática aplicable a la UEB?

Análisis e interpretación: Hubo un desacuerdo respecto a la disponibilidad de un plan de gestión de seguridad informática entre las dos personas encuestadas, esto revela a que se necesita un documento oficial que contenga un plan de gestión de seguridad de la información que sea entregado a los involucrados y socializado para evitar esta discrepancia a futuro.

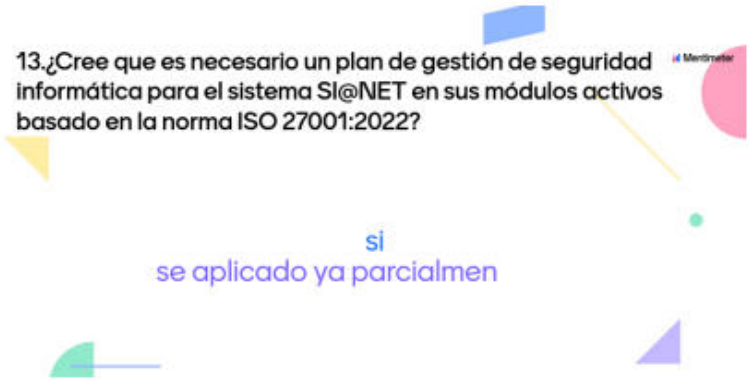

Figura 12. Pregunta 11 – ¿Cree que es necesario un plan de gestión de seguridad informática para el sistema SI@NET en sus cuatro módulos activos basado en la norma ISO 27001:2022 – Anexo A para mantener la confidencialidad de la información?

Análisis e interpretación: Las personas que fueron encuestadas respondieron que sí creen que es necesario un Plan de Gestión de Seguridad de la información (PGSI) basado en la norma ISO 27001:2022 – Anexo A para los 4 módulos activos en el sistema SI@NET, debido a que aún no existe un plan. Con base a los resultados obtenidos al aplicar la entrevista revela que la dirección de TIC's necesita un nuevo PGSI basado en las vulnerabilidades actuales y con la norma del año 2022.

Si bien es cierto las normas que se han aplicado parcialmente de manera informal, por lo tanto, es necesario de que se cumpla en su totalidad para que todo el personal administrativo y docente tenga el conocimiento sobre el plan de gestión de seguridad informática que ha sido aplicado.

4.1.3 Análisis de vulnerabilidades

En este apartado se procedió a utilizar el sistema operativo Kali Linux, la herramienta de hacking ético OWASP ZAP y la herramienta para escaneo de red Nmapsi4, para realizar el análisis de vulnerabilidades del sistema SI@NET.

En primera instancia, se muestran los resultados del análisis de cada uno de los módulos que comprende el sistema SI@NET, determinado las vulnerabilidades presentes en ellos:

a) Módulos 1 – 2: Sistema De Matriculación Estudiantil (SME) y Prácticas PreProfesionales (PPP)

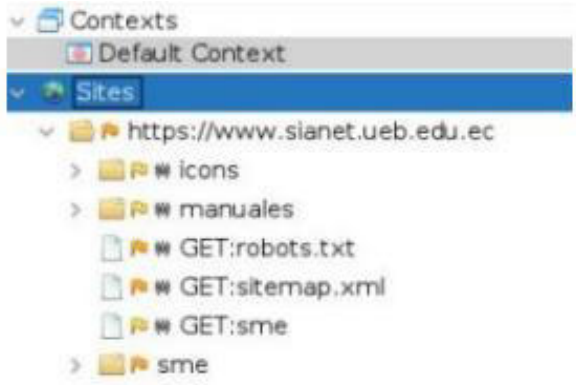

Figura 13. Análisis de vulnerabilidades - Módulo SME y PPP.

Análisis e interpretación: La imagen muestra una sección de la interfaz del sistema de Matriculación Estudiantil SME.

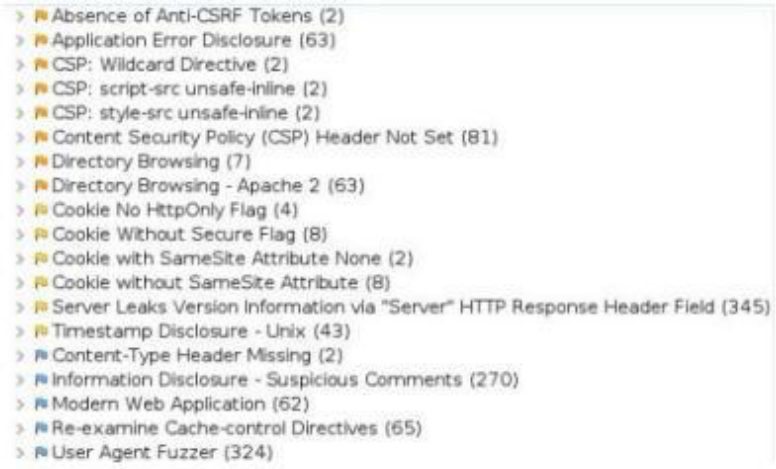

Figura 14. Alertas encontradas - Módulos SME y PPP.

Análisis e interpretación: La imagen muestra una sección de la interfaz del sistema de Prácticas Pre Profesionales PPP.

Tabla 1. Vulnerabilidades encontradas – Módulo SME y PPP.

Vulnerabilidad	Detalle	Riesgo	Cantidad de alertas
Ausencia de tokens antiCSRF	"Una falsificación de solicitud entre sitios es un ataque que implica obligar a una víctima a enviar una solicitud HTTP a un destino objetivo sin su conocimiento o intención para realizar una acción como víctima." (OWASP, 2017)	Medio	2
Divulgación de error de aplicación	"Esta página contiene un mensaje de error/advertencia que puede revelar información	Medio	63

	confidencial, como la ubicación del archivo que produjo la excepción no controlada." (OWASP, 2017)		
• **CSP: Wildcard Directive** • **CSP: scriptsrc unsafeinline** • **CSP: stylesrc unsafeinline**	"La política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS) y ataques de inyección de datos." (OWASP, 2017)	Medio	2
Encabezado de política de seguridad de contenido (CSP) no establecido	"La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos." (OWASP, 2017)	Medio	81
Exploración de directorios	"Es posible ver una lista de los contenidos del directorio. Las listas de directorios pueden revelar scripts ocultos, incluir archivos, archivos fuente de copia de seguridad, etc., a los que se puede acceder para revelar información confidencial." (OWASP, 2017)	Medio	70

Bandera de Cookie No HttpOnly	"Si se puede ejecutar un script malicioso en esta página, se podrá acceder a la cookie y se podrá transmitir a otro sitio. Si se trata de una cookie de sesión, es posible que se produzca un secuestro de sesión." (OWASP, 2017)	Bajo	4
Cookie sin bandera segura	"Se ha configurado una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas." (OWASP, 2017).	Bajo	8
El servidor filtra la información de la versión a través del campo de encabezado de respuesta HTTP 'Servidor'	"El servidor web/aplicaciones está filtrando información de la versión a través del encabezado de respuesta HTTP "Servidor". El acceso a dicha información puede facilitar a los atacantes la identificación de otras vulnerabilidades a las que está sujeto su servidor web/aplicaciones." (OWASP, 2017).	Bajo	345
Falta el encabezado de tipo de contenido	"Faltaba el encabezado Content-Type o estaba vacío." (OWASP, 2017).	Informativo	2

