**UNIVERSIDAD ESTATAL DE BOLÍVAR**

**FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA**

CARRERA DE SOFTWARE

**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIEROS EN SOFTWARE**

**FORMA:** PROYECTO DE INVESTIGACIÓN

**TEMA:**

# 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.

**AUTORES:**

MICHAEL DANIEL SORIANO PANCHANA

KLEVER DENNIS LLANOS VARGAS

**DIRECTOR:**

ING. HENRY ALBÁN YANEZ

**GUARANDA – ECUADOR**

**2023**

**TEMA DEL PROYECTO DE INVESTIGACIÓN**

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.

**AGRADECIMIENTO**

En primer lugar, queremos agradecer a Dios por darnos salud y fortaleza para poder cumplir una de las metas más anheladas en nuestra vida, además, agradecer infinitamente a nuestras familias quienes son los principales promotores de nuestros sueños, gracias por la confianza en cada uno de nosotros, por habernos inculcado valores y principios.

A nuestro director de proyecto, el Ing. Henry Albán, por su acompañamiento durante el desarrollo del proyecto, su dedicación y empeño para llevar a cabo este logro.

Al Ing. Rodrigo del Pozo y a la Ing. Galuth García tutores que durante todo el proceso nos brindaron su tiempo y orientaron con sus contribuciones en los lineamientos para los avances del proyecto.

A la Universidad Estatal de Bolívar y al departamento de TIC's por brindarnos la facilidad de poder realizar este estudio dentro de su sistema, por el acompañamiento y apoyo que me han permitido progresar en mi carrera profesional

A nuestros verdaderos amigos de la Universidad Estatal de Bolívar, quienes han estado presentes en los buenos y malos momentos, siempre brindando su apoyo y amistad absoluta.

***Llanos Klever & Soriano Michael***

## DEDICATORIA

Este proyecto de investigación quiero dedicar a mis padres, Alicia Mercedes Vargas Paantam y Kleber Mesías Llanos García, y hermanos, Katherine Cristina Llanos Vargas y Daniel Alejandro Vargas Paantam, por su amor y apoyo incondicional durante todo mi proceso de formación académica. Gracias por ser mi fuente de motivación y por brindarme la oportunidad de crecer y desarrollarme como persona y como un buen profesional.

Finalmente, me dedico esta tesis a mí mismo, por mi esfuerzo y dedicación en este proyecto. Espero que este trabajo sea una contribución valiosa en mi camino hacia la realización de mis metas y objetivos tanto personales como profesionales.

***Llanos Klever***

Esta tesis va dedicada:

A mis padres Rina Panchana y Felix Soriano quienes con su amor, paciencia y esfuerzo me dieron la oportunidad de cumplir un sueño más, gracias por criarme con valores y principios a lo largo de mi vida.

A mis abuelos Silvia Ruiz y Eddie Panchana por su afecto y apoyo incondicional, por estar conmigo en cada momento. A toda mi familia por estar presente aconsejándome y motivándome para lograr que crezca como persona y que me acompañan en todas mis metas y sueños.

***Soriano Michael***

# CERTIFICADO DE VALIDACIÓN

Ing. Henry Albán, Ing. Rodrigo Del Pozo e Ing. Galuth García, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "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" desarrollado por los señores Llanos Vargas Klever Dennis y Soriano Panchana Michael Daniel.

## CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 09 de junio del 2023

Firmado electrónicamente por:
EDGAR HENRY ALBAN YANEZ

Ing. Henry Albán
**Director**

Firmado electrónicamente por:
RODRIGO HUMBERTO DEL POZO DURANGO

Ing. Rodrigo Del Pozo
**Par Académico**

Firmado electrónicamente por:
GALUTH IRENE GARCIA CAMACHO

Ing. Galuth García
**Par Académico**

## DERECHOS DE AUTOR

Nosotros, **Michael Daniel Soriano Panchana y Klever Dennis Llanos Vargas** portadores de las cédulas de identidad **N° 2450066002** y **1600700452** respectivamente**,** en calidad de autor/res y titular/es de los derechos morales y patrimoniales del Trabajo de Titulación: **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,** modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizamos a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de titulación el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Los autores declaran que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
MICHAEL DANIEL SORIANO PANCHANA

Michael Daniel Soriano Panchana
CI. 2450066002

Firmado electrónicamente por:
KLEVER DENNIS LLANOS VARGAS

Klever Dennis Llanos Vargas
CI. 1600700452

**TABLA DE CONTENIDO**

INTRODUCCIÓN ..... 1

RESUMEN ..... 3

ABSTRACT ..... 4

CAPÍTULO I ..... 5

FORMULACIÓN GENERAL DEL PROYECTO ..... 5

1.1. Descripción del Problema ..... 5

1.2. Formulación del Problema ..... 5

1.3. Preguntas de Investigación ..... 5

1.4. Justificación ..... 6

1.5. Objetivos ..... 7

1.6. Idea a Defender ..... 7

CAPÍTULO II ..... 8

MARCO TEÓRICO ..... 8

2.1. Antecedentes ..... 8

2.2. Científico ..... 9

2.2.1. Seguridad Informática ..... 9

2.2.2. Seguridad de la Información ..... 9

2.2.3. Ransomware ..... 9

2.3. Conceptual ..... 9

2.3.1. Sistema operativo ..... 9

2.3.2. Kali Linux ..... 9

2.3.3. Base de datos ..... 10

2.3.4. Aplicación web ..... 10

2.3.5. Vulnerabilidad ..... 10

2.3.6. Firewall de red ..... 11

2.3.7. Firewall de aplicaciones web ..... 11

2.3.8. OWASP ZAP ..... 11
2.4. Legal ..... 12
2.4.1. Organización Internacional de la Normalización ..... 12
2.4.2. Norma ISO 27001 ..... 12
2.4.3. Comparativa ISO 27001:2013 vs 27001:2022 ..... 13
2.4.4. Decreto 1014 Software Libre en Ecuador ..... 13
2.5. Georreferenciación ..... 14
CAPITULO III ..... 15
METODOLOGÍA ..... 15
3.1. Tipo de Investigación ..... 15
3.2. Enfoque de la investigación ..... 15
3.3. Métodos de Investigación ..... 15
3.4. Técnicas e Instrumentos de Recopilación de Datos ..... 15
3.5. Universo, Población y Muestra ..... 16
3.6. Procesamiento de la Información ..... 16
CAPITULO IV ..... 17
RESULTADOS Y DISCUSIÓN ..... 17
4.1. Análisis, Interpretación y Discusión de Resultados ..... 17
4.1.1. Antecedentes ..... 17
4.1.2. Análisis de los niveles de seguridad actuales. ..... 18
4.1.3. Análisis de vulnerabilidades. ..... 24
4.1.4. Discusión de resultados. ..... 38
CAPITULO V ..... 40
PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (PGSI) ..... 40
5.1. Introducción ..... 40
5.2. Objetivo ..... 41
5.3. Control de acceso a la información ..... 41

5.3.1. Cifrado de información ..... 41
5.3.2. Acceso remoto ..... 41
5.3.3. Asignación de roles y responsabilidades. ..... 42
5.3.4. Contraseñas ..... 42
5.4. Gestión de activos ..... 43
5.5. Responsabilidades del personal ..... 44
5.6. Restricciones de instalación ..... 44
5.7. Seguridad física ..... 44
5.8. Sanciones por incumplimiento ..... 45
5.9. Mejoras de seguridad en el sistema académico integrado en red (SI@NET) de la Universidad Estatal de Bolívar ..... 46
CONCLUSIONES ..... 49
RECOMENDACIONES ..... 50
BIBLIOGRAFÍA ..... 51
ANEXOS ..... 54

**INDICE DE TABLAS**

**Tabla 1** Vulnerabilidades encontradas – Módulo SME y PPP ..... 25
**Tabla 2** Vulnerabilidades encontradas - Módulo CAED ..... 28
**Tabla 3** Vulnerabilidades encontradas - Modulo SDA ..... 30
**Tabla 4** Niveles de impacto de las vulnerabilidades ..... 34
**Tabla 5** Ficha de Observación – Impacto de vulnerabilidades ..... 34
**Tabla 6** Actividades urgentes ..... 36
**Tabla 7** Resumen de la probabilidad ocurrencia ..... 37
**Tabla 8** Solución a las vulnerabilidades encontradas ..... 46
**Tabla 9** Presupuesto ..... 55