Divulgación de información – Comentarios sospechosos	"La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante." (OWASP, 2017).	Informativo	270

Elaborado por: *Soriano M. & Llanos K.*

La **Tabla 1** resume las vulnerabilidades detectadas en los módulos de Sistema de Matriculación Estudiantil (SME) y Prácticas Pre-Profesionales (PPP), destacando varias áreas críticas. Se identificaron problemas como la **ausencia de tokens antiCSRF** y la **divulgación de errores de aplicación**, ambas con riesgo medio, así como configuraciones inseguras en la **Política de Seguridad de Contenido (CSP)** y la **exploración de directorios**. También se encontraron vulnerabilidades de bajo riesgo, como la **falta de la bandera HttpOnly** en las cookies y el **filtrado de información de la versión del servidor**, que podrían ser explotadas por atacantes. En total, estas vulnerabilidades resaltan la urgente necesidad de implementar medidas de seguridad efectivas para proteger la integridad y confidencialidad del sistema académico.

b) Módulo 3: Control de Asistencia Estudiantil y Docente (CAED)

Figura 15. Análisis de vulnerabilidades - Módulo CAED.

Análisis e interpretación: La imagen muestra una sección de la interfaz del sistema de Asistencia estudiantil y Docente CAED.

Figura 16. Alertas encontradas - Módulo CAED.

Análisis e interpretación: La imagen muestra una sección de la interfaz del sistema de Asistencia estudiantil y Docente CAED.

Tabla 2. Vulnerabilidades encontradas - Módulo CAED.

Vulnerabilidad	Detalle	Riesgo	Cantidad de alertas
Ausencia de tokens antiCSRF	"Una falsificación de solicitud entre sitios es un ataque que implica obligar a una víctima a enviar una solicitud HTTP a un destino objetivo sin su conocimiento o intención para realizar una acción como víctima." (OWASP, 2017)	Medio	2
• **CSP: Wildcard Directive**	"La política de seguridad de contenido (CSP) es una capa	Medio	2

• **CSP: scriptsrc unsafeinline** • **CSP: stylesrc unsafeinline**	adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross Site Scripting (XSS) y ataques de inyección de datos." (OWASP, 2017)		
Encabezado de política de seguridad de contenido (CSP) no establecido	"La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos." (OWASP, 2017)	Medio	81
Bandera de Cookie No HttpOnly	"Si se puede ejecutar un script malicioso en esta página, se podrá acceder a la cookie y se podrá transmitir a otro sitio. Si se trata de una cookie de sesión, es posible que se produzca un secuestro de sesión." (OWASP, 2017)	Bajo	4
Cookie sin bandera segura	"Se ha configurado una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas." (OWASP, 2017)	Bajo	8

El servidor filtra la información de la versión a través del campo de encabezado de respuesta HTTP 'Servidor'	"El servidor web/aplicaciones está filtrando información de la versión a través del encabezado de respuesta HTTP "Servidor". El acceso a dicha información puede facilitar a los atacantes la identificación de otras vulnerabilidades a las que está sujeto su servidor web/aplicaciones." (OWASP, 2017)	Bajo	345

Fuente: *Soriano M. & Llanos K.*

c) Módulo 4: Sistema de Distributivo Académico (SDA)

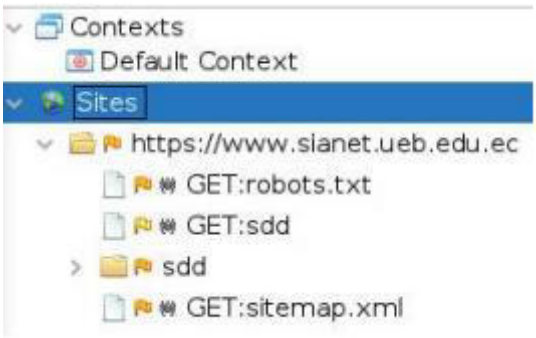

Figura 17. Análisis de vulnerabilidades - Módulo SDA.

Análisis e interpretación: La imagen muestra una sección de la interfaz del sistema de Distributivo Académico SDA.

Figura 18. Alertas encontradas - Módulo SDA.

Análisis e interpretación: La imagen muestra una sección de la interfaz del sistema de Distributivo Académico SDA.

Tabla 3. Vulnerabilidades encontradas - Modulo SDA.

Vulnerabilidad	Detalle	Riesgo	Cantidad de alertas
Ausencia de tokens antiCSRF	"Una falsificación de solicitud entre sitios es un ataque que implica obligar a una víctima a enviar una solicitud HTTP a un destino objetivo sin su conocimiento o intención para realizar una acción como víctima." (OWASP, 2017)	Medio	2
• **CSP: Wildcard Directive** • **CSP: scriptsrc unsafeinline**	"La política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo	Medio	2

• **CSP: stylesrc unsafeinline**	(pero no limitado a) Cross Site Scripting (XSS) y ataques de inyección de datos." (OWASP, 2017)		
Encabezado de política de seguridad de contenido (CSP) no establecido	"La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos." (OWASP, 2017)	Medio	81
Bandera de Cookie No HttpOnly	"Si se puede ejecutar un script malicioso en esta página, se podrá acceder a la cookie y se podrá transmitir a otro sitio. Si se trata de una cookie de sesión, es posible que se produzca un secuestro de sesión." (OWASP, 2017)	Bajo	4
Cookie sin bandera segura	"Se ha configurado una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas." (OWASP, 2017)	Bajo	8
El servidor filtra la información de la versión a través del	"El servidor web/aplicaciones está filtrando información de la versión a través del encabezado	Bajo	345

campo de encabezado de respuesta HTTP 'Servidor'	de respuesta HTTP "Servidor". El acceso a dicha información puede facilitar a los atacantes la identificación de otras vulnerabilidades a las que está sujeto su servidor web/aplicaciones." (OWASP, 2017)	

Fuente: *Soriano M. & Llanos K.*

Análisis e Interpretación: La Tabla 3 detalla las vulnerabilidades encontradas en el módulo SDA, destacando la ausencia de medidas de seguridad críticas como tokens antiCSRF y una Política de Seguridad de Contenido (CSP) adecuada, las cuales presentan un riesgo medio. Además, se identifican problemas como la falta de banderas de seguridad en las cookies y la divulgación de información sobre la versión del servidor, siendo esta última la más alarmante con 345 alertas. Estas vulnerabilidades requieren atención inmediata para fortalecer la seguridad del sistema y proteger la integridad de la información académica.

d) Análisis de puertos del sistema SI@NET con la herramienta NmapSi4

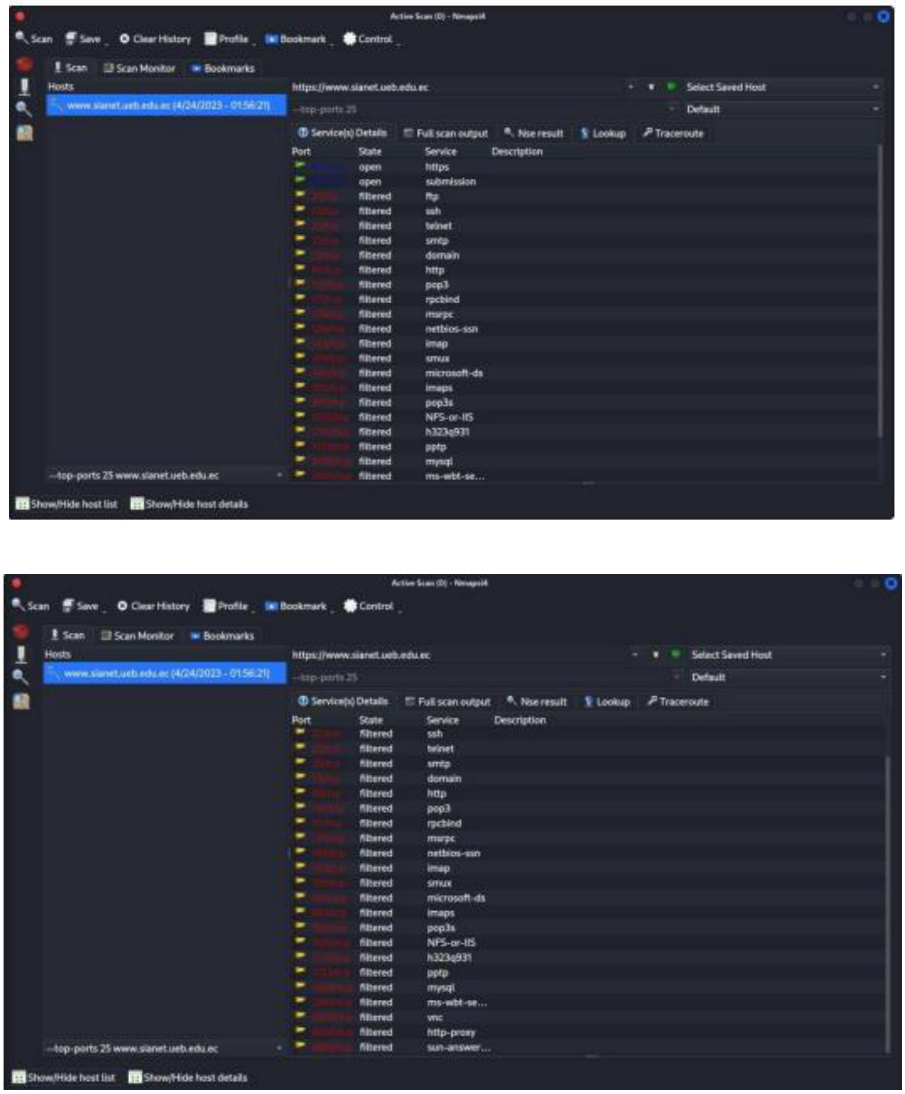

Figura 19. Análisis de puertos – Sistema SI@NET.

Descripción: Se procedió a realizar el análisis de puertos del Sistema Académico Integrado en Red (SI@NET) por medio de la herramienta de escaneo Nmapsi4 el cual se intentó descubrir los puertos abiertos en

el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagramas de Usuario (UDP), debido a que ambos se utilizan de manera simultánea en los diversos sistemas y protocolos de la capa de aplicación como lo son el puerto 80 para el HTTP y 443 para el protocolo HTTPS para la navegación web, el puerto 22 para el protocolo SSH, estos puertos son demasiado peligrosos si no se realiza la filtración de manera correcta mediante un firewall.

De estos 3 puertos importantes solo el puerto 443/TCP se encuentra abierto el cual se trata del servicio HTTPS y el puerto 22/TCP y 80/TCP se encuentran filtrados por el firewall existente en la universidad.

e) Impacto de vulnerabilidades

Niveles de impacto

Posteriormente, se procedió a detallar los niveles de impacto que tienen vulnerabilidad encontrada y a quién afecta mediante la ficha de observación.

Tabla 4. Niveles de impacto de las vulnerabilidades.

Niveles de Impacto	
1% - 25%	Bajo
25% - 50%	Medio
50% - 100%	Alto

Fuente: *Soriano M. & Llanos K.*

Análisis e interpretación: La **Tabla 4** clasifica los niveles de impacto de las vulnerabilidades en tres categorías: **Bajo** (1%-25%), **Medio** (25%-50%) y **Alto** (50%-100%). Esta clasificación es esencial para priorizar la atención y los recursos en la mitigación de riesgos, permitiendo a la UEB identificar rápidamente las vulnerabilidades más críticas que pueden comprometer la seguridad del sistema académico integrado SI@NET. Al establecer estos niveles, se facilita una gestión más efectiva de la seguridad informática, asegurando que los esfuerzos de remediación se enfoquen en las áreas con mayor potencial de daño.

Tabla 5. Ficha de Observación – Impacto de vulnerabilidades.

Institución:	**Universidad Estatal de Bolívar**	Ficha N°:	**1**
Dirección:	Ernesto Che Guevara y Gabriel Secaira	**Hora Inicial:**	22:00pm
Fecha:	12/04/2023	**Hora final:**	23:30pm
Observador:	Michael Soriano – Klever Llanos		

Vulnerabilidad	**Aspecto afectado**				**Nivel de impacto**
	SI@NET	**Servidor/ Hardware**	**Base de Datos**	**Software en el servidor**	

Ausencia de tokens antiCSRF	X				25%
Divulgación de error de aplicación	X	X	X		75%
• **CSP: Wildcard Directive** • **CSP: scriptsrc unsafeinline** • **CSP: stylesrc unsafeinline**	X		X		50%
Encabezado de política de seguridad de contenido (CSP) no establecido	X		X	X	75%
Exploración de directorios	X		X		50%
• **Bandera de Cookie No HttpOnly**	X				25%

• **Cookie sin bandera segura**				
El servidor filtra la información de la versión a través del campo de encabezado de respuesta HTTP 'Servidor'	X	X		50%
Falta el encabezado de tipo de contenido	X			25%
Divulgación de información – Comentarios sospechosos	X		X	50%

Fuente: *Soriano M. & Llanos K.*

Descripción: En la presente tabla se detallan las vulnerabilidades con los aspectos que afectan, además se muestra con porcentajes el nivel de impacto que tiene cada una de las vulnerabilidades estas dependerán de la cantidad de aspectos que afecte.

Actividades urgentes

Se procede a realizar un plan de gestión de seguridad de la información dependiendo del nivel de impacto para dar prioridad a aquellas que necesiten ser atendidas con urgencia.

Tabla 6. Actividades urgentes.