**INDICE DE FIGURAS**

**Figura 1** Mapa Georreferencial de la Universidad Estatal de Bolívar..... 14
**Figura 2** Pregunta 1 – ¿La institución ha tenido algún incidente relacionado con la seguridad informática en los últimos 3 años?..... 18
**Figura 3** Pregunta 2 – ¿Qué problemas de seguridad informática ha tenido el sistema académico integrado en red (SI@NET) en sus módulos activos?..... 19
**Figura 4** Pregunta 3 – ¿Qué módulos específicos han sufrido ataques?..... 19
**Figura 5** Pregunta 4 – ¿Cuáles fueron los problemas más relevantes para el sistema SI@NET? ..... 20
**Figura 6** Pregunta 5 – ¿Qué temas de seguridad aún no se puede controlar en su totalidad? ..... 20
**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?..... 21
**Figura 8** Pregunta 7 –¿Qué mecanismos, técnicas, herramientas o normas de seguridad se utilizan en el sistema SI@NET de la UEB?..... 21
**Figura 9** Pregunta 8 – ¿Qué conocimientos tiene sobre las políticas o normas que gestionan la Seguridad de la información?..... 22
**Figura 10** Pregunta 9 – ¿Tiene conocimiento sobre las Normas ISO 27001:2022 – Anexo A?..... 22
**Figura 11** Pregunta 10 – ¿Disponen de algún plan de gestión de seguridad informática aplicable a la UEB? ..... 23
**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?..... 23
**Figura 13** Análisis de vulnerabilidades - Módulo SME y PPP ..... 24
**Figura 14** Alertas encontradas - Módulos SME y PPP..... 25
**Figura 15** Análisis de vulnerabilidades - Módulo CAED ..... 27
**Figura 16** Alertas encontradas - Módulo CAED ..... 28
**Figura 17** Análisis de vulnerabilidades - Módulo SDA ..... 30
**Figura 18** Alertas encontradas - Módulo SDA ..... 30
**Figura 19** Análisis de puertos – Sistema SI@NET ..... 32
**Figura 20** Diagrama de actividades Gantt ..... 54
**Figura 21** Programa de hacking ético OWASP ZAP ..... 61

## 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.

**RESUMEN**

El objetivo del presente proyecto de investigación fue realizar el análisis de la seguridad informática y de puertos 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. Se realizó un estudio de campo que permitió conocer las vulnerabilidades en el Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, para lo cual se llevó a cabo varios ataques mediante la herramienta OWASP ZAP lo que permitió determinar las políticas de seguridad para el Plan de Gestión de Seguridad de la Información (PGSI) acorde a la norma antes señalada. Los resultados que se obtuvieron luego del ataque a los cuatro módulos activos es que el sistema tiene varias vulnerabilidades las cuales son expuestas en el capítulo 5 con sus respectivas soluciones, pero sin embargo existen 2 que deben ser mitigadas de manera urgente porque el nivel de impacto es demasiado alto, además, se debe tener conciencia sobre la importancia de la seguridad de la información por lo que el sistema mediante el PGSI debe tener la posibilidad de eliminar o mitigar los riesgos de posibles ataques y robo de información, finalmente se recomienda que se debe conformar un comité de seguridad informática con el fin de gestionar la seguridad.

**Palabras clave:** Seguridad informática, Vulnerabilidad, OWASP ZAP, ISO 27001:2022

## ABSTRACT

The objective of this research project was to carry out the analysis of computer and port security for the Integrated Network Academic System (SI@NET) of the State University of Bolívar, based on the ISO 27001:2022 standard - Annex A, for the year 2023. A field study was carried out that revealed the vulnerabilities in the Integrated Network Academic System (SI@NET) of the State University of Bolívar, for which several attacks were carried out using the OWASP ZAP tool, which allowed to determine the security policies for the Information Security Management Plan (ISMP) in accordance with the aforementioned standard. The results that were obtained after the attack on the four active modules is that the system has several vulnerabilities which are exposed in chapter 5 with their respective solutions, but nevertheless there are 2 that must be urgently mitigated because the level of impact is too high, in addition, one must be aware of the importance of information security, so the system through the ISMP must have the possibility of eliminating or mitigating the risks of possible attacks and theft of information, finally it is recommended that it be You must form a computer security committee to manage security.

**Keywords:** Computer security, Vulnerability, OWASP ZAP, ISO 27001:2022

# CAPÍTULO I

# FORMULACIÓN GENERAL DEL PROYECTO

## 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

### 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.

### 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

# MARCO TEÓRICO

## 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. Científico

### 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. 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

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. 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)

### 2.3.9. 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. Legal

### 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)

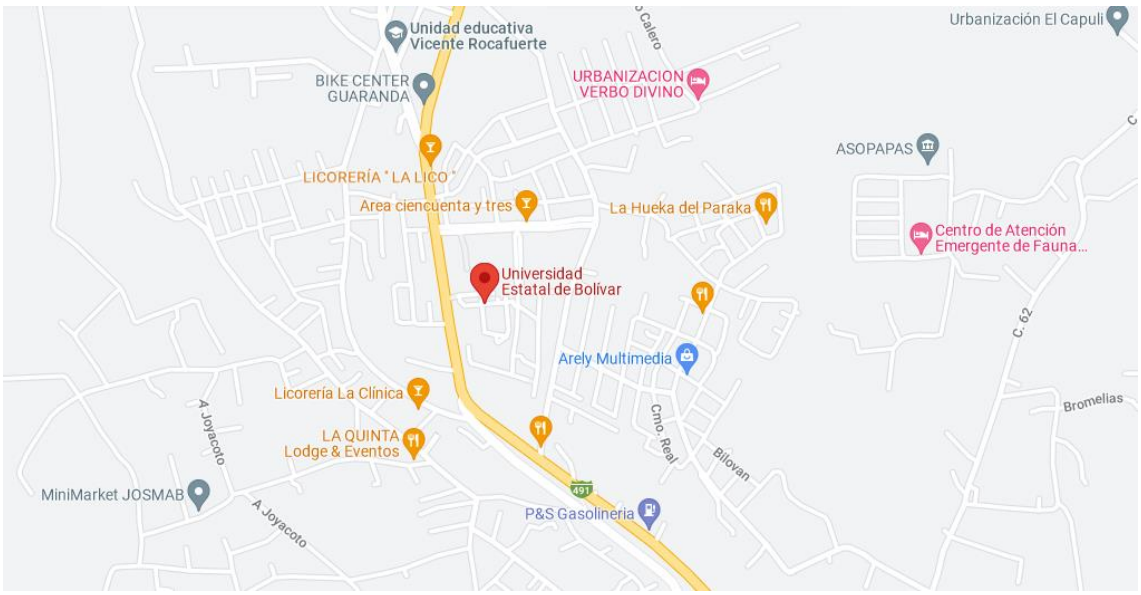
"Art. 4. Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo de seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno." (Presidencia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

## 2.5. Georreferenciación

**Dirección:** Av. Ernesto Che Guevara y Gabriel Sacaira

**Figura 1**

*Mapa Georreferencial de la Universidad Estatal de Bolívar*




**Fuente:** Google Maps.

**Coordenadas Geográficas:** -1.5706764830506152, -79.0061831592369

# CAPITULO III

# METODOLOGÍA

## 3.1. Tipo de Investigación

### 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

### 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

### 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).

**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.

# CAPITULO IV

# RESULTADOS Y DISCUSIÓN

## 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.

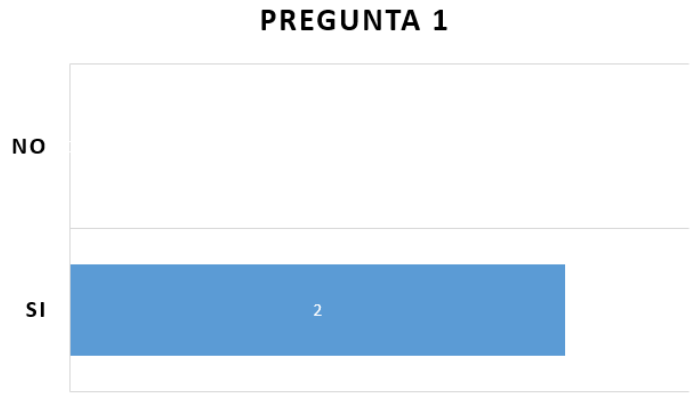
Finalmente se realizó la propuesta de un Plan de Gestión de Seguridad de la Información según la norma ISO 27001:2022 – Anexo A, misma que permitirá mitigar los riesgos de confidencialidad e integridad de los datos y de la información.