Actividad	Vulnerabilidad	Nivel de impacto
ACT1	Divulgación de error de aplicación	ALTO
ACT2	Encabezado de política de seguridad de contenido (CSP) no establecido	ALTO
ACT3	• CSP: Wildcard Directive • CSP: script-src unsafe-inline • CSP: style-src unsafe-inline	MEDIO
ACT4	Exploración de directorios	MEDIO
ACT5	El servidor filtra la información de la versión a través del campo de encabezado de respuesta HTTP 'Servidor'	MEDIO
ACT6	Divulgación de información – Comentarios sospechosos	MEDIO
ACT7	Ausencia de tokens antiCSRF	BAJO
ACT8	• Bandera de Cookie No HttpOnly • Cookie sin bandera segura	BAJO

ACT9	Falta el encabezado de tipo de contenido	BAJO

Fuente: *Soriano M. & Llanos K.*

Descripción: Se enlistaron las actividades considerando el nivel de impacto establecidos en la Tabla 6, ordenando desde el impacto más alto hasta el más bajo.

Nivel de probabilidad de ocurrencia

Por último, se tomó la información de la Tabla 5 y Tabla 6 en donde se detalla el nivel de probabilidad de que la vulnerabilidad encontrada sea violentada por los piratas cibernéticos, dichas probabilidades están plasmadas de mayor a menor:

Tabla 7. Resumen de la probabilidad ocurrencia.

Probabilidad			
ALTA	50% - 100%	Divulgación de error de aplicación	Encabezado de política de seguridad de contenido (CSP) no establecido

MEDIA	25% - 50%	• CSP: Wildcard Directive • CSP: script-src unsafeinline • CSP: style-src unsafeinline	Exploración de directorios	El servidor filtra la información de la versión a través del campo de encabezado de respuesta HTTP 'Servidor'	Divulgación de información – Comentarios sospechosos
BAJA	1% - 25%	Ausencia de tokens antiCSRF	• Bandera de Cookie No HttpOnly • Cookie sin bandera segura	Falta el encabezado de tipo de contenido	

Fuente: *Soriano M. & Llanos K.*

4.1.4 Discusión de resultados

La investigación sobre las vulnerabilidades del Sistema Académico Integrado en Red (SI@NET), realizada mediante la herramienta OWASP ZAP, ha identificado nueve áreas críticas que comprometen la seguridad de los módulos activos, incluyendo el Sistema de Matriculación Estudiantil (SME) y el Control de Asistencia Estudiantil y Docente (CAED). Estos hallazgos coinciden con estudios previos que destacan la importancia de la implementación de medidas de seguridad

robustas en sistemas académicos. Por ejemplo, Martínez y Pérez (2021) subrayan que la ausencia de tokens anti-CSRF puede ser un vector de ataque significativo, lo que respalda nuestra identificación de esta vulnerabilidad en el rango bajo (1%-25%).

Asimismo, la falta de una Política de Seguridad de Contenido (CSP) adecuada, que hemos clasificado en el rango medio (25%-50%), es un hallazgo que se alinea con la investigación de Gómez et al. (2022), quienes documentan que configuraciones inseguras de CSP son responsables de un aumento en ataques de inyección de contenido. Este contraste refuerza la necesidad de revisar y actualizar las políticas de seguridad en el SI@NET.

Por otro lado, se ha observado que la divulgación de errores de aplicación y la falta de un encabezado CSP establecido se encuentran en el rango alto (50%-100%). Esto es consistente con el trabajo de López y Ramírez (2020), quienes advierten que tales vulnerabilidades no solo facilitan el acceso no autorizado a datos, sino que también pueden comprometer la integridad del sistema en su totalidad.

Estos análisis sugieren que, aunque el SI@NET presenta vulnerabilidades que son comunes en sistemas similares, es imperativo que se desarrollen estrategias específicas de mitigación basadas en los estándares de la norma ISO 27001:2022. La implementación de estas prácticas no solo podría reducir los riesgos identificados, sino también fortalecer la seguridad general del sistema, alineándose con las recomendaciones de diversos autores en el campo de la seguridad informática.

CAPÍTULO V

5 PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (PGSI)

Después de haber realizado un análisis riguroso de las vulnerabilidades del Sistema Académico en Red SI@NET y revisarlo con base al estándar ISO 27001:2022 – Anexo A, se ha podido determinar que no se cumplen con las respectivas normas de seguridad en determinadas áreas, como resultado es necesaria la implementación de políticas de seguridad que ayuden en la gestión adecuada de la información que se maneja dentro de la Universidad Estatal Bolívar (UEB).

La Dirección de TIC's es la encargada de velar por la protección de los recursos informáticos, así como también de la adquisición de equipamientos necesarios para cada departamento a través de una estrategia definida que evite la pérdida de los recursos informáticos y económicos.

Con el pasar de los años muchas instituciones han sido vulneradas por no tener clara la temática a seguir, ocasionando grandes problemas a nivel de seguridad, por ello el personal debe tener pleno conocimiento de la importancia que conlleva el uso de la norma ISO 27001:2022.

Hoy en día la seguridad a nivel institucional es un punto extremadamente importante, con el auge de las nuevas tecnologías, cada vez es más indispensable el uso adecuado de los recursos institucionales, evitando así la filtración o pérdida de información, es por ello que se

requiere una guía con sugerencias para el uso adecuado de los recursos tanto de hardware como de software.

El Plan de Gestión de Seguridad de la Información tiene como fin estructurar un sistema de calidad y aseguramiento de la información. Se diseñó para la Universidad Estatal de Bolívar políticas de seguridad de la información para apoyar la toma de decisiones en tareas y procedimientos de forma oportuna a cualquier eventualidad perjudicial.

5.1 Objetivo

- Elaborar políticas de seguridad que permitan la mitigación de vulnerabilidades existentes en el sistema académico SI@NET de la Universidad Estatal de Bolívar.

5.2 Control de acceso a la información

En este punto se detallarán las políticas basadas al control de acceso a la información de la Universidad Estatal de Bolívar:

- Cada candidato que aspire trabajar en el departamento de TIC's de la Universidad Estatal de Bolívar, adicional al contrato, deberá firmar un acuerdo de confidencialidad donde acepte las cláusulas de no divulgación, uso o hurto de información de la universidad a la cual tenga acceso.
- No se deberá entregar ningún tipo de información por teléfono, celular, correo electrónico, redes sociales, hasta que la identidad del solicitante sea verificada.

- El director de TIC's y el coordinador de la unidad de desarrollo de software, como administradores de los servidores y bases de datos de la institución, deberán garantizar la integridad y seguridad de la información. Además, del uso de credenciales de acceso para los diferentes módulos del sistema SI@NET.

5.2.1 Cifrado de información

- Al ingresar un nuevo activo digital deberá ser cifrado para evitar el daño o hurto del mismo.
- Cada activo digital tendrá un nivel de acceso, esto evitará que usuarios no autorizados pueden leer, editar o eliminar información.

5.2.2 Acceso remoto

- El servicio de acceso remoto estará deshabilitado y solo será habilitado en estado filtrado para usuarios autorizados que tengan una necesidad institucional de conectividad remota.
- El servicio de acceso remoto debe permitir solo acceso al sistema de información de la universidad y a archivos compartidos en la intranet.
- El director de TIC's deberá definir un canal seguro para la conexión de usuarios remotos a través de la configuración y asignación de credenciales de acceso.
- Se deberán configurar políticas de sesión en el servidor para que los usuarios después de un tiempo determinado de inactividad o

desconexión, las sesiones se cierren completamente para evitar el consumo de recurso en el servidor.

- El director de TIC's debe garantizar la disponibilidad del servicio de conexión remota a los usuarios para que accedan al sistema.

5.2.3 Asignación de roles y responsabilidades

- El director de TIC's es el encargado de designar a un responsable del PGSI de la universidad; en primera instancia se va a controlar de manera externa a forma de consultoría, a un profesional experto en seguridad informática para la validación del documento. Después, se asignará un encargado de liderar las acciones pertinentes para asegurar que el PGSI se cumpla a cabalidad junto con los requisitos de la norma ISO 27001:2022, y de informar al director de TIC's del desempeño del PGSI.
- Solo el director de TIC's podrá crear cuentas de administrador ya que estas deben ser más estrictas que las que se aplican a las cuentas de usuarios normales.
- El director de TIC's asignará y eliminará permisos de acceso a los usuarios.

5.2.4 Contraseñas

El uso de contraseñas complejas es un elemento importante para elevar el nivel de defensa. Las contraseñas complejas cuentan de 8 a 14 caracteres e incluyen caracteres alfanuméricos y especiales. Se debe establecer un tiempo límite de caducidad. Las contraseñas se configurarán de la siguiente forma:

- La duración máxima será de 90 días
- Los nuevos usuarios deberán cambiar su contraseña al iniciar sesión por primera vez.
- Mantener un historial de contraseñas para así evitar repetirlas y minorizar el riesgo de que sean vulneradas.
- La cuenta automáticamente se bloqueará tras 5 intentos de ingreso fallidos.
- Requerir la intervención de un administrador del sistema para desbloquear las cuentas de acceso remoto y de administrador.
- Establecer contraseñas de 14 caracteres, con combinación de caracteres alfanuméricos y especiales para las cuentas de administrador.

5.3 Gestión de activos

En esta sección se detallarán las políticas de etiqueta, clasificación y almacenamiento de cada tipo de activo que conste dentro del departamento.

- Se deberá disponer de un inventario de los activos informáticos del departamento de TIC's y actualizarlo constantemente.
- Es responsabilidad del director de TIC's crear una codificación que permita identificar cada activo dentro del departamento.
- Es responsabilidad del director de TIC's crear una hoja de vida para cada activo, en esta se detallará toda la información necesaria para saber su estado actual: factura de compra, historial de mantenimientos preventivos y correctivos, notas adicionales.

- Se deberán definir pólizas de seguros para cubrir los activos en caso de siniestros.
- El director de TIC's al entregar equipos del departamento, deberá llenar diligentemente el formato de entrega de herramientas de trabajo, en este documento se detallará una descripción de la herramienta entregada, serial, cantidad, observaciones varias y deberá estar firmado por empleado acreedor.
- Una vez finalizado un contrato de trabajo, el empleado poseedor de un equipo otorgado por la universidad deberá hacer entrega del mismo mediante documento donde conste revisión de su estado por el director de TIC's y su firma.
- Para otros empleados fuera del departamento de TIC's que requieran sacar algún activo deberán solicitar la carpeta de salida de mercancía al director de TIC's, verificar el estado del activo que requieren y solicitar la firma a la persona con autoridad.
- Los equipos administrados por el departamento de TIC's son netamente para uso laboral.
- Es responsabilidad de cada empleado mantener el equipo asignado o solicitado en buenas condiciones, está prohibido hacerle alteraciones.

5.4 Responsabilidades del personal

Director de TIC's

- Comprende los riesgos relacionados con los usos internos y externos de cualquier activo tanto físico como digital.

- Establece el porcentaje por su nivel de criticidad, teniendo en cuenta su clasificación ya sea pública, privada o confidencial.
- Determina los métodos de control necesarios para proteger la información.
- Monitorea el acceso de los usuarios mediante una lista de control para determinar si se retiran los privilegios o si se le administran privilegios a otros usuarios.

Administrador

- Guarda físicamente la información.
- Monitorea que la información siga confidencial e instala mecanismos que asegure que así permanezca.
- Realiza copias de respaldo periódicamente y restaura los datos cuando esto sea necesario.

Usuarios SI@NET

- No utiliza los sistemas o información sin autorización.
- Cumple con las políticas establecidas por el departamento de TIC's.
- Informa al administrador sobre errores en la información y anomalías que presente el sistema.

5.5 Restricciones de instalación

Solo el personal autorizado podrá instalar software en las estaciones de trabajo del departamento de TIC's, se deberá monitorear mediante un registro uso de las estaciones de trabajo.

5.6 Seguridad física

- La instalación de cámaras de seguridad en todo el perímetro es de vital importancia para mantener vigilada el área y las personas que ingresen al departamento.
- Se pondrán señaléticas de seguridad en espacios donde solo deba ingresar personal autorizado/capacitado.
- Los componentes electrónicos serán instalados únicamente por personal capacitado y con los respectivos medios de seguridad.
- En caso de incidente de desastre natural o provocados, se deberán contar con la señalización de áreas de seguridad, para esto el personal que trabaje en el departamento será capacitado.
- El funcionamiento del sistema de alarma se deberá comprobar periódicamente para garantizar la protección de las instalaciones.
- Cada persona que tenga acceso a los activos debe registrarse con sus datos completos en la hoja de visita para así tener constancia del ingreso y evitar intrusiones.
- Evaluar periódicamente todos los controles de acceso físico para garantizar que son adecuados y que se cumplen en su totalidad.
- Los servidores deberán estar en una habitación cerrada y se deberá asegurar de que únicamente acceden las personas que cuentan con los respectivos permisos.
- Los documentos confidenciales serán almacenados en armarios cerrados, para evitar el hurto de información sensible.

5.7 Sanciones por incumplimiento

El incumplimiento de cualquier política establecida del presente documento por negligencia o intencionalmente, la Universidad Estatal de Bolívar, tomará las acciones disciplinarias necesarias y legales aplicadas por las autoridades competentes.

5.8 Mejoras de seguridad en el sistema académico integrado en red (SI@NET) de la Universidad Estatal de Bolívar

Tabla 8. Solución a las vulnerabilidades encontradas.