### 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**

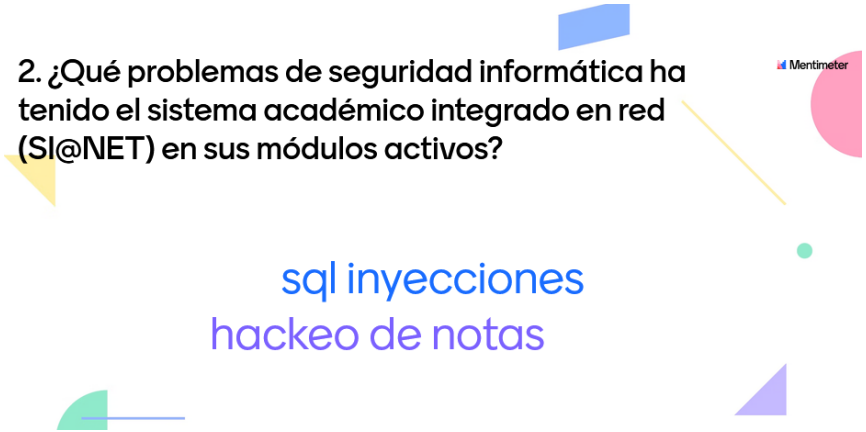
*Pregunta 1 – ¿La institución ha tenido algún incidente relacionado con la seguridad informática en los últimos 3 años?*




**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.

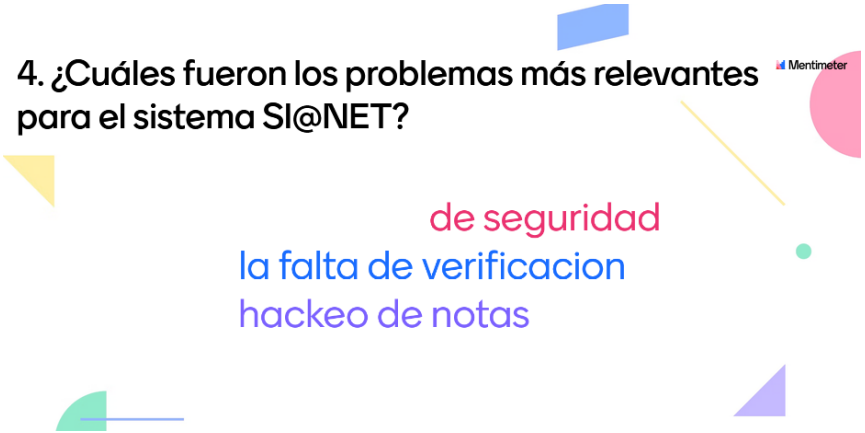
**Figura 4**

*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**

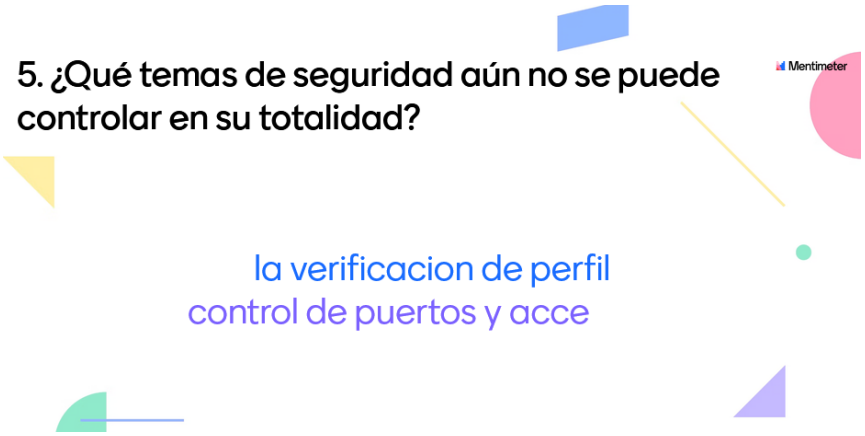
*Pregunta 4 – ¿Cuáles fueron los problemas más relevantes para el sistema SI@NET?*




**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**

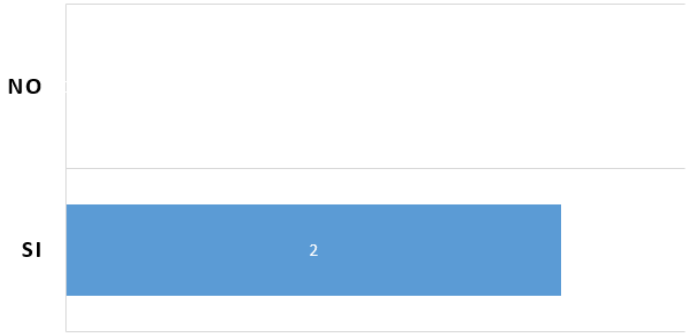
*Pregunta 5 – ¿Qué temas de seguridad aún no se puede controlar en su totalidad?*




**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**

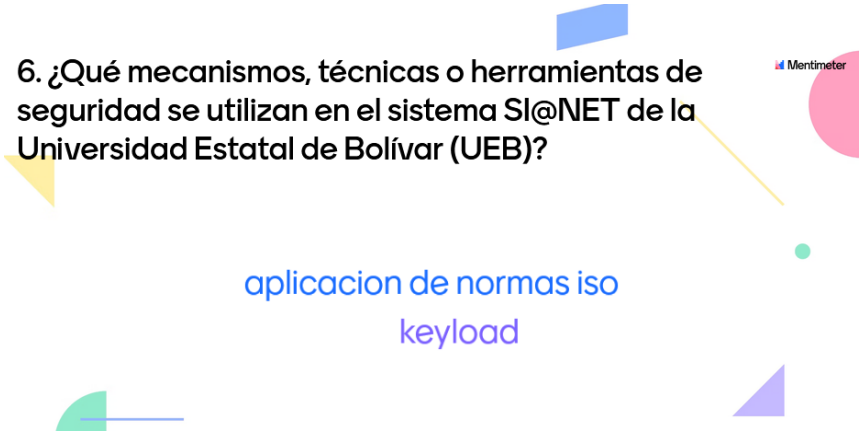
*Pregunta 6 – ¿Se aplica actualmente políticas o normas de seguridad para proteger la información en el sistema SI@NET en sus cuatro módulos activos?*




**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?*

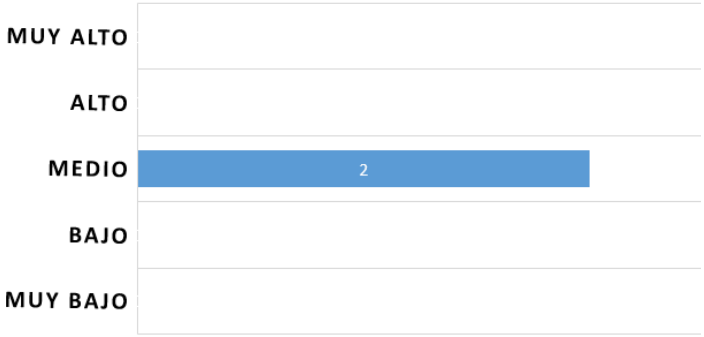



**Análisis e Interpretación:** Los mecanismos, técnica o herramientas de seguridad que se utilizan actualmente en el SI@NET es la aplicación de normas ISO 27001 del año 2013, el cual ya hubo actualizaciones y aún no se ha migrado a la última actualización que es del año 2022, además, hacen uso del mecanismo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

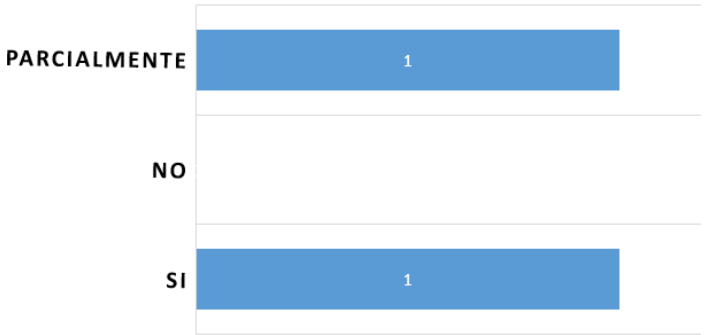
| | |
|---|---|
| MUY ALTO | |
| ALTO | |
| MEDIO | |
| BAJO | |
| MUY BAJO | |




**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**

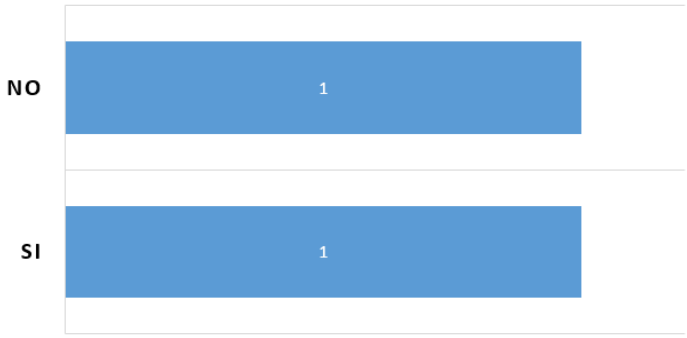
*Pregunta 9 – ¿Tiene conocimiento sobre las Normas ISO 27001:2022 – Anexo A?*




**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**

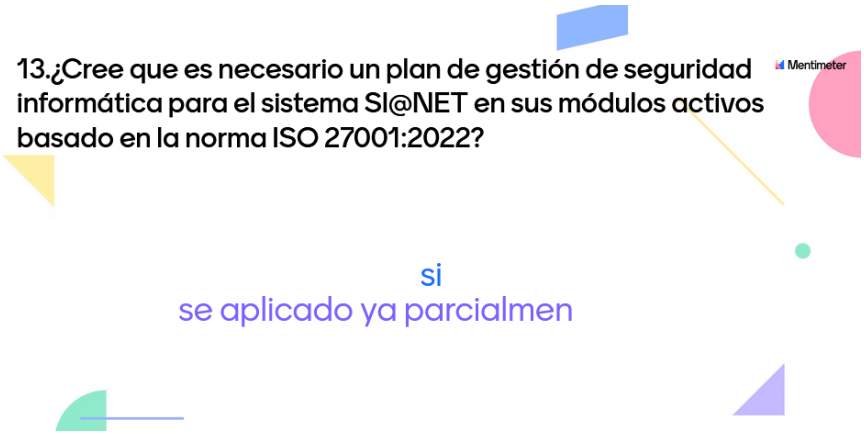
*Pregunta 10 – ¿Disponen de algún plan de gestión de seguridad informática aplicable a la UEB?*




**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:

**Módulos 1 – 2: Sistema De Matriculación Estudiantil (SME) y Prácticas Pre-Profesionales (PPP)**

**Figura 13**

*Análisis de vulnerabilidades - Módulo SME y PPP*

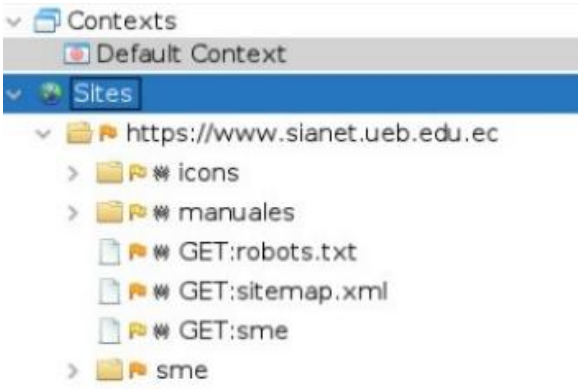


**Figura 14**

*Alertas encontradas - Módulos SME y PPP*


**Tabla 1**

*Vulnerabilidades encontradas – Módulo SME y PPP*

| **Vulnerabilidad** | **Detalle** | **Riesgo** | **Cantidad de alertas** |
|---|---|---|---|
| Ausencia de tokens anti-CSRF | "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 confidencial, como la ubicación del archivo que produjo la excepción no controlada." (OWASP, 2017) | Medio | 63 |

| | | | |
|---|---|---|---|
| • CSP: Wildcard Directive<br>• CSP: script-src unsafe-inline<br>• CSP: style-src unsafe-inline | "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.*

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

**Figura 15**

*Análisis de vulnerabilidades - Módulo CAED*

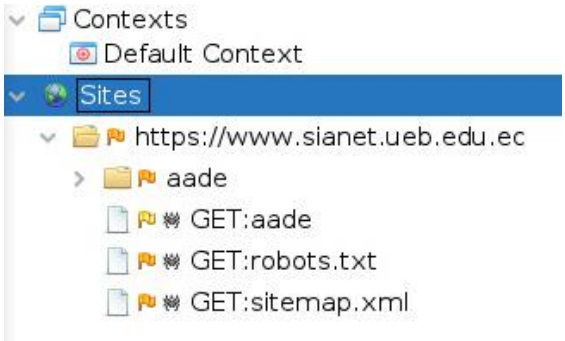


**Figura 16**

*Alertas encontradas - Módulo CAED*

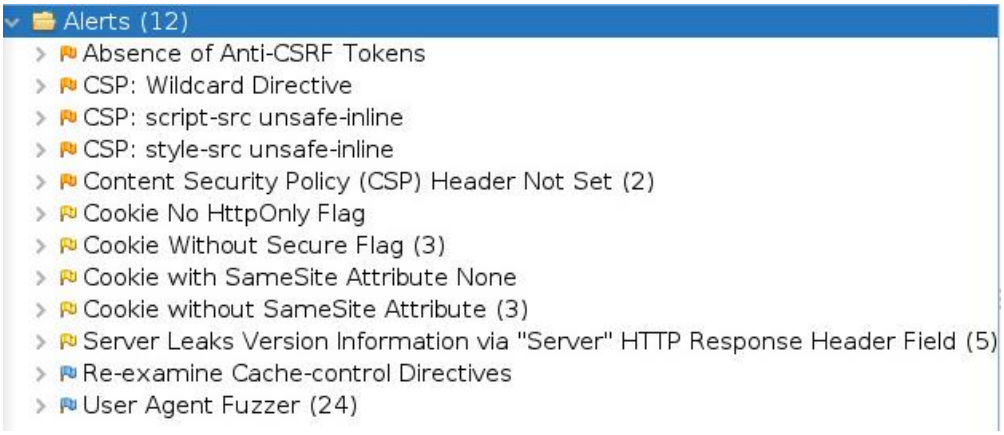



**Tabla 2**

*Vulnerabilidades encontradas - Módulo CAED*

| Vulnerabilidad | Detalle | Riesgo | Cantidad de alertas |
|---|---|---|---|
| Ausencia de tokens anti-CSRF | "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<br>• CSP: script-src unsafe-inline<br>• CSP: style-src unsafe-inline | "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 |
| 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 |

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

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

**Figura 17**

*Análisis de vulnerabilidades - Módulo SDA*

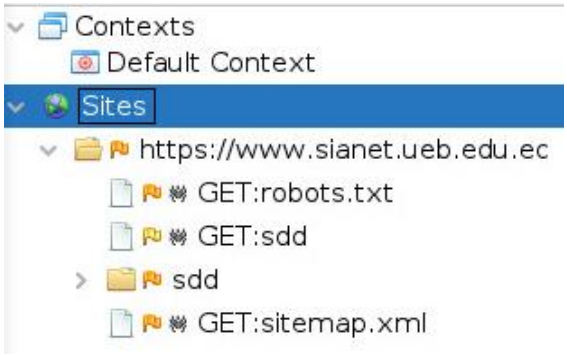



**Figura 18**

*Alertas encontradas - Módulo SDA*

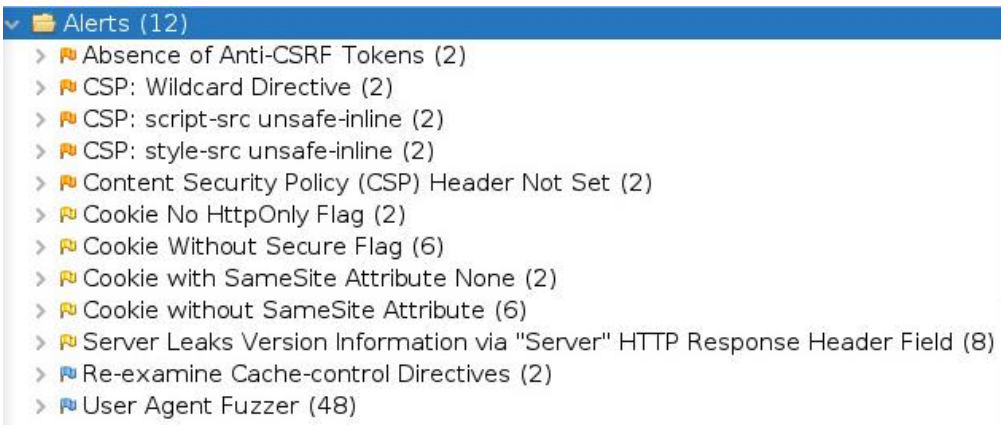



**Tabla 3**

*Vulnerabilidades encontradas - Modulo SDA*

| Vulnerabilidad | Detalle | Riesgo | Cantidad de alertas |
|---|---|---|---|
| Ausencia de tokens anti-CSRF | "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 | Medio | 2 |

| | | | |
|---|---|---|---|
| | realizar una acción como víctima.” (OWASP, 2017) | | |
| • CSP: Wildcard Directive<br>• CSP: script-src unsafe-inline<br>• CSP: style-src unsafe-inline | “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 |
| 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 | “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 | Bajo | 345 |