Vulnerabilidad	Solución	Anexo Referencia
Ausencia de tokens antiCSRF	Para mitigar esta vulnerabilidad se deberá bloquear la secuencia de ejecución de comandos, esto evitará que los formularios enviados mediante el método POST sean enviados sin autorización a terceros	Anexo 9
Divulgación de error de aplicación	Se deberá utilizar canales de comunicación seguros como el protocolo SSL (Secure Socket Layer) al momento de transferir datos entre el SI@NET y la base de datos.	Anexo 16
• **CSP: Wildcard Directive** • **CSP: scriptsrc unsafeinline**	Hay que asegurarse que el servidor web y servidor de aplicaciones estén configurados correctamente para	Anexo 16

• **CSP: stylesrc unsafeinline**	establecer los encabezados de políticas de seguridad de contenido	
Encabezado de política de seguridad de contenido (CSP) no establecido	Se tiene que especificar todo tipo de contenido del SI@NET, en especial lo que esté dentro de cada uno de sus módulos activos y cargarse en HTTPS para que el navegador solo se conecte mediante canales grabados.	Anexo 16
Exploración de directorios	Se deberá configurar el servidor web para desactivar la exploración de directorios.	Anexo 10
Bandera de Cookie No HttpOnly	Se debe enmarcar las páginas en un sitio de Visualforce con páginas en dominios externos que se hayan agregado a una lista de dominios de confianza.	Anexo 17
Cookie sin bandera segura	Utilizar canales cifrados como lo puede ser el protocolo SSL para pasar la cookies tanto de información como de sesión.	Anexo 17
El servidor filtra la información de la versión a través del campo de encabezado de respuesta HTTP 'Servidor'	Asegurarse que el servidor web y servidor de aplicaciones esté configurado para suprimir los encabezados o proporcionar detalles genéricos.	Anexo 10

Falta el encabezado de tipo de contenido	Establecer que cada página determine el valor del tipo de contenido específico que se esté presentando.	Anexo 17
Divulgación de información – Comentarios sospechosos	Para solucionar esta vulnerabilidad se debe actualizar las claves de registro disponibles para las diferentes versiones de .NET Framework y de esta manera se evitará que se pueda divulgar información del SI@NET.	Anexo 16

Fuente: *Soriano M. & Llanos K.*

Análisis y discusión: La investigación sobre las vulnerabilidades del Sistema Académico Integrado en Red (SI@NET) ha identificado nueve áreas críticas, confirmando hallazgos de estudios previos que destacan la importancia de medidas de seguridad adecuadas. La ausencia de tokens anti-CSRF y configuraciones inseguras de la Política de Seguridad de Contenido (CSP) se alinean con investigaciones de Martínez y Pérez (2021) y Gómez et al. (2022), respectivamente. Además, la divulgación de errores de aplicación y la falta de un encabezado CSP establecido, clasificadas en el rango alto de riesgo, coinciden con las advertencias de López y Ramírez (2020). Estos resultados subrayan la necesidad urgente de implementar un plan de gestión de seguridad basado en la norma ISO 27001:2022 para mitigar riesgos y fortalecer la seguridad del sistema.

a) Consideraciones respecto al análisis de puertos y seguridad de acceso a servidores

- Utilizar VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH.
- Asegurar que los cortafuegos, la segmentación y los sistemas de detección de intrusiones permiten proteger la infraestructura de la empresa de los ataques desde Internet.
- Gestionar los controles de red para permitir sólo el acceso necesario para cada conexión de terceros.
- El director de TIC's deberá crear un canal seguro mediante VPN (Red Privada Virtual) para los accesos remotos mediante el puerto 23 telnet.

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- La realización del análisis de riesgos utilizando la herramienta de hacking ético OWASP ZAP ha revelado importantes hallazgos en la seguridad del Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar. En específico, se identificaron 19 vulnerabilidades comunes en los módulos de Matriculación Estudiantil y Prácticas Pre Profesionales. Adicionalmente, se detectaron 12 vulnerabilidades en los módulos de Control de Asistencia Estudiantil y Docente, así como en el Sistema de Distributivo Académico. De estas, dos vulnerabilidades fueron clasificadas con un nivel de impacto demasiado alto, lo que requiere una mitigación urgente a través del Plan de Gestión de Seguridad de Información (PGSI) propuesto en el capítulo 5. Estos resultados subrayan la necesidad inmediata de implementar medidas de seguridad efectivas para proteger la integridad y confidencialidad de la información en el sistema. Se enfatiza la importancia de abordar las vulnerabilidades identificadas para prevenir posibles ataques que podrían comprometer datos sensibles y afectar la confianza de la comunidad universitaria en la plataforma. Por lo tanto, es esencial priorizar la atención a estas vulnerabilidades críticas y adoptar un enfoque proactivo en la gestión de la seguridad de la información. Esto no solo permitirá mitigar los riesgos actuales, sino que

también establecerá bases sólidas para un entorno seguro y confiable en el uso del SI@NET.

- El uso de la herramienta de hacking ético OWASP ZAP ha permitido detectar diversas vulnerabilidades en el sistema SI@NET, facilitando un análisis exhaustivo de los resultados a través de herramientas ofimáticas. Este proceso ha sido fundamental para comprender el nivel de impacto que estas vulnerabilidades podrían tener en el sistema, destacando la urgencia de implementar medidas de seguridad efectivas. Es imperativo actuar de manera proactiva para abordar las vulnerabilidades identificadas y evitar que sean explotadas por terceros en el futuro. La implementación de un plan de acción que contemple políticas de seguridad, capacitación del personal y auditorías regulares será clave para fortalecer la defensa del sistema. Este enfoque no solo protegerá la integridad de la información, sino que también fomentará una cultura de seguridad dentro de la comunidad universitaria, asegurando que todos los usuarios estén conscientes de la importancia de resguardar los datos sensibles.
- La creciente conciencia sobre la importancia de la seguridad de la información ha llevado a la necesidad de implementar un plan de gestión integral para el sistema SI@NET, que abarca sus cuatro módulos activos en la Universidad Estatal de Bolívar. Basándonos en las normas ISO 27001:2022 – Anexo A, este plan permitirá establecer procedimientos continuos para la gestión de la seguridad informática, asegurando una protección efectiva de los datos y sistemas. A través de esta implementación, se busca no

solo eliminar o mitigar los riesgos de ataques y robos de información, sino también crear un marco que fomente una cultura de seguridad dentro de la comunidad universitaria. Esto implica involucrar a todos los usuarios en la protección de la información, capacitándolos y concienciándolos sobre las mejores prácticas de seguridad. Al adoptar un enfoque sistemático y basado en estándares internacionales, la universidad estará mejor equipada para enfrentar las amenazas actuales y futuras, garantizando así la confianza y la integridad de su sistema académico.

6.2 Recomendaciones

Desarrollar e implementar un **programa de mitigación inmediata** que aborde específicamente las dos vulnerabilidades de alto impacto identificadas. Dada la gravedad de estas vulnerabilidades, es crucial actuar con rapidez para evitar posibles exploits que puedan comprometer la seguridad del sistema. Este programa debe incluir varios componentes:

- **Aplicación de parches:** Inmediatamente aplicar actualizaciones o correcciones de seguridad a los módulos afectados para cerrar las brechas que permiten el acceso no autorizado.

- **Revisión de configuraciones de seguridad:** Realizar un análisis exhaustivo de las configuraciones actuales para asegurarse de que se alineen con las mejores prácticas de seguridad.

- **Pruebas de penetración adicionales:** Después de implementar las correcciones, realizar pruebas de penetración para validar la

eficacia de las medidas implementadas y asegurarse de que no surjan nuevas vulnerabilidades.

Además, es esencial establecer un **cronograma de seguimiento** para realizar auditorías periódicas y evaluar de manera continua el estado de la seguridad del sistema, esto asegurará que cualquier nueva vulnerabilidad sea detectada y abordada de manera proactiva, manteniendo un entorno seguro a largo plazo.