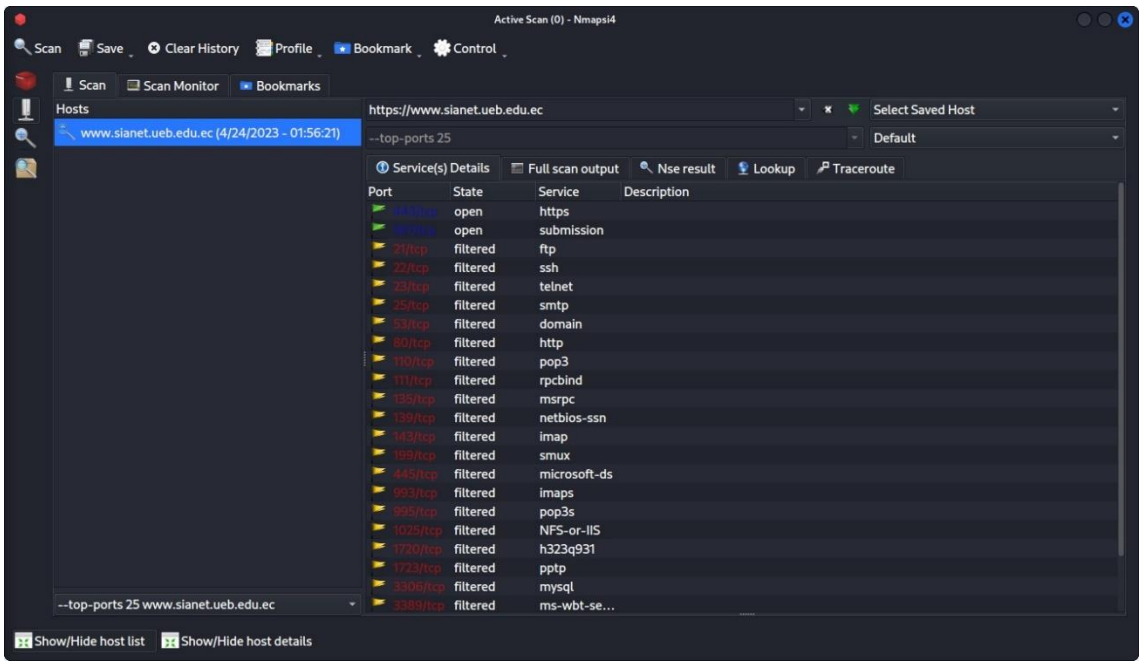
| | | |
|---|---|---|
| través del campo de encabezado de respuesta HTTP 'Servidor' | atacantes la identificación de otras vulnerabilidades a las que está sujeto su servidor web/aplicaciones.” (OWASP, 2017) | |

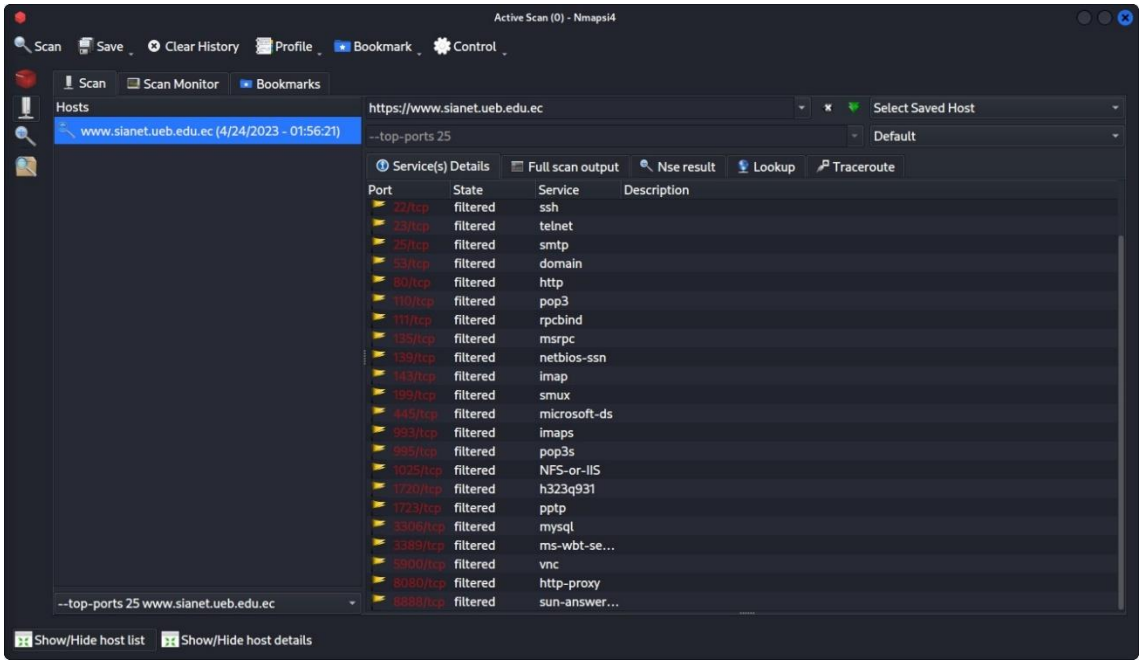
***Elaborado por:*** *Soriano M. & Llanos K.*

## 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.

#### 4.1.3.1. 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 |

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

**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 anti-CSRF | X | | | | 25% |
| Divulgación de error de aplicación | X | X | X | | 75% |
| • CSP: Wildcard Directive<br>• CSP: script-src unsafe-inline | X | | X | | 50% |

| | | | | | |
|---|---|---|---|---|---|
| • CSP: style-src unsafe-inline | | | | | |
| 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<br>• Cookie sin bandera segura | X | | | | 25% |
| 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 – | X | | | X | 50% |

| | | | | | |
|---|---|---|---|---|---|
| Comentarios sospechosos | | | | | |

**Elaborado por:** 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<br>• CSP: script-src unsafe-inline<br>• 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 | MEDIO |

| | | |
|---|---|---|
| | respuesta HTTP 'Servidor' | |
| ACT6 | Divulgación de información – Comentarios sospechosos | MEDIO |
| ACT7 | Ausencia de tokens anti-CSRF | BAJO |
| ACT8 | • Bandera de Cookie No HttpOnly<br>• Cookie sin bandera segura | BAJO |
| ACT9 | Falta el encabezado de tipo de contenido | BAJO |

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

**Descripción:** Se enlistaron las actividades considerando el nivel de impacto establecidos en la tabla 2, 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 | Exploración de directorios | El servidor filtra la información de la versión | Divulgación de información – |

| | | | | | |
|---|---|---|---|---|---|
| | | • CSP: script-src unsafe-inline<br>• CSP: style-src unsafe-inline | | a través del campo de encabezado de respuesta HTTP 'Servidor' | Comentarios sospechosos |
| **BAJA** | **1% - 25%** | Ausencia de tokens anti-CSRF | • Bandera de Cookie No HttpOnly<br>• Cookie sin bandera segura | Falta el encabezado de tipo de contenido | |

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

### 4.1.4. Discusión de resultados.

Una vez realizada la investigación sobre las diversas vulnerabilidades encontradas mediante el análisis producido con la herramienta de hacking ético OWASP ZAP a los módulos activos del Sistema Académico Integrado en Red (SI@NET) los cuales son: Sistema de Matriculación Estudiantil (SME), Control de Asistencia Estudiantil y Docente (CAED), Prácticas Pre-Profesionales (PPP) y el Sistema de Distributivo Académico (SDA). Los resultados obtenidos a través de la herramienta ya mencionada es de que existe nueve actividades como se puede observar en la Tabla 6, las cuales le hacen vulnerable al sistema anteriormente mencionado, además de la falta de implementación de la norma ISO 27001 – Anexo A, por lo cual es de suma importancia el desarrollo del plan de gestión de seguridad informática basado en los beneficios que ofrece actualmente la norma ISO 27001:2022 – Anexo A, para poder evitar o mitigar los problemas que se detallarán a continuación.