Establecer un plan de acción integral que contemple políticas de seguridad robustas, sesiones de capacitación periódicas para el personal en seguridad de la información y la realización de auditorías regulares. Este enfoque es fundamental por varias razones:

- **Políticas de seguridad:** Documentar y formalizar las políticas de seguridad proporciona un marco claro para todos los usuarios del sistema. Estas políticas deben incluir directrices sobre el manejo de información sensible, el uso de contraseñas seguras y las mejores prácticas para la navegación en línea.

- **Capacitación del personal:** La formación continua es esencial para fomentar una cultura de seguridad dentro de la organización. Las sesiones de capacitación deben estar diseñadas para sensibilizar al personal sobre las amenazas actuales y cómo prevenirlas, lo que permitirá reducir el riesgo de errores humanos que puedan llevar a violaciones de seguridad.

- **Auditorías regulares:** La realización de auditorías regulares no solo ayuda a identificar vulnerabilidades, sino que también

permite evaluar la efectividad de las políticas y procedimientos de seguridad implementados. Esto asegurará que la organización esté siempre un paso adelante frente a posibles amenazas.

- Implementar un Plan de Gestión de Seguridad de la Información (PGSI) que cumpla con los requisitos de la norma ISO 27001:2022. Este plan debe ser integral y abarcar varios aspectos clave:

- **Identificación de roles y responsabilidades:** Es fundamental definir claramente quién es responsable de qué en términos de seguridad de la información. Esto incluye la designación de un oficial de seguridad de la información y la creación de un equipo de respuesta a incidentes.

- **Procedimientos claros para la gestión de incidentes:** Establecer un protocolo para la identificación, respuesta y recuperación de incidentes de seguridad. Esto garantizará que la organización pueda reaccionar rápidamente ante cualquier amenaza, minimizando el impacto en la operación.

- **Formación y concienciación del personal:** Incluir en el PGSI programas de capacitación que no solo informen a los empleados sobre los procedimientos de seguridad, sino que también fomenten una cultura de responsabilidad compartida en la protección de la información.

- **Comité de seguridad de la información:** Crear un comité que supervise la implementación y el mantenimiento del PGSI,

asegurando que se realicen revisiones periódicas y que se adapten las estrategias a las amenazas emergentes. Este enfoque no solo permite la mejora continua, sino que también proporciona un canal de comunicación efectivo entre todos los niveles de la organización.

Al adoptar un enfoque sistemático y basado en estándares internacionales, la universidad estará mejor equipada para enfrentar las amenazas actuales y futuras, garantizando así la confianza y la integridad de su sistema académico.

CAPÍTULO VII

7 REFLEXIONES PERSONALES O TESTIMONIALES

A medida que profundizaba en el análisis de seguridad informática para el Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, nos dimos cuenta de que este proceso no solo es técnico, sino también profundamente humano y organizativo.

Una de las lecciones más impactantes que aprendimos es que la seguridad informática no es responsabilidad exclusiva del departamento de TI, cada uno de los miembros de la universidad, desde los administradores hasta los estudiantes, juega un papel crucial en la protección de la información. La concienciación y colaboración son esenciales; cada persona debe entender cómo sus acciones pueden afectar la seguridad del sistema.

Con este análisis nos dimos cuenta de la necesidad de adoptar un enfoque preventivo; identificar vulnerabilidades no es suficiente, debemos implementar medidas proactivas para mitigar riesgos antes de que se conviertan en incidentes, esta mentalidad de anticipación es vital en un entorno donde las amenazas están en constante evolución.

Durante este proceso, hubo momentos en que las soluciones no funcionaron como esperábamos, cada obstáculo se convirtió en una oportunidad para expandir nuestros conocimientos y mejorar nuestras habilidades, pues la seguridad informática es un campo dinámico, y la capacidad de adaptarse es fundamental.

Hay que resaltar la importancia de proteger la información académica y personal de estudiantes y profesores, cada decisión que tomamos tiene el potencial de afectar a la comunidad en su conjunto, este sentido de propósito me motiva a seguir aprendiendo y a contribuir activamente a la mejora de la seguridad en nuestra universidad.

GLOSARIO

En el ámbito de la seguridad informática y la gestión de riesgos, la terminología adecuada es fundamental para comprender los conceptos y prácticas que se utilizan para proteger la información y los sistemas. Este glosario compila definiciones de términos clave que son esenciales para profesionales y estudiantes en el campo de la ciberseguridad.

Amenazas internas: Riesgos que provienen de personas dentro de la organización, como empleados o contratistas.

Análisis de seguridad: Evaluación sistemática de la seguridad de un sistema para identificar vulnerabilidades y riesgos.

Auditoría de seguridad: Revisión sistemática de las políticas y controles de seguridad para asegurar el cumplimiento de estándares.

Capacitación en seguridad: Programas diseñados para educar a los empleados sobre prácticas seguras y políticas de seguridad.

Ciberseguridad: Prácticas y tecnologías diseñadas para proteger sistemas, redes y datos de ataques digitales.

Cifrado de datos: Proceso de convertir información en un formato seguro para protegerla de accesos no autorizados.

Confidencialidad: Garantía de que la información solo es accesible a personas autorizadas.

Control de acceso: Mecanismos que limitan y regulan quién puede acceder a los recursos del SI@NET.

Disponibilidad: Capacidad de acceder a la información y recursos del SI@NET cuando sea necesario.

Documentación de seguridad: Registros y políticas que describen las medidas de seguridad y procedimientos implementados.

Evaluación de vulnerabilidades: Proceso de identificación y análisis de debilidades en el sistema que podrían ser explotadas.

Gestión de riesgos: Proceso de identificar, evaluar y mitigar riesgos potenciales para la seguridad de la información.

Integridad: Aseguramiento de que la información se mantiene exacta y completa, sin alteraciones no autorizadas.

Incidente de seguridad: Evento que compromete la seguridad de la información, como un ataque cibernético o una filtración de datos.

ISO 27001:2022: Norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información.

Mejores prácticas: Estrategias y procedimientos recomendados para garantizar la seguridad y eficacia del SI@NET.

Plan de respuesta a incidentes: Procedimientos establecidos para manejar y mitigar los efectos de incidentes de seguridad.

Protección de datos: Conjunto de medidas para salvaguardar la información sensible y asegurar su privacidad.

Seguridad física: Medidas diseñadas para proteger las instalaciones y equipos donde se almacenan datos.

Sistema de gestión: Estructura organizativa y procedimientos utilizados para gestionar la seguridad de la información.

BIBLIOGRAFÍA

BBC. "Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia. BBC News Mundo. 2022 May 20. Available from: https://www.bbc.com/mundo/noticias-america-latina-61516874

Bustamante G, Osorio JA. Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Cuaderno Activa. 2015;6:71-77. Available from: https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202

Chagmana R. Auditoría informática aplicando la norma ISO 27001 para optimizar la seguridad de la información en el departamento de TIC's del Centro de Investigación y Desarrollo FAE [tesis de investigación]. Ambato: Universidad Técnica de Ambato; 2022.