Se puede observar el resultado en la Tabla 7 que en un rango de probabilidad bajo del 1% al 25% que existe la Ausencia de tokens anti-CSRF el cual su función es evitar el ataque de fuerza al navegador web a través del envío de peticiones a un sistema web, la Falta de encabezado de tipo de contenido, Bandera de Cookie No HttpOnly y la Cookie sin bandera segura, es peligroso debido a que es posible

robar o manipular sesiones de aplicaciones web y las cookies, por lo que es mejor administrar esto dentro de la codificación del software.

Dentro del rango de probabilidad de ocurrencia media del 25% al 50% se puede observar que existen cuatro vulnerabilidades las cuales son: la Política de Seguridad de contenido CSP (Wildcard Directive, script-src unsafe-inline y style-src unsafe-inline), el cual nos permite reducir el daño causado por los ataques de inyección de contenido y estos actualmente se encuentran inseguros, la exploración de directorios el cual se basa en una característica que proporciona automáticamente una página web predeterminada de los directorios y archivos disponibles, el servidor filtra la información de la versión a través del campo de encabezado de respuesta HTTP 'Servidor' y la Divulgación de información – Comentarios sospechosos.

El rango de nivel de probabilidad de ocurrencia de tipo alta que es del 50% al 100% se encuentra las vulnerabilidades de divulgación de error de aplicación el cual permite la comunicación de manera insegura al momento de transferir datos entre el sistema antes mencionado y la base de datos, y finalmente la última vulnerabilidad encontrada se trata del encabezado de política de seguridad de contenido (CSP) no establecido es un gran problema debido a que no especifica que todo el contenido del Sistema Académico Integrado en Red, en sus cuatro módulos activos, se debe cargar utilizando el HTTP para de esta manera asegurar que el navegador solo se conecte mediante los canales grabados.

# CAPITULO V

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

## 5.1. Introducción

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.

## 5.2. Objetivo

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

## 5.3. 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:

1. 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.
2. No se deberá entregar ningún tipo de información por teléfono, celular, correo electrónico, redes sociales, hasta que la identidad del solicitante sea verificada.
3. 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.

### 5.3.1. Cifrado de información

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

### 5.3.2. Acceso remoto

1. 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.
2. El servicio de acceso remoto debe permitir solo acceso al sistema de información de la universidad y a archivos compartidos en la intranet.
3. 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.

4. 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.
5. El director de TIC's debe garantizar la disponibilidad del servicio de conexión remota a los usuarios para que accedan al sistema.

### 5.3.3. Asignación de roles y responsabilidades.

1. 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.
2. 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.
3. El director de TIC's asignará y eliminará permisos de acceso a los usuarios.

### 5.3.4. 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:

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

## 5.4. 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.

1. Se deberá disponer de un inventario de los activos informáticos del departamento de TIC's y actualizarlo constantemente.
2. Es responsabilidad del director de TIC's crear una codificación que permita identificar cada activo dentro del departamento.
3. 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.
4. Se deberán definir pólizas de seguros para cubrir los activos en caso de siniestros.
5. 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.
6. 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.
7. 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.
8. Los equipos administrados por el departamento de TIC's son netamente para uso laboral.
9. Es responsabilidad de cada empleado mantener el equipo asignado o solicitado en buenas condiciones, está prohibido hacerle alteraciones.

## 5.5. 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.

## 5.6. 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.

## 5.7. Seguridad física

1. 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.

2. Se pondrán señaléticas de seguridad en espacios donde solo deba ingresar personal autorizado/capacitado.
3. Los componentes electrónicos serán instalados únicamente por personal capacitado y con los respectivos medios de seguridad.
4. 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.
5. El funcionamiento del sistema de alarma se deberá comprobar periódicamente para garantizar la protección de las instalaciones.
6. 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.
7. Evaluar periódicamente todos los controles de acceso físico para garantizar que son adecuados y que se cumplen en su totalidad.
8. Los servidores deberán estar en una habitación cerrada y se deberá asegurar de que únicamente acceden las personas que cuentan con los respectivos permisos.
9. Los documentos confidenciales serán almacenados en armarios cerrados, para evitar el hurto de información sensible.

## 5.8. 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.

## 5.9. 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 anti-CSRF | 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<br>• CSP: script-src unsafe-inline<br>• CSP: style-src unsafe-inline | Hay que asegurarse que el servidor web y servidor de aplicaciones estén configurados correctamente para establecer los encabezados de políticas de seguridad de contenido | Anexo 16 |
| 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 |

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

**Consideraciones respecto al análisis de puertos y seguridad de acceso a servidores.**

1. Utilizar VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH.
2. 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.

3. Gestionar los controles de red para permitir sólo el acceso necesario para cada conexión de terceros.
4. El director de TIC’s deberá crear un canal seguro mediante VPN (Red Privada Virtual) para los accesos remotos mediante el puerto 23 telnet.

## CONCLUSIONES

La elaboración del análisis de riesgos mediante la herramienta de hacking ético OWASP ZAP, en los módulos de Matriculación Estudiantil y en el de las Prácticas Pre Profesionales se encontraron las mismas 19 vulnerabilidades, en los módulos de Control de Asistencia Estudiantil y Docente, y en el Sistema de Distributivo Académico se encontró 12 vulnerabilidades, las cuales 2 actividades tienen un nivel de impacto demasiado alto el cual debe ser mitigado de manera urgente con base al Plan de Gestión de Seguridad de Información (PGSI) propuesto en el capítulo 5.

Al utilizar la herramienta de hacking ético OWASP ZAP se logró detectar las diferentes vulnerabilidades en el sistema SI@NET, tabulando los resultados en herramientas ofimáticas y haciendo el respectivo análisis se pudo comprender el nivel de impacto que podrían tener en el sistema, por lo tanto, se deben tomar medidas de seguridad para que en un futuro estas vulnerabilidades no sean aprovechadas por terceros.

Se toma conciencia sobre la importancia de la seguridad de la información actualmente por ende, mediante la implementación del plan de gestión de seguridad informática para el sistema SI@NET en sus cuatro módulos activos perteneciente a la Universidad Estatal de Bolívar, basándonos en las normas ISO 27001:2022 – Anexo A, para así establecer un procedimiento continuo en la gestión de la seguridad informática en el sistema antes mencionado y en sus módulos activos, además, de esta manera tener la posibilidad de eliminar o mitigar los riesgos de posibles ataque y robo de la información.

## RECOMENDACIONES

Con base a los análisis obtenidos por medio de la herramienta OWASP ZAP, se pudo conocer que existe 9 actividades que se deben mitigar conforme se encuentra establecido en el PGSI presentando en el capítulo 5, se recomienda solucionar las diversas vulnerabilidades existentes conforme el nivel de impacto, las cuales 2 actividades se deben resolver de manera urgente debido a que el nivel de impacto es demasiado alto.

Previo al análisis de vulnerabilidades, puertos y seguridad de acceso a los servidores se recomienda utilizar VPN para la conectividad de acceso de usuario remoto según las diversas tecnologías como lo son los protocolos de comunicación para configurar conexiones seguras (IPSec), el protocolo de navegadores web y servidores como lo es la capa de sockets seguros (Secure Sockets Layer – SSL) y el protocolo de red el cual se encuentra destinado principalmente al control de usuarios y a la modificación de sus servidores por medio del internet el cual su acceso es a través de la línea de comandos Secure Shell (SSH).

La seguridad y confidencialidad de la información es de vital importancia en todas las instituciones, por ello es importante que la Universidad Estatal de Bolívar (UEB) despierte el compromiso y el interés por parte del director del departamento de TIC's, con el objetivo de brindar apoyo al área de sistemas, por lo que se recomienda conformar un comité de seguridad informática con el fin de gestionar la seguridad de la información del Sistema Académico Integrado en Red (SI@NET) en especial en sus cuatro módulos activos, dando un seguimiento en el cumplimiento de normas y políticas estandarizadas en el Plan de Gestión de Seguridad de la Información (PGSI), basada en la norma ISO 27001:2022 – Anexo A, para un manejo controlado de la información y a su vez reducir las vulnerabilidades.

**BIBLIOGRAFÍA**


BBC. (20 de 05 de 2022). *BBC News Mundo*. Obtenido de "Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia: https://www.bbc.com/mundo/noticias-america-latina-61516874

Bustamante, G., & Osorio, J. (2015). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa, 6*, 71-77. Obtenido de https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202

Chagmana, R. (2022). 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).* Universidad Técnica de Ambato, Ambato.

Excellente ISOTools. (24 de 02 de 2016). *ISOTools.* Obtenido de La norma ISO 27001: Aspectos claves de su diseño e implantación: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Gómez, C., & Fernanda, L. (2019). Diseño de un sistema de gestión de seguridad informática para la e Empresa Flores Jayvana S.A.S. *(Proyecto aplicado).* Universidad Nacional Abierta y a Distancia UNAD, Bogotá.

López, P. A. (2018). *Seguridad Informática.* Editex.

NmapSi4. (2015). NmapSI4 | Security Interface. Nmapsi4.org: https://nmapsi4.org/

OWASP. (2017). OWASP ZAP - Absence of Anti-CSRF Tokens. Zaproxy.org: https://www.zaproxy.org/docs/alerts/10202/

OWASP. (2017). OWASP ZAP - Application Error Disclosure. Zaproxy.org: https://www.zaproxy.org/docs/alerts/90022/

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

OWASP. (2017). OWASP ZAP - Content-Type Header Missing. Zaproxy.org: https://www.zaproxy.org/docs/alerts/10019/

OWASP. (2017). OWASP ZAP - Cookie No HttpOnly Flag. Zaproxy.org: https://www.zaproxy.org/docs/alerts/10010/

OWASP. (2017). OWASP ZAP - Cookie Without Secure Flag. Zaproxy.org: https://www.zaproxy.org/docs/alerts/10011/

OWASP. (2017). OWASP ZAP - CSP: Wildcard Directive. Zaproxy.org: https://www.zaproxy.org/docs/alerts/10055-4/

OWASP. (2017). OWASP ZAP - Directory Browsing. Zaproxy.org: https://www.zaproxy.org/docs/alerts/10033/

OWASP. (2017). OWASP ZAP - Information Disclosure - Suspicious Comments. Zaproxy.org: https://www.zaproxy.org/docs/alerts/10027/

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

OWASP Risk Rating Methodology - OWASP. (2016). Recuperado de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Presidencia de la Repúbblica. (2008). *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. Obtenido de https://web.gestiondocumental.gob.ec/wp-content/uploads/2020/08/Decreto-Ejecutivo-N-1014.pdf

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

Rubens, P. (2018). Types of Firewalls: What IT Security Pros Need to Know. Retrieved from https://www.esecurityplanet.com/network-security/firewalltypes.html

Seguin, P., & Latto, N. (24 de 09 de 2021). *Qué es el ransomware y cómo protegerse de él*. Obtenido de Avast: https://www.avast.com/es-es/c-what-is-ransomware

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

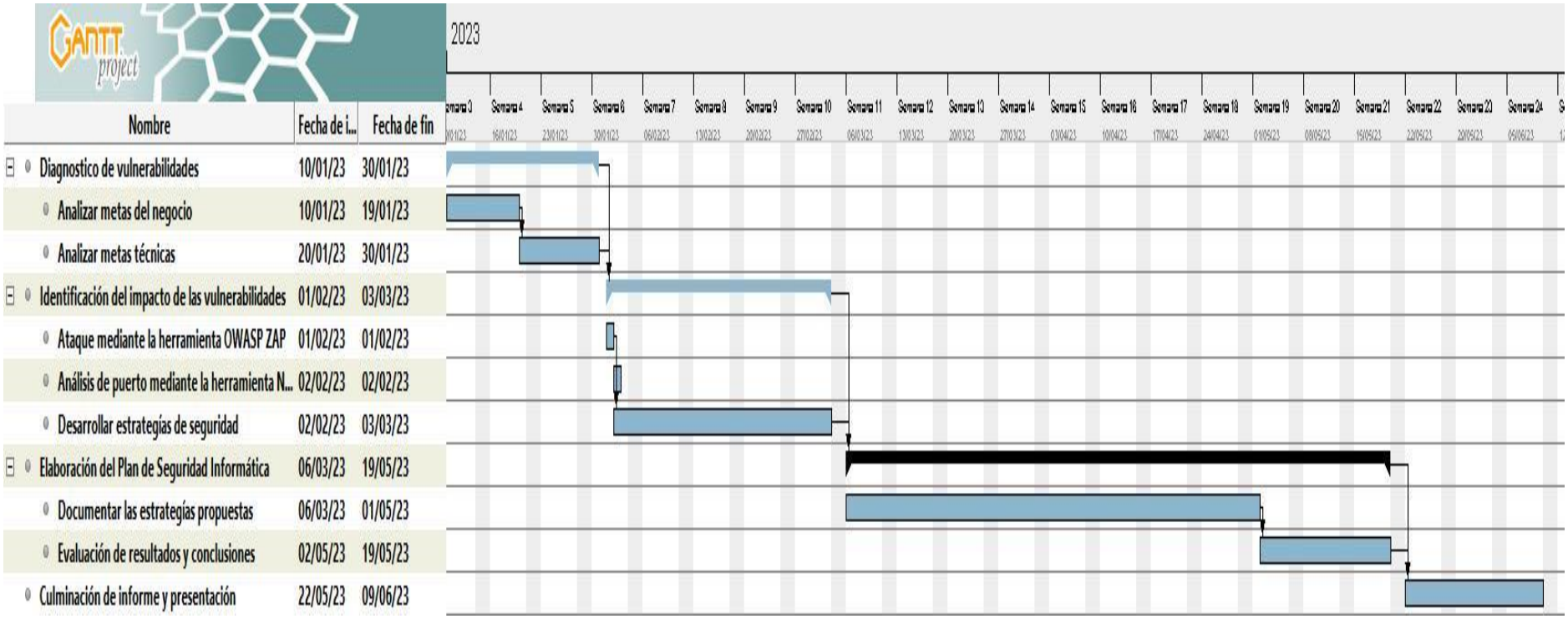
Talalaev, A. (2018). What is Web Application Firewall (WAF)?. Recuperado de https://www.webarxsecurity.com/web-application-firewall/

## ANEXOS

## ANEXO 1: CRONOGRAMA DE GANTT

**Figura 20**

*Diagrama de actividades Gantt*




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

## ANEXO 2: PRESUPUESTO

**Tabla 9**

*Presupuesto*

| DESCRIPCIÓN | CANTIDAD | VALOR UNITARIO | VALOR TOTAL |
|---|---|---|---|
| Laptop | 1 | 600 | 600 |
| Internet (por mes) | 6 | 35 | 210 |
| Carpetas | 2 | 0,5 | 1 |
| Esferos | 2 | 0,35 | 0,7 |
| Impresiones | 3 | 3 | 9 |
| Transporte | 25 | 1 | 25 |
| Pendrive | 1 | 5 | 5 |
| | | **Total** | $850,7 |

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

# ANEXO 3

Carta de Aceptación

**Memorando Nro. UEB-TIC´S-2022-0735-M**

**Guaranda, 20 de diciembre de 2022**

**PARA:** Srta. Mgs. Galuth Irene Garcia Camacho
**Profesora**

**ASUNTO:** SE AUTORIZA DESARROLLAR EL PROYECTO DE INVESTIGACIÓN DENOMINADO "ANÁLISIS DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UEB BASADO EN LA NORMA ISO 27001:2022-ANEXO A, EN EL AÑO 2023"

De mi consideración:

Con un cordial saludo, en atención al Oficio 039-2022-UIC-SOF de fecha 19 de diciembre de 2022, que manifiesta: "(...)Actualmente los estudiantes del octavo nivel de la carrera de software están cursando la asignatura trabajo de titulación e integración curricular, en la cual se da acompañamiento a su proceso de titulación en donde los jóvenes trabajan en dar solución a problemas en el área de la informática, mediante el desarrollo de proyectos de investigación y/o tecnológicos.