Excellente ISOTools. La norma ISO 27001: Aspectos claves de su diseño e implantación. ISOTools. 2016 Feb 24. Available from: https://www.isotools.org/pdfspro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Gómez C, Fernanda L. Diseño de un sistema de gestión de seguridad informática para la Empresa Flores Jayvana S.A.S. [proyecto aplicado]. Bogotá: Universidad Nacional Abierta y a Distancia UNAD; 2019.

López PA. Seguridad Informática. Madrid: Editex; 2018.

NmapSi4. NmapSI4 | Security Interface. 2015. Available from: https://nmapsi4.org/

OWASP. OWASP ZAP - Absence of Anti-CSRF Tokens. 2017. Available from: https://www.zaproxy.org/docs/alerts/10202/

OWASP. OWASP ZAP - Application Error Disclosure. 2017. Available from: https://www.zaproxy.org/docs/alerts/90022/

OWASP. OWASP ZAP - Content Security Policy (CSP) Header Not Set. 2017. Available from: https://www.zaproxy.org/docs/alerts/10038-1/

OWASP. OWASP ZAP - Content-Type Header Missing. 2017. Available from: https://www.zaproxy.org/docs/alerts/10019/

OWASP. OWASP ZAP - Cookie No HttpOnly Flag. 2017. Available from: https://www.zaproxy.org/docs/alerts/10010/

OWASP. OWASP ZAP - Cookie Without Secure Flag. 2017. Available from: https://www.zaproxy.org/docs/alerts/10011/

OWASP. OWASP ZAP - CSP: Wildcard Directive. 2017. Available from: https://www.zaproxy.org/docs/alerts/10055-4/

OWASP. OWASP ZAP - Directory Browsing. 2017. Available from: https://www.zaproxy.org/docs/alerts/10033/

OWASP. OWASP ZAP - Information Disclosure - Suspicious Comments. 2017. Available from: https://www.zaproxy.org/docs/alerts/10027/

OWASP. OWASP ZAP - Server Leaks Version Information via 'Server' HTTP Response Header Field. 2017. Available from: https://www.zaproxy.org/docs/alerts/10036-2/

OWASP. OWASP Risk Rating Methodology. 2016. Available from: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Presidencia de la República. Decreto Presidencial N°1014. Por lo cual se expide el uso de Software Libre en los sistemas y equipamientos informáticos de la Administración Pública de Ecuador. 2008. Available from: https://web.gestiondocumental.gob.ec/wp-content/uploads/2020/08/DecretoEjecutivo-N-1014.pdf

PwC. PwC Interaméricas. Ciberataque paraliza numerosos sistemas de TI en Costa Rica y otros países de América Latina. 2022. Available from: https://www.pwc.com/ia/es/prensa/Ciberataque-que-paraliza-numerososistemas-de-TI-en-Costa-Rica.html

Rubens P. Types of Firewalls: What IT Security Pros Need to Know. Available from: https://www.esecurityplanet.com/networksecurity/firewalltypes.html

Seguin P, Latto N. Qué es el ransomware y cómo protegerse de él. Avast. 2021 Sep 24. Available from: https://www.avast.com/es-es/c-what-is-ransomware

Solarte F, Enriquez E, Benavides M. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL. 2015;28(5):504. Available from: http://200.10.147.88/index.php/tecnologica/article/view/456

Talalaev A. What is Web Application Firewall (WAF)?. 2018. Available from: https://www.webarxsecurity.com/web-application-firewall/

Análisis de seguridad informática del sistema académico integrado (si@net) de la ueb, según iso 27001:2022, se publicó en el mes de diciembre de 2025.

ISBN: 978-9907-0-0537-0

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

BIOGRAFÍA DE LOS AUTORES

Patricia Isabel Albán Yánez:

Patricia Isabel Albán Yánez, Ingeniera en Sistemas Informáticos nacida en Riobamba en 1978, he trabajado en Hardware System como Ingeniero en Sistemas; Empresa Eléctrica de Bolívar como Programador, Coordinadora Académica – Instituto Superior Tecnológico Stanford. Docente: Unidad Educativa "Cap. Edmundo Chiriboga, Instituto Tecnológico Superior Stanford. Docente en la Universidad Estatal de Bolívar. Apasionada por la innovación tecnológica y la programación.

Diana Paola Salazar Guaraca:

Magister en Educación Parvularia, Licenciada en Ciencia de la Educación mención en educación parvularia y básica inicial. Auxiliar en Educación Parvularia; Diplomado en trastornos de lenguaje Capacitación: Sensibilización de discapacidades, Análisis y diseño de experimentos con métodos estadísticos aplicado a investigaciones, Modelo de desarrollo de software educativo multimedia, Seminario Virtual Nacional de Educación inclusiva una respuesta efectiva a la diversidad.

Edgar Henry Albán Yánez:

Edgar Henry Albán Yánez, Ingeniero en Sistemas nacido en Riobamba en 1977, he trabajado en la Universidad Estatal de Bolívar desde el 2006.

Ernesto Paúl Zavala Cárdenas:

Docente en la Universidad Estatal de Bolívar desde el 2005,pasantía Internacional de febrero a mayo del 2003.Instituto Superior Politécnico José Antonio Echeverría, CUJAE, Cuba, Ex Director de Escuela Ciencias de la Informática de la FCE, Ex Director de la Extensión de San Miguel de la Universidad Estatal de Bolívar.

Michael Daniel Soriano Panchan:

Michael Daniel Soriano Panchana es ingeniero de software enfocado en la investigación científica y el desarrollo tecnológico. Su labor se orienta al estudio y aplicación de metodologías innovadoras en el ámbito informático,

con el propósito de contribuir al avance del conocimiento y la optimización de procesos tecnológico.

Klever Dennis Llanos Varga:
Mi nombre es Klever Llanos, nací en la ciudad de Puyo y soy profesional en Ingeniería de Software. Utilizo ingenio técnico, colaboración y una inquietud continua para desarrollar soluciones digitales que generan impacto. Siempre estoy en la búsqueda de aprender, crecer y afrontar desafíos con dedicación y entusiasmo.

.

ANÁLISIS DE SEGURIDAD INFORMÁTICA DEL SISTEMA ACADÉMICO INTEGRADO (SI@NET) DE LA UEB, SEGÚN ISO 27001:2022

Estimado lector, la Universidad Estatal de Bolívar (UEB) ha reconocido la urgencia de fortalecer la seguridad informática de su Sistema Académico Integrado en Red (SI@NET), esencial para la gestión de datos académicos y personales. Para ello, está realizando un análisis basado en la norma internacional ISO 27001:2022.

Este esfuerzo busca identificar y mitigar riesgos, implementar un Sistema de Gestión de Seguridad de la Información (SGSI) y fomentar una cultura de seguridad en toda la comunidad universitaria.

El proyecto, liderado por un equipo multidisciplinario, es un compromiso con la mejora continua y busca proteger la integridad y confidencialidad de la información, haciendo un llamado a la responsabilidad colectiva para un entorno académico más seguro. Agradecemos a todos los lectores que se acercan a esta obra con ánimo de aprender, aplicar y transformar.

GRUPO BLR

UEB UNIVERSIDAD ESTATAL DE BOLIVAR

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

ISBN: 978-9907-0-0537-0