Por lo expuesto, solicito de la manera más comedida se dé la autorización para desarrollar el proyecto de investigación denominado "SE AUTORIZA DESARROLLAR EL PROYECTO DE INVESTIGACIÓN DENOMINADO "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" propuesto por los señores Llanos Vargas Klever Dennis con cédula de identidad1600700452 y Soriano Panchana Michael Daniel con cédula de identidad 2450066002, con la finalidad de dar respuesta a necesidades informáticas reales de nuestro contexto".

Sobre el particular, me permito comunicar que se autoriza el desarrollo del PROYECTO DE INVESTIGACIÓN DENOMINADO "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".

Particular que pongo en su conocimiento para los fines consiguientes.

Atentamente,

**Memorando Nro. UEB-TIC´S-2022-0735-M**

**Guaranda, 20 de diciembre de 2022**

***Documento firmado electrónicamente***

Ing. Edgar Henry Albán Yánez
**DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**

la

Firmado electrónicamente por:
EDGAR HENRY ALBAN YANEZ

**ANEXO 4: GUIÓN DE LA ENTREVISTA**

**Dirigido a:** Ing. Henry Albán

**Objetivo:** Recopilar información del director de TIC's y el coordinador de la unidad de desarrollo de software sobre las incidencias ocurridas en el sistema SI@NET de la Universidad Estatal de Bolívar.

**Fecha:** 27 de febrero de 2023

**Descripción:** Se realizará la entrevista al director de TIC's y al coordinador de la unidad de desarrollo de software de la Universidad Estatal de Bolívar.

1. **¿La institución ha tenido algún incidente relacionado con la seguridad informática en los últimos 3 años?**
   SI ( )
   NO ( )
2. **¿Qué problemas de seguridad informática ha tenido el sistema académico integrado en red (SI@NET) en sus módulos activos?**
   Respuesta: _____
3. **¿Qué módulos específicos han sufrido ataques?**
   Respuesta: _____
4. **¿Cuáles fueron los problemas más relevantes para el sistema SI@NET?**
   Respuesta: _____
5. **¿Qué temas de seguridad aún no se puede controlar en su totalidad?**
   Respuesta: _____
6. **¿Se aplica actualmente políticas o normas de seguridad para proteger la información en el sistema SI@NET en sus cuatro módulos activos?**
   SI ( )
   NO ( )
7. **¿Qué mecanismos, técnicas o herramientas o normas de seguridad se utilizan en el sistema SI@NET de la Universidad Estatal de Bolívar (UEB)?**
   Respuesta: _____
8. **¿Qué conocimientos tiene sobre las políticas o normas que gestionan la Seguridad de la información?**
   MUY ALTO ( ) MEDIO ( ) MUY BAJO ( )
   ALTO ( ) BAJO ( )

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

   SI ( )

   NO ( )

10. **¿Disponen de algún plan de gestión de seguridad informática aplicable a la UEB?**

    SI ( )

    NO ( )

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

    SI ( )

    NO ( )

## ANEXO 5: FICHA DE OBSERVACIÓN

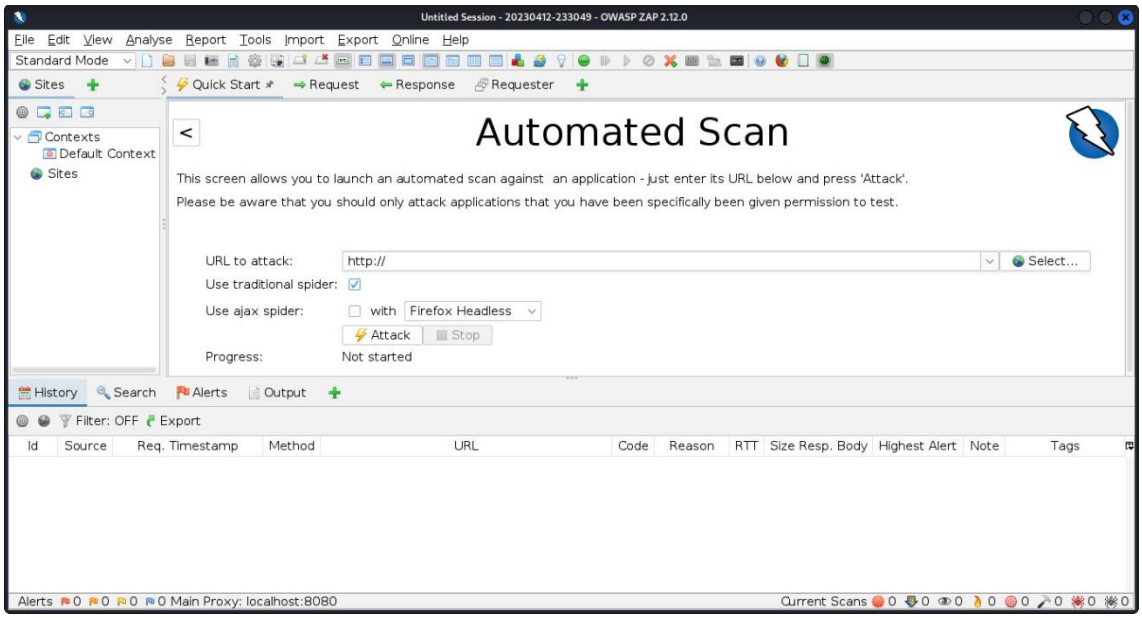
| | | | |
|---|---|---|---|
| **Institución:** | Universidad Estatal de Bolívar | **Ficha N°:** | 1 |
| **Dirección:** | Ernesto Che Guevara y Gabriel Secaira | **Hora Inicial:** | 00:00pm |
| **Fecha:** | 00/00/2023 | **Hora final:** | 00:00pm |
| **Observador:** | Michael Soriano – Klever Llanos |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

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

## ANEXO 6: HERRAMIENTA DE HACKING ÉTICO OWASP ZAP

**Figura 21**

*Programa de hacking ético OWASP ZAP*



# ANEXO 7

Certificado y Reporte Antiplagio

UEB
UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

**ING. EDGAR HENRY ALBÁN YÁNEZ EN CALIDAD DE DIRECTOR(A) DEL TRABAJO DE INTEGRACIÓN CURRICULAR,**

# CERTIFICA

Que el trabajo de integración curricular denominado **"ANÁLISIS DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA ACADÉMICO INTEGRADO EN RED (SI@NET) DE LA UNIVERSIDAD ESTATAL DE BOLIVAR, BASADO EN LA NORMA ISO 27001:2022 – ANEXO A, EN EL AÑO 2023."**, presentado por **MICHAEL DANIEL SORIANO PANCHANA & KLEVER DENNIS LLANOS VARGAS** estudiantes de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta **URKUND**, reflejando un porcentaje de similitud del **3%**, como se puede evidenciar en el documento adjunto.

Guaranda, 15 de mayo del 2023

Atentamente,

Ing. Edgar Henry Albán Yánez
**Director**

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

# Document Information

| | |
|---|---|
| Analyzed document | Proyecto de Investigación (Correccion_20).pdf (D166928702) |
| Submitted | 2023-05-15 01:36:00 |
| Submitted by | |
| Submitter email | msoriano@mailes.ueb.edu.ec |
| Similarity | 3% |
| Analysis address | halban.ueb@analysis.urkund.com |

# Sources included in the report

# Entire Document

# Hit and source - focused comparison, Side by Side

- Submitted text
  As student entered the text in the submitted document.
- Matching text
  As the text appears in the source.

Firmado electrónicamente por:
EDGAR HENRY ALBAN YANEZ

# ANEXO 8

Certificado de Entrega

Guaranda, 23 de junio del 2023

**CERTIFICA**

Por medio de la presente, certifico que el Sr. **Michael Daniel Soriano Panchana** y **Klever Dennis Llanos Vargas** portadores de las cédulas de identidad **N° 2450066002** y **1600700452** respectivamente; egresados de la **Universidad Estatal de Bolívar** de la Carrera de **SOFTWARE**, realizaron la entrega del "Plan de Gestión de Seguridad de la Información (PGSI)", correspondiente a su proyecto de Integración Curricular, en el cuál estoy conforme con el producto final.

Es todo cuanto puedo mencionar en honor a la verdad, pudiendo las partes interesadas hacer uso del presente según consideren conveniente.

Atentamente,

Firmado electrónicamente por:
EDGAR HENRY ALBAN YANEZ

Ing. Henry Albán